SENADO FEDERAL

Secretaria-Geral da Mesa

ATA DA 4ª REUNIÃO DA SUBCOMISSÃO PERMANENTE DE DEFESA CIBERNÉTICA DA 2ª SESSÃO LEGISLATIVA ORDINÁRIA DA 57ª LEGISLATURA, REALIZADA EM 09 DE JULHO DE 2024, TERÇA-FEIRA, NO SENADO FEDERAL, ANEXO II, ALA SENADOR ALEXANDRE COSTA, PLENÁRIO Nº 7.

Às quatorze horas e quinze minutos do dia nove de julho 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, Nelsinho Trad e Astronauta Marcos Pontes, e ainda dos Senadores Paulo Paim, Marcos do Val, Sérgio Petecão, Angelo Coronel, Professora Dorinha Seabra, Hamilton Mourão, Rogério Carvalho, Izalci Lucas e Weverton, não-membros da comissão. 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:** Destinada a debater os riscos internacionais em segurança cibernética e a importância de uma agência nacional de segurança digital no Brasil. **Participantes:** Senhor Belisario Contreras, Diretor Sênior (representante de: Venable Advocacia (LLP)); Senhor Santiago Paz, Especialista Setorial em Segurança Cibernética (representante de: Banco Interamericano de Desenvolvimento (BID)); Senhor Jorge Blanco, Diretor de Segurança da Informação (CISO) (representante de: Google); Senhor Rafael Gonçalves, Executivo (representante de: Trellix); Senhor Paulo Manzato, Chefe da Área de Setor Público (representante de: Cloudfare); e Senhora Patricia Soler, Líder no Colaborativo Conjunto de CiberDefesa (representante de: CISA - Agência Americana de Cibersegurança e Infraestrutura). **Resultado:** Audiência Pública Interativa realizada. Nada mais havendo a tratar, encerra-se a reunião às dezesseis horas e cinquenta e dois 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/2024/07/09

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 4ª 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 3ª Reunião da Subcomissão, ocorrida em 18 de junho de 2024.

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

Está aprovada.

Finalidade desta reunião: a presente audiência pública interativa tem como objetivo debater os riscos internacionais em segurança cibernética e a importância de uma agência nacional de segurança digital no Brasil. Ou seja, nós estamos numa jornada em que o Governo brasileiro também está estudando alternativas de como se posicionar em face a este risco internacional, que é reconhecido. Qual modelo a ser adotado incumbirá quase que certamente a uma iniciativa do Executivo e a uma manifestação do Legislativo.

Aproveito para registrar aqui a presença do Senador Mourão.

Aqui eu procurei resumir o que nós temos de informação advinda do Governo Federal.

A reunião será interativa. Portanto, a nossa busca é de subsídios para dar eficácia a tal política pública, a esta política pública. Então, é transmitida ao vivo, 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.

O presente encontro contará com a tradução simultânea, quando necessário, em inglês-português.

Contaremos com a participação dos seguintes convidados: Sr. Belisario Contreras, Diretor Sênior da Venable Advocacia, com mais de 120 anos de experiência; Sr. Santiago Paz, Especialista Setorial em Segurança Cibernética do Banco Interamericano de Desenvolvimento; Sr. Jorge Blanco, Diretor de

Segurança e Informação do Google; Sr. Rafael Gonçalves, Executivo da Trellix; Sr. Paulo Manzato, Chefe da Área de Setor Público da Cloudflare; e a Sra. Patricia Soler, Líder do Colaborativo Conjunto de CiberDefesa da Cisa, Agência Americana de Cibersegurança e Infraestrutura.

Registo mais uma vez, com satisfação, a presença de todos os que estão assistindo e registo, mais uma vez, a presença do Senador Mourão.

Esclareço que nós vamos dividir os oradores em dois painéis: o primeiro, com ênfase no tema "A importância de uma agência nacional de cibersegurança para o Brasil", e o segundo, com o tema "A importância da cooperação entre o poder público e o setor privado no combate aos crimes cibernéticos".

Os senhores debatedores terão inicialmente dez minutos para a sua participação. Claro que esse limite de tempo é um limite especificado para que a reunião não se prolongue por um tempo demasiado. Se houver necessidade de prolongar por algum momento, a Presidência não fará objeções intransigentes.

Caso necessário, será permitida uma réplica de até cinco minutos e tréplica de três.

Portanto, este primeiro painel tem como objetivo, repito, a ênfase à importância de uma agência nacional de cibersegurança para o Brasil. Esse seria o principal tema dos três primeiros convidados, ao tempo em que registro, com grande satisfação, a presença do Senador Fernando Dueire.

Concedo a palavra... Em homenagem à paz, concedo a palavra primeiro à Paz.

Salaam ou *Shalon*, estaremos dizendo a mesma coisa.

O SR. SANTIAGO PAZ (Para expor.) – Muito obrigado.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – O senhor tem dez minutos, por favor, Sr. Santiago.

O SR. SANTIAGO PAZ – Perfeito.

Então, boa tarde a todos.

Muito obrigado, Senador, pelo convite, muito obrigado a todos pelo tempo.

Eu sou o Santiago Paz. Desculpe-me pelo meu portunhol, mas eu vou fazer o maior esforço.

Hoje eu vou falar da importância que tem um modelo de governança nacional para a segurança cibernética.

Eu gostaria de compartilhar a apresentação.

A próxima.

Então, primeiro, a importância do risco cibernético.

Eu não quero perder muito tempo falando disso, mas todos aqui conhecemos os riscos cibernéticos que existem. Hoje, o Fórum Econômico Mundial considera o risco cibernético um dos dez maiores riscos do mundo.

Uma vez depois da pandemia, a quantidade de incidentes no ano foi duplicada nos últimos quatro anos, e isso está muito relacionado com o aumento da transformação digital. Todos os governos, todas as empresas tiveram que fazer uma transformação digital muito grande. Então, a superfície de exposição cresceu e, agora, está exposta a ter mais ataques.

O Instituto Ponemon fala que o custo médio de um ataque a uma organização do governo é uns US$4 milhões. E temos países pequenos, como a Espanha, com 40 milhões de habitantes, que tem 100 mil incidentes no ano. Os Estados Unidos têm muitos, mas estamos falando de bilhões de dólares de impacto econômico que têm os ataques cibernéticos todos os anos.

O Brasil, vocês sabem, tem um nível de digitalização muito bom, é o segundo país melhor do mundo em governo digital. Tem um nível de exposição muito alto e tem que fazer alguma coisa para melhorar.

Você pode ir à próxima?

Então, no desafio da governança você tem mais e mais atores envolvidos todos os dias. Hoje não é somente um atacante e um defensor; tem muitos atacantes e muitos defensores: organizações que podem ser públicas, que podem ser privadas, e todas estão inter-relacionadas, trabalhando juntas.

Temos empresas de tecnologia que dão suporte a instituições de saúde, temos empresas de organizações do Governo que dão serviços a empresas do setor financeiro, temos um nível de

relacionamento muito grande, e isso faz muito complexo poder ter uma governança da cibersegurança correta no país.

Eu vou usar o exemplo da NIS 2, a normativa europeia de cibersegurança, que começou no fim de 2022 e tem que ser adotada, agora, neste ano, por todos os países da Europa. A Europa é a região do mundo que tem maior maturidade em temas de cibersegurança.

Então, a NIS 2 define 18 setores críticos para a segurança cibernética, 11 de alta criticidade e 7 também críticos. Cada um dos setores vai ter organizações que são essenciais para o funcionamento do país e organizações que são importantes, mas muitas organizações importantes podem mudar um problema, um serviço que é essencial.

Pode passar para o próximo.

Eu estou falando disso porque eu quero mostrar o exemplo de um caso em que não aconteceu uma boa governança, e, por isso, tiveram um problema muito, muito grande.

Você tem setores onde tem organizações de energia, tem o setor bancário, com os bancos, tem o mercado financeiro, saúde, instituições médicas, produtos químicos, água potável, todos os setores que trabalham, de forma diferente, que têm culturas diferentes e que respondem a reguladores diferentes, mas, ao mesmo tempo, todos os operadores, todas as organizações que trabalham, em cada um dos setores...

Se puder, o próximo.

Tem algumas organizações que são públicas – pode ser um hospital público, pode ser a Petrobras, pode ser o Banco Central –, mas tem também organizações privadas – você tem empresas privadas, bancos privados. Então, na hora de ter um incidente, a coordenação não é somente entre setores diferentes, não é somente entre o setor elétrico e o setor de infraestrutura digital, mas é também entre o setor público e o setor privado. Eles têm diferentes interesses, e é muito complexo fazer isso ao mesmo nível que a organização que está sendo afetada.

Então, vou falar um exemplo muito interessante que aconteceu, infelizmente, ano passado, na Colômbia, no caso, com a empresa IFX Networks, um provedor de serviços da nuvem, que trabalha em 17 países da América Latina. É um provedor privado da nuvem que teve um ataque de *ransomware*

que fez com que toda a sua infraestrutura estivesse fora de serviço por muito tempo, um ataque de *ransomware* que afetou uma empresa do setor privado.

Essa empresa do setor privado, no caso da Colômbia, tinha 50 órgãos do Governo instalados na mesma infraestrutura do provedor da nuvem do setor privado, especialmente o sistema de saúde, que a Colômbia não pôde ter, por uns dias. Até os planos de contingência começarem a funcionar, a Colômbia não tinha capacidade para fazer a gestão da saúde e do sistema de Justiça também. Então, não podia atender os casos, teve que passar tratamentos em papel, assinaturas dos juízes, novamente, em papel, e priorizar os casos. Foi um ataque a uma empresa do setor privado que afetou o setor da Justiça e que afetou o setor da saúde.

Porque, se vocês se lembram, cada um deles são setores críticos ao mesmo tempo, e, para fazer a coordenação da resposta a incidentes, a Colômbia não tinha uma organização centralizada para poder coordenar a todos, isto é, trabalhava, por um lado, o Ministério da Saúde, por outro lado, o Ministério de Justiça, por outro lado, a Presidência, por outro lado, o Ministério de Tecnologias; todos, ao mesmo tempo, tentando solucionar um problema cuja origem era uma empresa privada. Então, isso foi muito complexo e gerou um impacto muito grande, especialmente nos cidadãos da Colômbia, que não tiveram acesso à saúde e não tiveram acesso à Justiça.

A mesma infraestrutura do IFX Networks afetou também os sistemas de aquisições do Governo do Chile, o ChileCompra.

O ChileCompra teve um impacto de US$2 milhões por dia do incidente, porque não pôde fazer compras e vendas eletrônicas, tiveram que mudar tudo novamente para o papel. Também, o Governo, outro setor, mas outro país também.

Então, você imagina que tinha o Ministério da Saúde tentando falar com o nosso setor do Governo de compras e aquisições do Chile, justiça, setor privado. Isso provocou, nos 20 dias, um serviço muito defeituoso, afetando os colombianos e os chilenos.

Então, esse caso de incidentes mostra que, agora, você tem uma matriz em que o setor privado, o setor público, diferentes setores, como o setor elétrico, o setor de telecomunicações, de infraestrutura digital, estão todos, todos misturados.

Levando isso em conta, eu vou falar de umas ações que estão chegando aos países mais maduros em temas de cibersegurança.

Primeiro, do ponto de vista da estratégia, nós fizemos um estudo de umas 40 estratégias de cibersegurança no mundo, em que 75% das estratégias mais modernas, mais maduras da terceira geração consideram a segurança cibernética como um habilitador para a prosperidade econômica. A economia digital precisa de cibersegurança para poder funcionar.

Oitenta por cento das estratégias consideram que a parceria público-privada tem que ser feita, tem que ser levada em conta; sessenta por cento das estratégias mais modernas consideram também a promoção do setor local, da indústria de cibersegurança como uma indústria próspera em seus países.

Um caso muito bom é o caso de Israel. Eles têm uma indústria muito forte em desenvolvimento da cibersegurança...

(*Soa a campainha.*)

O SR. SANTIAGO PAZ – ... e 80% das estratégias falam da cooperação internacional.

Também estamos fazendo outro estudo, que é um estudo de agências de segurança cibernética nacionais, agências nacionais de segurança cibernética dos países mais avançados, especialmente Europa, Espanha, França, Itália, Austrália e Estados Unidos, em que encontramos que o objetivo principal de todas as agências nacionais de cibersegurança é a coordenação, obviamente, mas a coordenação de quem? Do setor público, do setor privado e do de defesa.

Não é uma coisa tanto dentro dos diferentes setores, mas sim do público-privado.

As atribuições mais comuns que têm as agências nacionais.

Capacidade regulatória: as agências podem regular o setor público, mas também o setor privado diretamente, fiscalizar e sancionar *incumplimiento*; têm muito foco na gestão de incidentes, como eu mostrei o caso da Colômbia, da IFX; e têm muito da inteligência, *cyber threat intelligence*, como um dos pontos importantes para a troca das informações.

Também, se falamos do orçamento, do orçamento anual aproximado, nós encontramos que vai de uns 20 milhões para agências menores, países como Itália, ou US$200 milhões de dólares para agências maiores, países como França. Estamos falando de países muito menores que o Brasil.

Tem uma estrela, porque tem o caso da Cisa, por exemplo, que é de bilhões de dólares. Os Estados Unidos investem muito mais, mas os países da Europa têm isso, e, em todos os casos, o orçamento incrementa ano após ano, uma vez que foi criada a agência.

Do número de...

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Poderia só repetir o valor do orçamento da agência da França?

O SR. SANTIAGO PAZ – Sim, França, exatamente, se me recordo, US$176 milhões para o ano de 2025.

Pode checar?

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

O SR. SANTIAGO PAZ – Por ano. Por ano. (*Pausa.*)

Sim, exatamente isso.

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

Pode prosseguir.

O SR. SANTIAGO PAZ – São 176 milhões de euros – são euros, não dólares – por ano para o ano 2025. Mas também foi aumentando ano após ano.

E o número da RHs também. Países como França e Itália têm de 150 a 800, mas têm uma estrela. Países maiores... A Austrália, por exemplo, tem 1,9 mil pessoas, aproximadamente, trabalhando lá. A Cisa também tem milhares de pessoas trabalhando lá. Mas países como a França e a Itália, da Europa, têm isso, umas 150 a 800.

Então, isso é para ter um comparativo do que estão fazendo outros países.

A Europa começou criando um enfoque muito *bottom-up*. Eles começaram criando um centro de resposta para o Governo, um centro de resposta da internet, muito parecido com o Brasil, especializado na parte de saúde, o setor financeiro sempre foi muito líder em cibersegurança, e, depois, eles criaram... Porque, uma vez que tiveram todo o desenvolvimento necessário, encontraram os problemas da governança.

Mas todos fizeram tudo em fases. Essa é a mesma recomendação. Não pode começar de zero e criar tudo, uma agência... Você pode ter uma primeira fase, nos primeiros anos, onde você vai colocar o foco na criação institucional e desenvolvimento do modelo de governança, a parte da capacidade normativa, a capacidade dos padrões técnicos, e um ponto muito importante é o fortalecimento do capital humano...

(*Soa a campainha.*)

O SR. SANTIAGO PAZ – ... porque, sem pessoas, você não vai poder desenvolver nada.

Na segunda fase, finalmente, é onde tem um fortalecimento operacional, capacidade operativa e distribuição geográfica.

A Coreia, com o tamanho da Coreia, tem quatro centros distribuídos geograficamente na Coreia. Pelo tamanho do Brasil, tem que se pensar que vai ter que ter vários centros também.

E, finalmente, cinco ou sete anos depois, você vai já estar numa fase de melhora contínua, onde tudo vai ser mais aprimorado, ano após ano.

É tudo. Desculpe-me pelo tempo.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Eu quero me congratular com o senhor, porque o senhor focalizou pelo menos dois aspectos que fazem parte das nossas prioridades. Eu não vou comentar, mas, naturalmente, os Senadores vão se inscrever.

Eu lhe agradeço por enquanto e passo a palavra ao Sr. Jorge Blanco, desejando que o senhor siga a trilha da objetividade do Paz.

O SR. JORGE BLANCO (Para expor. *Tradução simultânea*.) – Boa tarde, caro Presidente, Senador Amin, Senadores membros do subcomitê de segurança cibernética, caros senhoras e senhores.

Primeiramente, gostaria de agradecer em meu nome, em nome do Google, o convite para participar desta audiência pública.

E agora eu vou mudar do português. Eu consigo entender portunhol, mas está bem ruim. Perdão, eu vou falar em inglês. O.k.? Então, é o portunhol avançado.

Eu gostaria de começar a minha apresentação dando uma introdução sobre o cenário da ciberameaça brasileira, que tem um papel geopolítico em assuntos globais que continua a crescer: vários atores, com diferentes...

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Só para esclarecer aos nossos telespectadores e aos (*Fora do microfone.*)... quem tem acesso: canal 19, em português; canal 16, em inglês.

Obrigado.

O SR. JORGE BLANCO (*Tradução simultânea.*) – Muito obrigado.

Vários atores, com diferentes motivações vão ter a oportunidade para usar a infraestrutura eletrônica do Brasil e todos os aspectos da sociedade.

Indivíduos e organizações no Brasil têm uma ameaça ciberúnica. É uma interconexão global e local de ameaças, colocando riscos aos indivíduos, organizações e setores críticos da sociedade brasileira.

O *status* do Brasil como um poder de grande influência e como a maior economia da América do Sul trouxe a atenção de ciberespiões, e outras atividades financeiramente motivadas são uma ameaça constante aos usuários.

Notavelmente, temos uma variedade de operações, incluindo *data fetch* e outras distorções. Tem o fórum subterrâneo para ter acesso a pessoas maliciosas, informação sensível e ferramentas para comprometer usuários e instituições brasileiras.

Na medida em que o Brasil continua a crescer em significância econômica e geopolítica, vai permanecer um alvo para vários atores com diversas motivações. Esse cenário é uma arena complexa, desenvolvido e expandido ao longo dos anos pela convergência de ameaças globais e locais.

Para efetivamente salvaguardar as empresas brasileiras e os usuários brasileiros, é importante que essa ameaça... E ter uma tendência proativa para a cibersegurança. Então, da Google, realmente recomendamos ter um *approach* bem proativo para a cibersegurança.

Na escala nacional, cibersegurança é difícil, tem desafios únicos, diferentes da área privada. As coisas são muito conectadas por governos, a infraestrutura é crítica, desenvolvimento econômico, operações militares e o dia a dia dos cidadãos

Depois de ciberataques devastadores, como o que teve na corte, no STJ, em novembro de 2022, ou o ataque de *ransomware* na Costa Rica, tem um reconhecimento global sobre a importância da cibersegurança em nível nacional.

A Google oferece os princípios centrais e recomendações para todas as organizações, incluindo governos, para desenvolver uma postura de cibersegurança robusta, seguindo os princípios que nós também tomamos para a segurança interna.

Falando desses princípios, o primeiro passo é criar uma estratégia de cibersegurança... O Brasil publicou em fevereiro de 2022 e atualizou em dezembro de 2023.

Mesmo com uma forte estratégia para acessar o plano de cibersegurança, alguns desenvolvimentos inesperados ou circunstâncias inesperadas podem surgir: atores que antes não eram ameaças, mudanças políticas globais, como temos agora com o nosso ambiente geopolítico ou qualquer um dos eventos disruptivos. Dada essa realidade, as estratégias que sejam adaptáveis, flexíveis e responsivas são as mais efetivas.

Em cibersegurança, é crítico aprender sobre o passado e não reinventar a roda. Aprender da experiência de outros governos e companhias. Há muitos bons exemplos, alguns já foram mencionados. Nos Estados Unidos, tem as agências de segurança, a Cisa, que protege a infraestrutura crítica, e vocês vão ter a oportunidade de ouvir deles diretamente, depois desse painel.

No Reino Unido, eles têm um centro, CNC, que dá conselho ao Governo, negócios e ao público sobre cibersegurança.

Também temos vários exemplos na América Latina, iniciativas que já existem, como no Chile, a Agência Nacional de Cibersegurança do Estado. Tem o exemplo colombiano e do México... Centro internacional de cibersegurança.

Também tem a Agência da União Europeia para Cibersegurança, trabalhando para melhorar a cibersegurança entre os estados membros da União Europeia.

Cada uma dessas agências tem diferentes responsabilidades, mas todas compartilham o objetivo de coordenar os esforços de cibersegurança nacionais e internacionais, criando mecanismos robustos para a colaboração privada e pública e colaboração com parceiros... Desenvolvam um plano para uma emergência nacional, criando um plano de resposta nacional, mantendo-o e coordenando as diferentes instituições e os CSIRTs, que são responsáveis por uma resposta em nível nacional, é também uma responsabilidade centralizada.

Cria a sua força de trabalho cibersegurança...

Tem uma falta de profissionais de cibersegurança, como vocês provavelmente já sabem, e o problema só piora. Revolver esse problema não requer somente investimento em profissionais, mas investimento e planos devem ser coordenados de forma centralizada.

Uma das responsabilidades de uma agência de cibersegurança é investir em educação de cibersegurança, com avenidas formais e informais, durante a carreira de um profissional. Isso pode ter um impacto não somente na segurança nacional, mas também no setor privado, criando um sistema efetivo em volta da cibersegurança, que pode ter um impacto direto no PIB do país.

Outro princípio crítico tem a ver com infraestrutura segura e dispositivos seguros.

Dispositivos e redes do governo são de alta visibilidade e alvos de alto valor para ciberataque. Então, é importante usar a melhor segurança possível, para prevenir a perda de serviços, recursos, tempo e dinheiro. Com essa atividade crítica deve se lidar de forma coordenada.

Em termos de cibereducação, a escala de sociedade... Os setores públicos e privados não são os únicos *stakeholders* no sistema. Quase todo mundo usa a internet e a tecnologia para se comunicar...

(*Soa a campainha.*)

O SR. JORGE BLANCO (*Tradução simultânea.*) – ... fazer negócios e aprender. E, se eu não me engano, no Brasil estamos falando de 150 milhões de usuários de internet. O governo tem a obrigação de aumentar a conscientização do público (*Falha no áudio.*)... campanhas públicas para empoderar seus cidadãos e serviços providos por agências de cibersegurança.

Na medida em que se constrói seu programa de cibersegurança, haverá oportunidades para se regular, em que se pode avaliar onde se pode beneficiar de regulações. É importante pensar sobre o impacto no ecossistema como um todo, mantê-lo competitivo, saudável, dentro do seu país e dos seus mercados.

Em conclusão, o estabelecimento de uma cibersegurança robusta é uma tarefa multifacetada, requer planejamento estratégico e colaboração em vários setores. Uma entidade central coordenadora modelada em exemplos internacionais de sucesso ajuda a harmonizar o esforço, ajudando as colaborações privadas para emergências nacionais. Investir nisso e no desenvolvimento de uma força, garantir a infraestrutura de governo e promover o ecossistema nacional são importantes para garantir a infraestrutura crítica e os interesses nacionais.

Adicionalmente, educar o público empodera os cidadãos para participarem na defesa nacional contra as ciberameaças.

Muito obrigado.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Desejo registrar aqui (*Fora do microfone.*) a presença – acho que não fiz o registro – do Senador Marcos Pontes e do Senador Sergio Moro.

Quero agradecer também a presença do Brigadeiro Luiz Fernando, do Dr. Marcelo Malagutti e do Dr. André Molina, do Gabinete de Segurança Institucional do Governo Federal, presenças muito oportunas e que nos prestigiam sobremodo.

Concedo a palavra agora ao Sr. Rafael Gonçalves, da Trellix – eu pedi para ele nos apresentar o que quer dizer Trellix.

Registro a presença do Senador Jorge Seif, afinal, voltando ao nosso convívio sem o disfarce que vinha utilizando...

(*Intervenção fora do microfone.*)

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – ... sem se assemelhar aos Peaky Blinders.

É sempre muito bem-vindo.

E o Sr. Rafael Gonçalves, que é o Gonçalves, definiu a Trellix como sendo uma plataforma aberta e agnóstica – isso me remeteu aos meus tempos de quase jesuíta –, para conectar múltiplos sistemas de segurança, permitindo um ecossistema integrado de ciberdefesa.

Isso tem muito a ver, juntamente com as palavras do Sr. Santiago Paz, Senador Moro, com algo que V. Exa. já trouxe à nossa reflexão.

Com a palavra o Sr. Rafael Gonçalves.

O SR. RAFAEL GONÇALVES (Para expor.) – Muito obrigado.

Boa tarde a todos.

Até parafraseando o contexto que eu passei sobre o que seria a proposta agnóstica, faz muito jus ao que foi falado aqui já nesta Comissão.

A (*cyber)*segurança ou a cibersegurança – é um termo que eu preciso adaptar ao meu vocabulário – traz um desafio para as empresas, que é o volume de eventos, o alto volume de eventos e a escassez de pessoas para lidar com esse volume de eventos. Para dizer apenas esse como um único desafio, mas a gente poderia elencar outros, como a falta de mão de obra qualificada.

Um estudo da PUC Campinas demonstra que a gente tem, hoje, um déficit de 500 mil pessoas capacitadas em tecnologia, das quais apenas 140 mil, ou boa parte disso, são necessárias em cibersegurança.

Da forma como a gente vê a integração de múltiplos sistemas, a gente entende que não adianta a gente priorizar a coordenação de um ou outro sistema, mas interconectar qualquer um deles, independente da plataforma ou do fabricante dessa tecnologia.

Até por isso – um pouco da minha experiência: eu atuo diretamente aqui em Brasília, moro aqui em Brasília, meu principal papel é o aconselhamento de gestores públicos –, a gente percebe essa escassez, essa dificuldade no dia a dia do combate aos incidentes cibernéticos, muitos dos quais são, na verdade, traduzidos em crimes cibernéticos.

A atuação do crime cibernético tem crescido exponencialmente e só tende a aumentar. Então, respondendo à pergunta do Senador Esperidião Amin, sobre qual seria a importância da criação de

uma agência que possa olhar para a cibersegurança, coordenar, padronizar, eu diria que ela é indispensável e urgente.

A gente percebe uma falta de padrão, muitas vezes uma falta de priorização daquilo que seria o processo básico de padronização e proteção das empresas, não somente do setor público, mas muitas empresas do setor privado, que sofrem do mesmo problema, talvez até por uma situação cultural que a gente percebe diluída, mediante a ocorrência de uma situação, de uma ocorrência, de um incidente cibernético.

Muitas vezes, o aconselhamento se torna ineficaz, diante de uma despriorização das necessidades de cibersegurança.

Quando há um evento, quando há um incidente, tudo se ajeita, tudo se prioriza, mas, como mostram dados do relatório Insights do The World Economic Forum, o Global Risks Report, a gente percebe um pareamento, um crescimento muito vertical do ciber-risco ou da ciberinsegurança, como um consumidor de recursos financeiros, apontando na casa de dezenas de trilhões com o passar dos anos, dado este, inclusive, presente no estudo que embasa a própria fundamentação da agência, do comitê e da Política Nacional de Cibersegurança.

Então, dentro de todas as dificuldades que a gente percebe na gestão pública, na gestão dos recursos financeiros, o principal entrave para se conseguir um arcabouço básico que permita aos gestores públicos conhecerem os incidentes e responderem a contento é justamente a falta de um ecossistema integrado, e isso joga a luz exatamente sobre grande parte dos pontos da proposta, em que a centralização e a padronização seriam funções vitais da agência. Isso, para não dizer também um ponto importante, que é a orientação ou o embasamento para que agências do setor público possam buscar parâmetros definitivos e diretos em como elas podem construir esse ambiente favorável para o monitoramento e defesa contra ataques cibernéticos.

Dentro dessa proposta, a gente percebe que existem muitas coisas que hoje faltam ao dia a dia do gestor público. Para dar um dado um pouco mais empírico, relacionado à prática, à convivência, do que eu atuo no dia a dia, muitas empresas não possuem um profissional de cibersegurança especificamente. Acredito que deva haver – e acho que a agência é fundamental para isso – uma reformulação até mesmo da própria carreira pública em torno da tecnologia da informação e – por que não? – da cibersegurança.

Uma coisa que ainda agrava as condições de como a cibersegurança é sustentada no serviço público é a evasão de profissionais, dos poucos profissionais que existem, para fora do Brasil; a gente vem exportando profissionais de tecnologia da informação. E também há uma evasão de pessoas do serviço público para o setor privado, dado também demonstrado com bastante presteza dentro de todos os documentos e todos os estudos que embasam a criação da agência, onde se demonstra que a própria carreira pública precisa de uma reformulação em torno do profissional de cibersegurança, pela relevância que ele tem para a organização.

Mas eu vejo com bons olhos a mentalidade, neste momento, cercada pelo advento de inovações, como, por exemplo, a inteligência artificial, que vem muito para ajudar. Mas, da mesma forma como ela pode ajudar a ciberdefesa, ela também é veículo, também é ferramenta do cibercriminoso.

Então, eu diria que a necessidade é vital, é vital que a gente possa determinar e orientar o gestor público, suportando o déficit de conhecimento de pessoas capacitadas, de sustentação dos processos de cibersegurança, porque, por trás dessas atividades, pode não ter mais – e aí, entregando um pouco a idade aqui – uma pessoa muito estudiosa querendo se vangloriar de que obteve um dado do governo, mas sim uma pessoa mal-intencionada, visando a obter recursos de maneira ilícita, visando até ao financiamento de crime organizado, e isso passa pela tecnologia, passa pela reformulação, passa por tudo isto que a gente discute hoje aqui e que está muito bem colocado dentro do estudo de embasamento para a criação da agência.

Então, eu queria trazer essa visão prática, essa vivência que eu tenho em ciberdefesa.

Tive a felicidade, há alguns anos, de participar de uma das coordenações dos Jogos Olímpicos Rio 2016, na parte de cibersegurança, e, de lá para cá, dedico todo o meu tempo, a minha vida profissional, justamente a orientar e a auxiliar o setor público federal a como se proteger e a como resguardar as informações e – por que não? – os processos sistêmicos que sustentam a sociedade hoje em dia.

Então, agradeço muito a presença de todos os interessados, principalmente o convite e a possibilidade de discutir esse tema...

(*Soa a campainha.*)

O SR. RAFAEL GONÇALVES – ... tão importante para o nosso país.

Obrigado.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Parabéns pela exatidão do tempo. (*Risos.*)

Eu estou abrindo aqui a inscrição.

Temos a inscrição do Senador Sergio Moro, a inscrição do Senador Marcos Pontes e a inscrição do Senador Jorge Seif.

Antes de passar a palavra para o Senador Sergio Moro, eu só queria oportunizar duas questões: primeiro, uma das nossas propostas é conhecer mais a fundo a NCFTA. Trata-se... Vou me socorrer aqui da minha anotação.

O SR. SERGIO MORO (Bloco Parlamentar Democracia/UNIÃO - PR. *Fora do microfone.*) – The National Cyber-Forensics and Training Alliance

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

É, pelo menos a nosso ver, algo que vem ao encontro do que aqui foi exposto.

Mas, como esse interesse foi despertado pelo próprio Senador Sergio Moro, e ele é o primeiro inscrito, eu só assinalei isso como primeiro ponto para a sua colocação.

O SR. SERGIO MORO (Bloco Parlamentar Democracia/UNIÃO - PR) – Perfeito.

Agradeço ao Senador Esperidião Amin, cumprimento também os demais colegas aqui presentes e cumprimento também os expositores.

Eu creio que não existe aí uma controvérsia sobre a oportunidade, a necessidade de criação de uma agência nacional de cibersegurança no Brasil. Talvez a questão mais pertinente seja a estruturação de um formato e de um financiamento, até porque, infelizmente, embora entendamos que o investimento nessa área traz um retorno positivo, até mesmo para a economia do país, o Brasil vive um momento de aperto fiscal.

Mas as minhas perguntas são, assim, bastante objetivas.

As agências nacionais que foram mencionadas têm, entre as suas tarefas, a de combater ameaças cibernéticas, tanto à defesa nacional como à infraestrutura crítica, mas também crimes cibernéticos contra o setor público e o setor privado? É possível misturar todas essas tarefas numa única agência nacional? Por exemplo, as ameaças à defesa nacional, normalmente, têm uma peculiaridade em relação a, por exemplo, ameaças cibernéticas, por exemplo, golpes contra usuários privados da internet. Esses modelos que foram mencionados reúnem essas tarefas, especificamente?

O Senador Esperidião mencionou... Eu, quando fui Ministro da Justiça e Segurança Pública, fiquei muito bem impressionado com a experiência que existe nos Estados Unidos, mas também em outros países, dos chamados *fusion centers*, que reúnem agentes da lei de diversas agências governamentais, compartilhando inteligência, compartilhando estratégias e iniciativas.

Em particular, chamou-me a atenção essa NCFTA (National Cyber-Forensics and Training Alliance), que é um *fusion center*, até onde compreendi, criado a partir da iniciativa privada. As empresas e indústrias de vários ramos criaram esse centro de fusão, para compartilhar experiências, informação e para coordenar ações contra ameaças cibernéticas contra o setor privado, especificamente – inclusive, promovendo treinamento.

Não creio que esse tipo de centro substitui uma agência nacional, mas gostaria de ouvir a opinião dos senhores a respeito, caso, evidentemente, se sintam confortáveis em tratar desse assunto.

E, por fim – e aqui é uma pergunta bastante específica –, como as entidades que os senhores representam, por exemplo, o próprio BID, o Google ou a Trellix, poderiam ajudar o Brasil na criação de uma agência nacional de segurança cibernética, com modelos, projetos, assessoria, e, talvez, especificamente ao BID, com financiamento, porque essa é uma pergunta...

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC. *Fora do microfone*.) – Se já houve precedente...

O SR. SERGIO MORO (Bloco Parlamentar Democracia/UNIÃO - PR) – ... importantíssima para nós.

São essas as três indagações.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Eu considero as perguntas – as colocações – muito objetivas. Por isso, nós vamos fazer em bloco; somos poucos.

Eu concedo a palavra, pela ordem, ao Santiago Paz, ao Jorge Blanco e ao Rafael Gonçalves, para um comentário de – em torno de – três minutos, podendo ser prorrogado.

O SR. SANTIAGO PAZ (Para expor.) – Perfeito.

Senador, muito obrigado pelas perguntas muito interessantes.

Em relação à primeira pergunta, de se ter um centro integrado com cibersegurança, cibercrime e ciberdefesa, tudo junto, no estudo que nós fizemos, dos seis países que analisamos, não é possível encontrar um padrão em que você pode ver tudo junto, tudo separado. Alguns países têm as agências de inteligência, onde também tem a parte de cibersegurança; outros países têm no âmbito civil a parte de cibersegurança.

Então, a coisa mais fácil de poder ver é que a mistura não é uma boa opção. Em geral, as agências nacionais são a coisa que faz coordenação entre os corpos da *law enforcement* – a polícia, o Ministério Público, a Justiça –, coordenação também com ciberdefesa e coordenação de tudo no âmbito civil e em infraestruturas críticas. É uma missão em que está tudo integrado e pode ter algum risco da troca incorreta das informações.

Se a polícia está vendo um ataque, tem que ver do ponto de vista do crime, mas, se a cibersegurança está vendo um ataque, tem que ver do ponto de vista de contenção e mitigação. Então, tem algumas diferenças.

Esse é o primeiro. O segundo é de *fusion center*.

Eu gosto também muito de *fusion center,* ISAC, *information sharing alliance* ou centros de excelência, que também têm... A Otan tem um centro de excelência na Estônia de cibersegurança, tem muitos exemplos de pontos de contacto...

(*Soa a campainha.*)

O SR. SANTIAGO PAZ – ... para troca de conhecimentos e para troca de informações de cibersegurança, mas acho que é outro modelo.

Habitualmente, os órgãos centrais de coordenação de cibersegurança têm uma visão mais operativa, têm uma regulação mais direta. *Fusion center* tem mais desenvolvimento de conhecimento, desenvolvimento de capacidades, mas não tem a capacidade de gerar uma regulação, porque é

obrigatório ter uma política de cibersegurança e fazer a fiscalização, e também não tem a capacidade de sancionar. Então, acho que é muito bom ter um – ou mais de um, para o tamanho do Brasil –, mas acho que não é uma substituição do órgão central de coordenação de cibersegurança.

E o terceiro ponto do papel do BID, como podemos apoiar vocês.

O BID tem diferentes instrumentos de trabalho, todos gêneros de desenvolvimento de conhecimento. Vocês sabem que, junto com a OEA, o BID tem um reporte de maturidade em cibersegurança de toda a região que fazemos a cada quatro anos, usando o modelo de maturidade da Universidade de Oxford. Temos também muitos documentos da cibersegurança para setores específicos, para setores de saúde, para *smart cities*, para setor de energia, para setor de água potável. Então, temos toda uma linha de trabalho, que é desenvolvimento de conhecimento.

Temos também ações de cooperação técnica, em que temos apoiado a SGD, o desenvolvimento do Centro Integrado de Cibersegurança, em que temos apoiado o Uruguai e muitos países da região, com assistência técnica para desenho, para consultorias de apoio aos países.

E também temos a linha de empréstimo, de financiamento, em que temos operações de financiamento de crédito para todo o desenvolvimento do Centro Nacional de Operações do Uruguai, que foi financiado pelo BID, também do Centro de Cibersegurança para Infraestruturas Críticas da Argentina, que também foi financiado pelo BID.

Então, temos diferentes instrumentos. Então, contem conosco para trabalhar coisas de que vocês precisam.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Posso passar para o seguinte?

O SR. JORGE BLANCO (Para expor. *Tradução simultânea*.) – Obrigado.

Sobre a primeira pergunta, sobre uma agência única, sobre os diferentes exemplos em diferentes países... O modelo, como o Sr. Paz mencionou, não é homogêneo. Então, por exemplo, nos Estados Unidos, temos muitas agências de segurança que estão cuidando de operações militares ou de defesa, inteligência contra ameaças... No final, todas as organizações estão coordenadas e reguladas.

Sobre a estratégia da Cisa, por exemplo, no Reino Unido é a mesma coisa. A Agência Nacional de Cyber Segurança no Reino Unido cuida não só do setor privado, mas também do setor público e dos cidadãos.

Eu posso falar mais sobre o meu próprio país. Na Espanha, por exemplo, nós temos duas agências diferentes. Uma lida com o setor público e com a inteligência. Então, lida também com as ameaças militares. É o Centro Criptológico Nacional. A outra cuida do setor privado, especialmente de empresas pequenas e médias e de cidadãos, mas ambos são coordenados pelo Departamento de Segurança Nacional. Sempre tem uma entidade, pode ser uma agência com o poder de execução, mas também pode ser uma agência só com orientações e uma estratégia que está coordenando tudo.

Então, é uma mistura de diferentes modelos, dependendo do país, sobre os Fusion Centers, ou CISAs, que também são conhecidos na indústria, que são os Centros de Compartilhamento...

(*Soa a campainha.*)

O SR. JORGE BLANCO (*Tradução simultânea.*) – ... de Informação.

Nos Estados Unidos, por exemplo, temos vários centros para cada indústria, e é obrigatório compartilhar inteligência entre as diferentes empresas no setor privado, mas esse modelo não está funcionando muito bem em diferentes locais. Eu tenho experiência na Europa e na América Latina porque o compartilhamento não é obrigatório. Esse modelo não funciona bem, se não o for.

Sobre como o Google pode ajudar o Brasil a criar um centro nacional de cibersegurança, podemos fornecer nossa própria experiência, ajudando outros governos. Nós temos uma referência pública, e foi mencionado.

Estamos ajudando o Governo de Israel, em um conceito chamado *cyber shield*, ou *cyber* escudo, que contém nossas melhores práticas, processos e serviços. Também já estamos desenvolvendo o mesmo conceito em outros países, que não é referência pública. Por exemplo, no Oriente Médio, em um país na África e em alguns países da América Latina. Então, nós temos experiências em proteger governos.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) – Agradeço ao Sr. Jorge Blanco e passo a palavra ao Sr. Rafael Gonçalves.

O SR. RAFAEL GONÇALVES (Para expor.) – Obrigado.

Bom, com relação à primeira pergunta, a criação da agência, num primeiro momento, figuraria muito importante, de maneira a orientar e a regular o ciclo de vida da segurança de informação, para depois embasar um processo de resposta a incidentes. Então, como a gente chama, é uma segurança viva que precisa evoluir a cada instante, principalmente porque o próprio ofensor se moderniza também.

Então, o papel da agência para lidar com o próprio volume de eventos precisaria ter um corpo muito, muito maior, mas, em termos de proposição mandatória do compartilhamento de dados, este eu acredito que já não seria exatamente o caminho para a agência, mas sim o de regulamentar, o de propor ações e até mesmo fiscalizar as empresas que não adotam a postura mínima, que não adotam a padronização, cuja criação seria vital.

Com relação a como a gente pode auxiliar, seria justamente com a nossa experiência, a nossa presença – como empresa americana, muito presente no próprio Governo americano.

A experiência que a gente pode trazer é, justamente, de como é pensada a ciberdefesa em outros países. A gente tem atuação no mundo inteiro, claro, mas essa presença no próprio Governo americano nos traz muita "vanguarda" em como a gente poderia auxiliar, de repente, fazendo uma proposição de intercâmbio de informações dentro do possível da confidencialidade, mas acredito que, dentro dessa proposta...

(*Soa a campainha.*)

O SR. RAFAEL GONÇALVES – ... de compartilhamento dessa *expertise*, a gente já faz isso naturalmente e a gente poderia buscar uma forma de intensificar essas ações, trazendo realmente o nosso conhecimento e o nosso interesse para fomentar aqui iniciativas de inovação, padronização e melhoria do monitoramento e resposta a incidentes cibernéticos no Brasil.

Obrigado. (*Fora do microfone.*)

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Antes de passar a palavra para o Senador Marcos Pontes, pergunto se o Senador Sergio Moro gostaria de fazer algum comentário sobre as respostas.

Eu vou fazer um, para estimular o senhor a fazer uma pequena colocação.

Se a memória não estiver me falhando, quando o GSI fez o levantamento da proposta de constituição de uma agência, fez inclusive um pré-orçamento e, se a memória não estiver me falhando, ele chegou ao valor de R$594 milhões por ano. É isso? (*Pausa.*)

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – E um número de servidores de até 800, coincidindo com o padrão que o BID aqui apresentou. Por serem euros, dá um pouco mais do que isso...

O SR. HAMILTON MOURÃO (Bloco Parlamentar Aliança/REPUBLICANOS - RS. *Fora do microfone.*) – Compartilhamento.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – ... ou seja, eu tenho a impressão de que alguém espionou alguém. (*Risos.*)

O SR. HAMILTON MOURÃO (Bloco Parlamentar Aliança/REPUBLICANOS - RS. *Fora do microfone.*) – Eu acho que alguém espionou alguém.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Com a palavra o Senador Sergio Moro, se quiser fazer alguma...

O SR. SERGIO MORO (Bloco Parlamentar Democracia/UNIÃO - PR. *Fora do microfone.*) – Não, eu acho...

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Então vamos ouvir o nosso Senador Marcos Pontes.

O SR. SERGIO MORO (Bloco Parlamentar Democracia/UNIÃO - PR. *Fora do microfone.*) – ... mas agradeço.

O SR. ASTRONAUTA MARCOS PONTES (Bloco Parlamentar Vanguarda/PL - SP. Pela ordem.) – Obrigado, Presidente, boa tarde. Boa tarde a todos.

Prezados, obrigado por estarem aqui conosco para compartilhar informações.

Também tenho três perguntas relativamente simples, mas importantes nesse sentido.

Eu faço parte da Comissão de Inteligência Artificial, e essa discussão tem sido bastante intensa aqui no Brasil.

(*Intervenção fora do microfone.*) (*Risos.*)

O SR. ASTRONAUTA MARCOS PONTES (Bloco Parlamentar Vanguarda/PL - SP) – Inicialmente, nós tínhamos uma proposta de uma agência para a inteligência artificial – regulação – e, no final, essa proposta acabou caindo, porque inteligência artificial é uma tecnologia, é uma agência para uma tecnologia, é algo que não faz muito sentido.

Então, isso aí ficou de lado e foi substituído por uma ideia mais de um conselho formado por vários representantes de diversos setores, das agências reguladoras, por exemplo, que podem trabalhar levando os princípios dessa lei para dentro de cada uma das suas respectivas áreas de atuação., e eu fui um dos proponentes dessa ideia de não haver uma agência e de que tivesse esse tipo de conselho.

E aí, dentro desse contexto, dessa estrutura, quando eu ouço a respeito de uma agência para segurança cibernética, eu vejo de uma forma um pouco diferente, porque não é uma tecnologia. Ela envolve diversas tecnologias e acaba sendo um sistema, ou até um setor, pode-se imaginar, que até conteria essa ideia de uma agência.

Mas aí entra o que o Senador Sergio Moro falou nessa questão, também comentado pelo Sr. Santiago Paz, da dificuldade de se colocar defesa cibernética, segurança cibernética, crimes cibernéticos, todos no mesmo contexto, mesmo porque nós temos já, dentro do Exército Brasileiro, um setor destinado à defesa cibernética, pensando em nível de país, logicamente.

A minha pergunta, a primeira pergunta, é em relação a essa estrutura.

Uma das ideias que eu andei pensando, à medida que trabalhávamos com a inteligência artificial, é a seguinte: a nossa Autoridade Nacional de Proteção de Dados, que trabalha com dados de pessoas... É lógico que inteligência artificial usa muitos dados, incluindo de pessoas, mas de outras coisas. Então, ela seria a coordenadora desse conselho, que, de acordo com o texto atual, está dessa forma, para que nós tivéssemos ali o próprio Conselho Nacional de Proteção de Dados, que já existe, um outro conselho ligado à inteligência artificial, que são, de certa forma, correlatos, existe uma correlação entre eles, e a minha ideia seria de que ali também tivesse um conselho para segurança

cibernética, relativamente, da mesma forma, com representantes dos diversos setores reguladores, com representantes da sociedade civil e, aí sim, representante do Exército Brasileiro, na questão da segurança, da defesa cibernética, e, obviamente, do setor privado, que já tem os seus setores de segurança cibernética estabelecidos, principalmente as empresas maiores, como bancos e etc.

Dentro desse contexto, a minha pergunta é o que vocês acham dessa estrutura, se vocês a acham adequada e se ela poderia responder às necessidades, colocando dessa forma.

Ainda nessa sequência, falando de estruturas, nós vemos, por exemplo, nos Estados Unidos, existe lá o Nist, que tem já desenvolvido uma série de estudos de fragilidades, vulnerabilidades com relação à segurança cibernética, que são utilizados... Os desenvolvedores de *software* utilizam aquilo frequentemente, para verificar e testar seus *softwares* para ver onde e como podem ser vulneráveis. Se for em termos de *network*, por exemplo, ou de *websites*, o ASP também... O ASP publica sempre, anualmente, as dez maiores fragilidades, e assim por diante, o que também é utilizado. Ela é uma organização que não é do Governo, é uma organização não governamental. Nós não temos algo semelhante ou com essa estrutura aqui no Brasil, embora nós tenhamos algumas coisas ligadas mais à internet.

Como vocês veem a cooperação internacional, pensando do ponto de vista de que segurança cibernética é algo que transcende as fronteiras? Como que essa cooperação internacional pode ser vista? Mesmo porque os nossos fornecedores ou desenvolvedores de *software* também utilizam aquelas informações para esse desenvolvimento.

E, finalmente, a terceira pergunta é a utilização da inteligência artificial, porque, à medida que nós aumentamos as utilizações boas da inteligência artificial, também vêm as possibilidades de utilizações ruins da inteligência artificial, no contexto de dificultar inclusive a própria segurança cibernética, com ferramentas que você pode utilizar da inteligência artificial para buscar meios de ataque ou mascarar, por exemplo, uma anormalidade na rede. Existem dispositivos, logicamente, para detectar anormalidades na rede, IDS e assim por diante, que trabalham com isso, mas, logicamente, sempre uma inteligência artificial pode... Mas a gente pode usar também do lado positivo para a segurança cibernética. Eu só coloquei isso aí como exemplo, mas, de forma geral, como vocês veem a utilização de inteligência artificial, positiva ou negativamente, afetando a segurança cibernética? São essas três perguntas.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Concedo a palavra ao Sr. Santiago Paz.

O SR. SANTIAGO PAZ (Para expor.) – Muito obrigado pela pergunta, muito interessantes todas.

Da primeira pergunta, infelizmente eu não conheço os detalhes da legislação brasileira para saber se o nome é agência ou é, por isso eu falei todo o tempo de órgão central, uma organização, mas tem que ter uma estrutura orgânica com capacidade operativa. Então, habitualmente você tem um nível mais estratégico, político, em que os conselhos, os comitês fazem muito bom trabalho, porque eles têm uma visão estratégica, mais política, mas não é operativa. Então, o conselho trabalha, discute, chega a recomendações, mas não tem uma capacidade operativa como você precisaria, como no caso da Colômbia, que eu falei. Você não tem justiça, não tem saúde, tem que responder rápido. Então, você tem um nível político-estratégico, em que habitualmente os comitês e os conselhos funcionam muito, tem um nível tático e tem um nível operativo. Os lugares mais embaixo são onde as organizações operativas têm que trabalhar, que é a parte mais difícil. Muitas vezes os conselhos fazem isso, um bom trabalho político e estratégico, mas, na hora de ter uma resposta operativa, que você precisa o mais cedo possível, o conselho não é a melhor opção. É essa a minha percepção.

Isso primeiro. Depois, falando da cooperação internacional, de OWASP, de NIST, de diferentes padrões internacionais, isso é muito importante, o ponto. Creio que meu colega falou do ecossistema de cibersegurança. Não é somente o governo que vai desenvolver todas as ferramentas necessárias...

(*Soa a campainha.*)

O SR. SANTIAGO PAZ – ... não é somente a academia, não é somente a sociedade civil e o setor privado. São todos juntos trabalhando que vão conseguir o resultado.

Finalmente, a inteligência artificial: sim, acho que tem mais benefícios o uso de inteligência artificial do que os riscos de cibersegurança pelos ataques, mas eu prefiro que meus colegas falem mais disso.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Antes de passar a palavra ao Sr. Jorge Blanco, eu vou conceder ao Senador Seif, que vai ter que se retirar, para que ele faça uma intervenção. Pelo que eu entendi – foi gestual apenas –, a pergunta é para o Sr. Santiago Paz.

O SR. JORGE SEIF (Bloco Parlamentar Vanguarda/PL - SC. Para interpelar.) – Não, na verdade, Sr. Presidente, primeiramente quero parabenizá-lo pela Comissão, por esta reunião, que nós estamos fazendo, e cumprimentar o Sr. Santiago, o Sr. Jorge e o Sr. Rafael.

Na verdade, é só uma reflexão; depois, eu vou acompanhar a resposta dos senhores, porque eu tenho uma videoconferência para participar e já estou até um pouco atrasado.

A vida imita a arte, porque nós vemos hoje muitos filmes de Hollywood em que terroristas invadem, por exemplo, torres de aeroportos, causam caos nos centros de semáforos e causam confusão, alteram a leitura de GPS dos satélites para que aconteçam acidentes aéreos, etc. E, na vida real, nós vemos, hoje, empresas sendo sequestradas, ou seja, vai um ciberterrorista, bloqueia ali os dados de nota fiscal, de cobrança, de cliente, de receita, de produtos e fala o seguinte: "Rafael, ou você me paga R$2 milhões, ou vou deletar o seu banco de dados".

Deletar esse seu banco de dados é destruir a história da sua empresa. Você não sabe nem para quem cobrar mais nada, até que você se recupere; inclusive, existem reportagens de muitas empresas que jamais se recuperaram, não se propuseram a negociar com os terroristas e tiveram suas atividades encerradas.

A minha pergunta é simples. A iniciativa privada é muito mais eficiente, muito mais eficaz, muito mais veloz do que qualquer governo – pode ser Governo brasileiro, espanhol, americano, não adianta. As empresas privadas têm a capacidade de atrair os melhores talentos, pagar os melhores salários para profissionais de TI, sejam mais jovens, sejam mais antigos. Então elas têm uma condição... O próprio Google, dando aqui um exemplo, tem uma capacidade de atrair talentos, por exemplo, para cibercrimes ou ciberdefesa muito melhor do que se eu tiver uma agência aqui no Governo brasileiro, em que eu tenho uma meta fiscal, eu tenho teto de gastos e eu posso pagar, no máximo, sei lá, US$1 mil, US$2 mil ou US$3 mil.

A pessoa vai falar assim: "Poxa, se eu for para o Google, eu vou ganhar isso, aquilo e ainda posso subir; no Governo brasileiro, criaram aqui a agência de cibersegurança e o máximo de teto que eu tenho são US$3 mil; não tenho dúvida, eu vou para o Google".

Então, a minha pergunta para os senhores é: não é melhor que os governos façam contratos com empresas de defesa que façam segurança das suas plataformas digitais do que criar uma agência que, muitas vezes, fica obsoleta, muitas vezes vira um cabide de emprego e não vai ter os melhores

talentos? Não é melhor que os governos – e vou falar, obviamente, do Brasil – terceirizem essa atividade de segurança, para fazer um *firewall* sobre os sistemas dos municípios, dos estados ou do Governo Federal?

Essa é a minha dúvida, vou ouvir vocês depois pelo YouTube e peço perdão, porque o debate está interessantíssimo, mas eu tenho uma videoconferência.

Muito obrigado.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Antes de passar a palavra para o Sr. Jorge Blanco, eu vou dizer que os meus ouvidos não perceberam uma imparcialidade na sua pergunta (*Risos.*), mas ela é muito válida e vem ao encontro do que o Senador Sergio Moro falou sobre a NCFTA.

(*Intervenção fora do microfone.*)

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Sim, sim. Uma coisa não exclui a outra.

Com a palavra... Não sei se o Santiago quer fazer algum comentário a respeito, especificamente...

O SR. SANTIAGO PAZ (Para expor.) – Não, não. Somente... É simples, eu posso responder muito rápido, porque o que você falou do Governo e do setor privado é coisa que acontece em todos os países do mundo.

O Governo dos Estados Unidos faz um *outsourcing* no setor privado, muitas vezes para a capacidade operativa de ciberdefesa, para trabalhar tecnologia, para gerir os incidentes. A coisa que não acontece é a transferência da capacidade de regulação. Então, se você transferir para o setor privado, você vai regular a companhia elétrica... Isso não acontece. Então, é uma combinação que tem agências...

No caso da Espanha, é a mesma coisa. Eles têm a capacidade regulatória, têm algumas pessoas que trabalham lá e têm muitos serviços no setor privado, que são os que trabalham com a tecnologia.

O SR. JORGE SEIF (Bloco Parlamentar Vanguarda/PL - SC. *Fora do microfone.*) – Entendi. Obrigado.

O SR. SANTIAGO PAZ – Sou eu quem agradeço.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Jorge Blanco, voltando à pergunta do Senador Marcos Pontes e, complementarmente, à pergunta do Senador Jorge Seif...

O SR. JORGE BLANCO (Para expor. *Tradução simultânea*.) – Eu vou tentar responder às suas perguntas.

Em relação à estrutura, é diferente a criação de um conselho, como vocês estavam pensando, de inteligência artificial – ou uma agência, seja lá que nome vocês queiram dar – para uma entidade que vai ter responsabilidade operacional. O Sr. Paz mencionou o mesmo. Você não está trabalhando só em criar a legislação e a estratégia, mas você tem que agir, responder a um incidente e fazer uma análise forense... a proteção de um país... Então, essa é a diferença. Num conselho... E há outras iniciativas em termos de inteligência artificial globalmente, até nos Estados Unidos e na União Europeia. Estamos tentando engajar e, com o uso responsável de inteligência artificial, criar uma legislação para proteger os efeitos dessa tecnologia... A ausência de viés e o uso correto, e a proteção de dados com os quais eu estou pronto para, usando os modelos... legislando ou regulando, mas não operando. Essa é a grande diferença.

Desculpem-me.

No Google, como um jogador-chave da inteligência artificial, estamos promovendo esse uso responsável da IA. Em relação ao uso da IA em cibersegurança, devemos equilibrar, porque os criminosos...

(*Soa a campainha.*)

O SR. JORGE BLANCO (*Tradução simultânea*.) – ... estão usando esse tipo de tecnologia já faz muitos anos. Eles têm muitos recursos, mas também podemos usar – não só podemos, como devemos usar – a inteligência artificial para defender nossas organizações e governos. Em ambos, assegurar o uso da inteligência artificial e, do outro lado, usá-la para melhorar nossa cibersegurança. Então, são ambos.

Só para complementar a pergunta do Senador, de fato, o modelo que o meu colega mencionou é o mais comum, não só nos Estados Unidos e na Espanha.

O setor público – e isso é uma realidade – não tem os mesmos recursos que o setor privado, mas deveria depender de alguma taxa ou de uma camada de pessoas públicas ou trabalhadores públicos que mantivessem e protegessem os interesses nacionais, e, sobre esses, você pode usar quaisquer contratados, mas você tem que ter em conta essas confrontações geopolíticas com nações. Por exemplo, na Espanha, usamos não só servidores espanhóis, mas também empresas americanas, e novamente a gente só trabalhava com agências de ciberseguranças nacionais. Então, o uso de ambas as forças de trabalho é a melhor combinação.

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

O SR. RAFAEL GONÇALVES (Para expor.) – Bom, com relação às três perguntas, na criação de um conselho no lugar de uma agência – e aí concordando totalmente com o colega Santiago –, a operacionalidade vai fugir. Como lidar com o uso nos computadores pessoais, nos dispositivos pessoais, sabendo que essa informação trafega por meios controláveis? Mas como controlar esses meios?

O próprio uso do que a gente chama de *deep web*, que é uma internet não conhecida para o grande público, contrasta com o quanto a inteligência artificial ficou famosa. Apesar de ela ser novidade na sociedade, ela não é novidade na computação. Então, controlar a forma como o Governo poderia influenciar no uso da inteligência artificial é algo um tanto difícil, mesmo para uma agência, mesmo para um conselho.

O que eu vejo, na proposta do conselho, seria a observação desse tema na sociedade, os impactos que o uso da inteligência artificial – os impactos nocivos, claro – podem causar na sociedade, a coleta de insumos para o embasamento de políticas ou até mesmo de legislações que visem ali a auxiliar e a melhorar a sociedade quando a inteligência artificial for mal utilizada.

A segunda pergunta: cooperação internacional. Então, apesar de ser novidade para o Brasil e para o grande público a utilização da inteligência artificial, também é novidade para boa parte dos países. Então, a cooperação internacional...

(*Soa a campainha.*)

O SR. RAFAEL GONÇALVES – ... acho que é um tema que vai surgir naturalmente, mas, realmente, para fomentá-lo, são discussões como essa, são proposições como essa que vão beneficiar o pensamento para que se vá em direção realmente de uma cooperação nesse sentido.

Com relação ao uso da inteligência artificial, é extremamente benéfico na aceleração de alguns processos, mas, de maneira muito crítica, beneficamente, no ensino. O aprendizado com a inteligência artificial é muito mais facilitado.

Então, é claro que abusos podem ocorrer mesmo dentro disso, e isso, sim, é passível de observação e de controle, mas, dentro da utilização da inteligência artificial, a gente percebe que uma pessoa, talvez, sem determinado conhecimento prévio, para ir buscar capacitação num assunto, pode fazer uma busca muito mais orientada, embora o próprio Google já tenha revolucionado os motores de busca. Mas a inteligência artificial, sem dúvida nenhuma, pelo comportamento de ela, permita-me aqui o paralelo, falar com a pessoa com quem está interagindo, cria um cenário mais favorável para o ensino.

O uso da inteligência artificial, na minha opinião, deve ser encorajado, mas, em contrapartida, ele também não é algo controlável. Então, ele vai acontecer sim ou sim.

E, com relação ao que foi colocado pelo Senador antes de sair, se a agência se tornaria obsoleta, se haveria a possibilidade de se substituir esse trabalho, essa função por contratos de *outsourcing*, aí eu volto ao que eu falei inicialmente. A gente sofre com a falta de padronização, com a falta de priorização, e a agência entraria com regulamentação, fiscalização e, também, é claro, criação desses padrões mínimos de estratégia em cibersegurança.

Obrigado.

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

Como tinha sido anunciado inicialmente, nós vamos ter um segundo painel agora com três outros participantes.

O SR. SERGIO MORO (Bloco Parlamentar Democracia/UNIÃO - PR. *Fora do microfone*.) – Deixe só uma pergunta, Senador.

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

O SR. SERGIO MORO (Bloco Parlamentar Democracia/UNIÃO - PR. Para interpelar.) – Só para esclarecer a natureza: talvez se possa ter como referência uma das agências espanholas ou a Cisa americana.

Então, vamos colocar uma situação hipotética. Um ataque cibernético ao sistema financeiro brasileiro, a bancos, vários bancos, para roubar dados de correntistas. A atuação contra esse ataque caberia, no nível operacional, à agência ou isso já é *law enforcement*? Como funciona? Qual é a missão para a gente poder delimitar... Porque, é claro, a atividade regulatória é uma, a fiscalizatória é outra, mas, no nível operacional, na reação imediata a esse ataque, caberia a coordenação pela agência? Caberia também a investigação?

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Se me permite, só um detalhamento: se fosse só um banco e se fossem vários bancos.

O SR. SERGIO MORO (Bloco Parlamentar Democracia/UNIÃO - PR) – Perfeito.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Até para se saber sobre a solidariedade.

O SR. SANTIAGO PAZ (Para expor.) – Sim.

A responsabilidade final de cibersegurança é da organização dona dos dados. O banco é o responsável final pela sua defesa, mas o banco tem regulações setoriais, em que vai ter que ter alguma normativa.

Então, primeira linha de defesa, o próprio banco. Depois, depende do nível de maturidade dos países. No caso de Israel, por exemplo, eles têm, setorialmente, no setor financeiro, um centro de defesa para o setor financeiro e depois têm um nível nacional de defesa, e o nível nacional tem não somente o setor financeiro, mas tem todos os outros setores, então tem uma visão muito mais abrangente, em que eles podem ver se é o mesmo atacante que está atacando o setor financeiro e, ao mesmo tempo, a energia.

Então, como é a colaboração com a *law enforcement?* Habitualmente, o objetivo da *law enforcement* é procurar e processar o criminoso. Esse é o objetivo principal. Então, eles trabalham coordenados. Habitualmente, a primeira linha é a cibersegurança, e, uma vez que eles podem conter,

levando em conta os procedimentos para preservação das informações, entra a equipe da *law enforcement,* que faz toda a investigação para processar o atacante.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Acho que foi respondido.

Senador Marcos Pontes.

O SR. ASTRONAUTA MARCOS PONTES (Bloco Parlamentar Vanguarda/PL - SP. Para interpelar.) – Só uma curiosidade, uma pergunta, aproveitando o Google aqui. Realmente, é só um comentário com relação a isso.

Eu vejo essa dificuldade que talvez exista de uma organização governamental interferir com a parte privada, etc., o que pode ser um tanto complexo. Portanto, essa utilização como a de Israel, setorial, é interessante.

Mas só uma curiosidade. A respeito de inteligência artificial, lógico que isso evolui no dia a dia, e, como o Google está sempre trabalhando na fronteira desses desenvolvimentos, não sei se é possível falar sobre isso ou não, mas, por enquanto, hoje em dia, nós temos alguns grandes centros ou algumas grandes inteligências artificiais que trabalham com muitos dados – Gemini, ChatGPT e assim por diante –, mas são grandes e centralizados. O que eu quero dizer é que o sistema é centralizado. Então, se eu quero utilizar, eu tenho que utilizar uma conexão para entrar em contato com aquele ente e buscar as informações aqui. Ótimo.

Ideias de *federated learning*, por exemplo, em que os dados ficam no usuário e são transmitidas só as informações, me levam a crer que, eventualmente, esses sistemas vão se descentralizar, e eu imagino, por exemplo, a possibilidade de, assim como os nossos cérebros separados, pensando em separado, não conectados com um cérebro central, chegar a um certo momento em que a inteligência artificial vai estar contida em um dispositivo separado, um usuário separado, o que modifica o contexto como um todo, porque, por enquanto, a gente consegue regular. Se eu quiser desenvolver algum sistema, eu posso usar APIs para tentar conectar, buscar dados, mas eu estou usando um sistema central. De repente, se o sistema é isolado, tudo isso que a gente tem discutido sobre inteligência artificial, de repente, toma outro sentido, porque vai ficar muito mais difícil controlar uma situação como essa.

Existe algum desenvolvimento do Google nesse sentido, em se descentralizar a inteligência artificial? Só curiosidade, não sei se pode responder ou não.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Sem dar a pergunta por vencida, não sei se vocês assistiram, ontem, a uma descrição de um golpe que está sendo dado em alguns bancos no Brasil. O "eletricista", entre aspas, falso, que vai lá e altera o cabo de conexão, ou seja, com isso ele passa a manobrar, pelo menos, o arquivo daquela agência, os dados daquela agência. E, um dos bancos – não sei se foi o Banco do Brasil ou um outro que foi vítima – diz que gasta, por ano, na sua defesa – daquele banco, não dos bancos – R$9 bilhões.

O SR. ASTRONAUTA MARCOS PONTES (Bloco Parlamentar Vanguarda/PL - SP) – Essa é uma das...

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – E R$9 bilhões é o dobro do custo da agência daqui a cinco anos, se ela fosse criada. Aliás, o dobro não, são vinte vezes.

O SR. ASTRONAUTA MARCOS PONTES (Bloco Parlamentar Vanguarda/PL - SP) – É um dos tipos de ataques *man in the middle,* homem no meio, esse tipo de ataque cibernético.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Inclusive, um fato que ocorreu – chega a ser hilário – do falso eletricista querendo entrar no forro do banco, no teto, e o teto desmanchou em cima dele... Ele numa escada, e o teto desmanchou em cima dele. (*Risos.*)

O SR. ASTRONAUTA MARCOS PONTES (Bloco Parlamentar Vanguarda/PL - SP) – Tecnicamente, a gente chama isso de *spoofing* com *man in the middle*. (*Risos.*)

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Mas só para acrescentar, para fazer a individualização do que é o sistema bancário e do que é uma instituição bancária.

O SR. JORGE BLANCO (Para expor. *Tradução simultânea*.) – Sobre a sua pergunta mais relacionada à sua curiosidade, eu tenho que dizer que não sou um especialista em inteligência artificial; eu sou especialista em cibersegurança, mas eu posso responder. Isso não é algo que o Google está pensando, ou até os nossos competidores; isso é o presente. E nós temos visto essa centralização e descentralização desde o início da computação.

Então, lembrem do *mainframe*, depois os microcomputadores. Depois, tudo na inteligência artificial foi descentralizado alguns anos atrás. Mas agora temos que considerar que estamos treinando os modelos de forma centralizada e estamos disseminando os resultados até para o seu celular. Vocês estão executando: não só perguntando e fazendo perguntas a esse modelo centralizado, mas executando minimodelos de inteligência artificial no celular de vocês, no seu *smartwatch*. Isso está acontecendo agora e tem a ver com a pergunta sobre cibersegurança que você fez.

E a coordenação... O exemplo do setor financeiro ou de um banco, de um ataque a banco, depende, como foi mencionado antes, do tipo de ataque. Não é a mesma coisa se, em nível nacional, estamos falando sobre um ataque a um setor sistêmico. Todo o setor financeiro na Espanha recebe um ataque ao mesmo tempo, por exemplo; não dá para responder a esse ataque só com a lei. A lei investiga e tenta achar os atores do crime. Se só um banco for atacado, provavelmente a capacidade própria, com a ajuda da lei, consegue lidar com a situação, mas, se for um ataque sistêmico, precisamos da coordenação de uma entidade. Pode ser uma agência nacional ou como vocês quiserem chamar, mas coordenar não só com o setor financeiro, mas também com os agentes da lei, com as pessoas no Judiciário, os procuradores, tudo tem que ser coordenado da mesma forma.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Algum comentário adicional? Posso fazer, então, a conversão? (*Pausa.*)

Vou lhes pedir para abrir o espaço para os nossos próximos debatedores. Os senhores podem se instalar nas cadeiras. (*Pausa.*)

(*Intervenção fora do microfone.*)

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Não, vamos ver ainda. (*Fora do microfone.*)

Não estou mandando vocês embora, não; é só uma modificação de plateia. (*Pausa.*)

O Sr. Paulo Manzato e o Sr. Belisario Contreras são nossos convidados para tratar especialmente da segunda visada da nossa reunião.

Aqui, nós queremos conhecer especialmente...

Você tinha me mandado...

O SR. ASTRONAUTA MARCOS PONTES (Bloco Parlamentar Vanguarda/PL - SP. *Fora do microfone*.) – Eu já vi lá, já estou de acordo.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – O segundo tema que nos reúne é a importância da cooperação entre o poder público e o setor privado no combate aos crimes cibernéticos. De alguma forma, a questão foi abordada, com respostas que estimulam, mas que não esgotam o assunto, de forma que eu passo a palavra, inicialmente... (*Pausa.*)

Quem está *online*? (*Pausa.*)

Está *online*, também – estou sendo informado –, a Sra. Patricia Soler, Líder no Colaborativo Conjunto de Ciberdefesa da CISA (Agência Americana de Cibersegurança e Infraestrutura), por videoconferência.

Eu vou passar a palavra, inicialmente, à Sra. Patricia, dentro daquele princípio universal de *ladies first*.

A senhora tem dez minutos para fazer a sua manifestação, especialmente sobre este enfoque, ainda que o nosso tema seja mais abrangente.

A SRA. PATRICIA SOLER (Para expor. *Por videoconferência*. *Tradução simultânea*.) – Ótimo. Muito obrigada por me receberem.

Eu tenho alguns eslaides que vou compartilhar.

Vocês conseguem me ouvir? (*Pausa.*)

O.k.?

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – *We are understanding you and hearing you.*

[Tradução simultânea: Sim, te ouvimos e te entendemos.]

A SRA. PATRICIA SOLER (*Por videoconferência*. *Tradução simultânea*.) – Ótimo.

Vocês veem a minha tela, o PowerPoint? (*Pausa.*)

O.k.

Muito obrigada por me receberem, novamente. Eu sinto muito não poder estar presencialmente com vocês, mas obrigada pelo convite. Eu realmente gostei muito da conversa até agora, incluindo os ótimos comentários e ideias compartilhados na primeira sessão.

Eu vou falar hoje sobre parcerias público-privadas e o papel da CISA (Agência Americana de Cibersegurança e Infraestrutura) nos Estados Unidos.

Para falar um pouco sobre o que nós fazemos no Governo norte-americano – um palestrante anterior mencionou que temos muitas agências que têm autoridades de cibersegurança nos Estados Unidos –, o que nós fazemos que é diferente e qual é o nosso mandato, da perspectiva legislativa? Somos responsáveis pela infraestrutura crítica nos Estados Unidos e, recentemente, nos beneficiamos de um esclarecimento feito pela Casa Branca, em abril desse ano, especificando, em um memorando de segurança nacional sobre infraestrutura, segurança e resiliência críticas, que a Cisa lidera o Governo nesse assunto. Isso clarifica o nosso papel com as outras agências nos Estados Unidos.

Temos muitas legislações sobre cibersegurança, especialmente, porque precisamos acompanhar o que os atores de ameaça estão fazendo. Quanto a atores de ameaça, eu quero dizer tanto os criminosos quanto os Estados nacionais que os protegem, dentro de suas divisas. Então, não é só cibercrime, mas diferentes tipos de atividades que um governo estrangeiro pode estar fazendo contra a nossa infraestrutura.

Três diferentes itens que eu quero enfatizar, nesse memorando, é que a Cisa, agora, é o coordenador nacional para essa infraestrutura crítica de segurança e resiliência. Nós temos responsabilidade de coordenação e também temos responsabilidade de gestão de oito setores críticos de infraestrutura e um subsetor. Temos 16 setores de infraestrutura críticos nos Estados Unidos. Somos a agência que comanda oito deles e, agora, um subsetor.

Nós também apoiamos o trabalho feito por nossos parceiros em todo o Governo dos Estados Unidos. Esse trabalho não é novo. A Cisa tem pouco mais de cinco anos de idade, então somos relativamente novos, mas muitas das nossas autoridades e programas já existiam antes da criação da agência. Nós estamos sob o Departamento de Segurança Interna, e isso é relevante porque, no primeiro painel, falamos sobre como o modelo é diferente em cada país e como essa estruturação, para apoiar os espaços de missão de cibersegurança, é diferente.

Aqui, estamos sob o Departamento de Segurança Interna e trabalhamos, é claro, com o Departamento de Segurança Interna, mas também com o FBI, a NSA e outros. Tudo isso depende das nossas autoridades individuais dentro do Governo dos Estados Unidos. A Cisa, especificamente, é responsável por ciberdefesa. Nós somos civis, não somos agentes da lei e não fazemos parte do setor de inteligência ou de defesa.

Vai ficar diferente, em outros países, como eles vão querer estruturar... Também temos a responsabilidade CERT. A função de resposta de emergência está dentro da divisão da CISA e eu vou falar isso mais tarde, na minha apresentação.

Na direita da tela, vocês podem ver os nossos 16 setores de infraestrutura crítica. Eu peço perdão pelo tamanho, mas é para dar uma visualização de quais são os 16 setores e de como estamos posicionados como uma agência para identificar, avaliar atividade maliciosa de outros países ou de criminosos e melhorar a nossa compreensão desses riscos para a cibercomunidade mais ampla. Isso inclui nossos participantes internos e nossos parceiros internacionais. E, nesse caso, eu sou responsável por trabalhar com os nossos parceiros CERT, a função CERT que existe em outros países. Eu queria mencionar que é uma coisa comum do governo e, cada vez mais, é raro chegar a um país que não tem um CERT.

Trabalhamos com CERTs globo afora para o propósito de ciberdefesa. Nós recebemos informação acionável de organizações, no nosso país, para podermos proteger redes, dados e empregados de ciberataques maliciosos e de algo que nos incomoda a todos, que são os *ransomwares*.

Queremos trabalhar com o setor privado, com nossos outros parceiros de agência para fazer com que seja realmente difícil para cibercriminosos operarem. Queremos aumentar os custos deles e interromper suas operações. Não estamos do lado da ciberofensiva, mas temos que trabalhar como uma cibercomunidade, dependendo das autoridades e dos nossos papéis.

Outro pedaço de legislação que é relevante para a CISA, em termos de cibersegurança, é *cyber incidents,* de 2022. É a lei para a proteção de infraestrutura crítica. Ainda está sendo desenvolvida, mas requer que a CISA coordene, com nossos parceiros federais, o que são relatórios obrigatórios de incidentes. Daqui a pouco, vamos receber dados de entidades, geralmente de entidades de

infraestrutura crítica, que vão ter que relatar entre *cyber incidents* e *ransomware*. Isso não é o final, mas pode mudar.

Que identidades seriam necessárias... Tem a ver com entender o ambiente das ameaças. Muito dela é voluntária, e não temos uma imagem holística do que está acontecendo à infraestrutura crítica e com relatórios obrigatórios, mas o que é mais e mais comum com nossos parceiros internacionais é que vamos ter um melhor entendimento e entender riscos específicos para certos setores, o que está acontecendo no setor de água, no nuclear, e trabalhar nossos parceiros entre agências, nossos parceiros do setor público e a indústria privada.

Teve umas conversas mais cedo sobre a força de trabalho. Para a CISA, algo que eu queria indicar é que CISA não faz só cibersegurança. Também fazemos a segurança de infraestrutura. Então, metade do nosso trabalho tem a ver com cibersegurança. E a última informação pública disponível era que temos mais de 3 mil pessoas com a divisão de cibersegurança, tendo 1.150 empregados. Esses dados são de 2023, e só aumentamos o nosso pessoal. Eu não tenho o orçamento aqui nesse eslaide, mas a última informação pública disponível é que foi de US$3 bilhões.

Uma coisa que nos faz diferentes, dado o tamanho dos Estados Unidos e a diversidade geográfica, é que temos dez escritórios regionais. Muitos estão em Washington, mas temos empregados em todo o país nesse modelo regional com escritórios em cada região. E esses empregados são responsáveis por entender as necessidades daquela região e, talvez, as empresas de pequeno, médio ou grande porte naquele local com essas entidades. E, certamente, não podemos fazer tudo de Washington. Então, é importante para nós termos esse modelo regional, mas isso é devido ao tamanho do país. Nem todo país faz isso, mas é um exemplo de como isso pode funcionar num modelo nacional usando empregados que não estão somente em Washington. Parcerias público-privadas.

Uma coisa que eu mencionei: a CISA só tem cinco anos, e o nosso colaborativo de ciberdefesa, que é para trabalhar com o setor privado, tem três anos de idade, o que significa que trabalhamos com empresas privadas. Eu sei que o Google está aqui no auditório. Então, suas empresas têm seus QGs nos Estados Unidos e os gigantes da internet do mundo, e trabalhamos com eles numa base voluntária para entendermos, usar a telemetria deles de quais são as ciberameaças. Isso não é um modelo regulatório, isso é como podemos, em boa-fé, compartilhar ameaças ciber e entender o que está acontecendo com a infraestrutura e também com as nossas agências federais. E, se temos uma

informação que é mais relevante a um parceiro internacional, é a parte em que entro para compartilhar com a minha equipe e com as nossas contrapartes CERT.

Queremos ser proativos com o setor privado, mas sempre tentando alcançar as últimas ameaças. Como é que avaliamos o risco coletivo a que todos estamos sujeitos para não sempre estarmos atrasados? Temos parcerias entre agências e especificamente com o Departamento de Defesa, somos parte do DHS, Departamento de Justiça, NSA e FBI. Temos muito claramente colocado com quem trabalhamos, não são só essas agências, mas essas agências estão no lugar em que elas podem entender o tipo de informação técnica com que estamos lidando. Nem todos conseguem falar esse idioma, e aí tem um papel para traduzir os aspectos mais técnicos para os que fazem as políticas e de volta. É importante que os que fazem as políticas entendam o ambiente, mas necessariamente não serão especialistas. Como é que podemos facilitar essa conversa para entender se algo é importante ou não?

Coisas com as quais trabalhamos, com os nossos parceiros, eu vou pular um eslaide aqui. Trabalhamos com parceiros interagências e parceiros internacionais, em diretivos, aconselhamentos, alertas, e podemos dizer que melhoramos no Governo americano. Em vez de o FBI, CISA e NSA fazerem algo diferente em relação à ameaça, vamos colocar o nosso selo no mesmo produto e colaborar para trabalharmos juntos para produzir um guia que os nossos operadores possam usar. Estamos tentando muito falar com uma voz e não falar muito tecnicamente para assim termos uma diretriz de mitigação clara para as nossas partes interessadas. Pus uma planta de água no meio dos Estados Unidos, temos que ser capazes de alcançar essa audiência e também com as nossas contrapartes internacionais.

Eu falei sobre o que a JCDC faz, eu posso compartilhar esse eslaide. Eu sei que estou quase sem tempo, mas uma coisa que eu gostaria de mencionar é que isso é um esforço colaborativo e as nossas parcerias são críticas ao trabalho que fazemos, à função de coordenação, de nós termos autoridade legal para fazê-lo no local central. Nós valorizamos nossas parcerias externas com as indústrias, Estado local, tribal e nossos parceiros internacionais. Esperamos continuar o nosso trabalho com o Brasil e com outros países vizinhos nas Américas.

Muito obrigada por me ter e aguardo ansiosamente o resto da conversa.

Obrigada.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Quero agradecer à Sra. Patricia Soler.

Passo a palavra ao Sr. Paulo Manzato, chefe da área de setor público da Cloudflare.

O SR. PAULO MANZATO (Para expor.) – Boa tarde a todos.

Exmo. Sr. Senador Esperidião Amin, muito obrigado pela gentileza e pelo convite.

Demais Senadores, em especial o Exmo. Sr. Senador Sergio Moro, o tema de agora foi mencionado no painel anterior, mas acho que vale uma reflexão, que é a importância da cooperação entre o poder público e o setor privado.

A crescente ameaça dos crimes cibernéticos tem se tornado uma preocupação significativa para governos, empresas e indivíduos em todo o mundo. A complexidade e a sofisticação dos ataques cibernéticos exigem uma abordagem colaborativa para garantir uma defesa eficaz. A cooperação entre o poder público e o setor privado é essencial para enfrentar esses desafios de forma eficiente.

Os crimes cibernéticos, que incluem desde o roubo de dados pessoais até ataques de *ransomware*, espionagem digital, afetam não apenas a segurança nacional, mas também a estabilidade econômica e a privacidade individual. Os recursos e a *expertise* necessários para combater essas ameaças são vastos e diversificados, e nenhuma entidade isolada pode enfrentar esses desafios de maneira adequada.

O setor privado, com suas inovações tecnológicas e rápida adaptação às mudanças no mundo digital, como foi mencionado anteriormente, desempenha um papel crucial na identificação e mitigação das ameaças cibernéticas. Empresas de tecnologia, como provedores de serviços de internet, desenvolvedores de *softwares* de segurança e firmas de consultoria em cibersegurança, possuem conhecimentos especializados e recursos avançados que são vitais na detecção precoce de ataques e na implementação de medidas preventivas.

Por outro lado, o setor público possui a autoridade legal e os recursos necessários para coordenar esforços em uma escala nacional e internacional. Agências governamentais podem promulgar leis e regulamentos que incentivem práticas de segurança cibernética robustas, além de facilitar a troca de informações entre diferentes setores. Além disso, as forças de segurança e as

agências de inteligência possuem a capacidade de conduzir investigações criminais e desmantelar redes de criminosos; neste caso, cibercriminosos.

A colaboração entre esses dois setores permite a criação de um ecossistema de segurança resiliente. Programas de parceria público-privada, como a partilha de informações sobre as ameaças em tempo real e a realização de treinamentos conjuntos, podem melhorar significativamente a capacidade de resposta a incidentes. Além disso, iniciativas conjuntas podem promover a conscientização sobre cibersegurança entre o público em geral e as pequenas empresas, que são muitas vezes alvos fáceis dos atacantes.

Foi uma coincidência, mas, sinceramente, uma felicidade a Cloudflare falar depois da CISA. A Cloudflare, por exemplo, ao trabalhar com a CISA – é um parceiro nosso –, fornece os serviços de DNS autoritativo e registros para os domínios "*dot* gov": os .gov.

Não vou entrar em detalhes técnicos, mas gostaria muito, depois, de ter a possibilidade de explicar como a Cloudflare estabeleceu essa parceria, que é pública. Essa parceria exemplifica como a colaboração entre setor público e privado pode fortalecer a infraestrutura digital de uma inteira nação: vocês podem imaginar que todos os domínios "*dot* gov" dos Estados Unidos são protegidos pela Cloudflare.

Através dessa parceria, é possível reduzir a superfície de ataques e automatizar a segurança de DNS, protegendo informações sensíveis e garantindo a confiança nas comunicações governamentais. A cooperação também permite a criação de padrões e protocolos de segurança unificados, que podem ser adotados em diferentes setores – novamente uma abordagem talvez setorial.

Isso assegura que as melhores práticas de segurança sejam seguidas amplamente, aumentando a resiliência contra ataques cibernéticos em escala global. Além disso, a parceria facilita a criação de centros de resposta a incidentes cibernéticos – no nosso caso – ou de infraestrutura crítica, onde especialistas de ambos os setores podem trabalhar juntos para responder rapidamente às ameaças emergentes.

Um comentário apenas aqui: vários elementos que eu acabei de citar são acelerados, não quero voltar ao item anterior, mas são acelerados através de uma entidade que coordena isso, chamada agência ou outro nome.

A cooperação também permite a criação de padrões e protocolos de segurança unificados. Não há outra maneira de criar esses protocolos se não tiver uma agência coordenando isso.

Eu vou passar aqui. Encaminho-me para algumas conclusões.

Um outro aspecto importante da colaboração é o compartilhamento de inteligência das ameaças cibernéticas; como realizar esse compartilhamento e essa coordenação, sem uma entidade legal, é um ponto a se debater.

O setor privado pode fornecer informações valiosas sobre as ameaças e vulnerabilidades descobertas em suas operações diárias. É assim que, de fato, acontece na nossa parceria com a CISA, enquanto o Governo pode compartilhar dados de suas investigações e suas redes de inteligência. Esse intercâmbio é fundamental e crucial para antecipar e neutralizar ataques antes que causem danos significativos.

Um último ponto é a educação e a capacitação, também como áreas de cooperação entre o poder público e o setor privado. São áreas em que a cooperação tem um impacto significativo. Programas de formação desenvolvidos conjuntamente podem equipar tanto os funcionários do setor público quanto os do privado, com habilidades e conhecimentos necessários para enfrentar os desafios cibernéticos. *Workshops*, seminários e cursos de cibersegurança podem ser realizados para disseminar as melhores práticas e mais recentes inovações de ciberdefesa.

O nível e a disparidade da maturidade em cibersegurança, tanto no setor público, quanto no privado, são muito grandes. Eu tenho a sorte de conversar com setores com um nível de maturidade excepcional, todos aqui brasileiros, como de conversar com entidades governamentais com um baixo nível de maturidade. As pequenas empresas e médias claramente não estão equipadas com as mesmas ferramentas e conhecimentos para combater as ameaças cibernéticas. Isso também é verdade no setor público, como eu acabei de fazer referência, reforçando a necessidade de uma coordenação público-privada.

Em conclusão, a cooperação entre o setor público e o privado é fundamental para enfrentar a crescente ameaça dos crimes cibernéticos. Somente através de um esforço coordenado e colaborativo, podemos garantir um ambiente digital seguro e protegido para todos. A integração de recursos, conhecimento e capacidade de ambos os setores cria uma defesa mais robusta, adaptável contra as ameaças cibernéticas em constante evolução.

Muito obrigado pela palavra.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Obrigado ao Dr. Paulo Manzato. (*Fora do microfone.*)

Concedo a palavra ao Sr. Belisario Contreras, da Venable.

O SR. BELISARIO CONTRERAS (Para expor.) – Muito prazer, Senador Esperidião Amin, Presidente da Subcomissão Permanente de Defesa Cibernética, Senador Sergio Moro, distinguidos colegas brasileiros, é uma honra para mim estar aqui hoje.

Meu portunhol não é o melhor. Eu vou falar em inglês, mas, se eu ler, tomei a caipirinha e o rodízio, então é melhor um pouco. (*Risos.*)

Sempre falam isso.

Mas é muita honra. Há quase 20 anos, estive pela primeira vez em Brasília, numa missão oficial da OEA. Meu primeiro chefe, Rômulo Dantas, era oficial da Abin, estava designado pela OEA. Ele transmitiu para mim muito amor, carinho pelo Brasil, mas a mensagem é do prazer de estar aqui. Há 20 anos ou mais, estamos trabalhando o tema de segurança cibernética no Brasil. Então, é importante um chamado de atenção para vocês.

Agora eu vou trocar para o inglês.

O SR. BELISARIO CONTRERAS (*Tradução simultânea.*) – Agora eu vou trocar para o inglês.

Primeiro, boa tarde, honrados assessores e distintos convidados. É uma honra conversar com vocês sobre um assunto tão importante, a cibersegurança. Na era digital, a nossa dependência da tecnologia vem crescendo, e isso traz oportunidades, mas também risco. E estamos em uma encruzilhada de progresso e temos que tomar ações para salvar o nosso futuro digital.

Hoje eu estou com os meus distintos colegas para discutir o risco internacional de cibersegurança e suas implicações para o Brasil, a importância e os benefícios de estabelecer uma agência nacional de segurança digital e as lições aprendidas de outras nações, como os Estados Unidos, que já navegaram por esses desafios com sucesso.

A paisagem de ameaças globais está aumentando. As ciberameaças não são mais incidentes isolados; elas se tornaram um grande desafio que afeta todas as nações. A pandemia acelerou a adoção de novas tecnologias, mas essa integração rápida também expôs muitas vulnerabilidades.

Para o Brasil, as implicações são profundas. O país é um dos principais alvos de ciberataques e é responsável por 42% de todos os incidentes na América Latina na primeira metade de 2023. Com os nossos 328 mil ataques testemunhados, estamos testemunhando um ataque generalizado em nossa infraestrutura. O Brasil é a quarta maior economia do mundo e o uso de *smartphones,* muito disseminado aqui, torna a nação especialmente vulnerável.

De acordo com a Forbes, essa situação é mais exacerbada pelo fato de que é o segundo país mais suscetível globalmente aos ciberataques, apenas atrás dos Estados Unidos. O impacto financeiro desses ataques é muito alto. De acordo com os especialistas, o mercado de cibersegurança no Brasil foi avaliado em 8,3 bilhões em 2023 e vai chegar a 20 bilhões em 2028.

Eu quero enfatizar que cibercrime é um negócio muito bom. Um grupo estimou que os danos causados por todas as formas de cibercrime, incluindo o custo de recuperação, totalizaram 3 trilhões em 2015, 6 trilhões em 2021 e chegarão a 10,3 trilhões anuais até 2025. O Brasil, o México e a Colômbia, que são responsáveis por quase 80% dos ataques cibernéticos na região, têm muito desse fardo.

A maioria desses ataques são *malwares*, vazamento de dados, e isso enfatiza a necessidade de uma abordagem unificada. A segurança não é só uma questão de segurança corporativa ou individual, mas uma responsabilidade coletiva que exige unidade e colaboração. A falta de educação do usuário e a configuração errada das tecnologias deixaram lacunas significativas que os criminosos ficam cada vez mais capazes de explorar.

A abordagem no Brasil é fragmentada e as responsabilidades são de diversas agências. Esse sistema desagregado cria confusão e impede a nossa habilidade de responder às ciberameaças de forma eficiente. Nós precisamos de uma entidade centralizada para dar uma direção. O estabelecimento de uma agência nacional de segurança digital é um passo muito necessário. Essa agência vai centralizar recursos e acelerar a execução da estratégia nacional de cibersegurança, além da coordenação e supervisão, para garantir que os esforços sejam unificados e eficientes.

Os benefícios estão claros. Uma agência nacional de segurança digital dá resiliência ao país contra ciberameaças, definindo papéis e responsabilidades de forma mais clara e facilitando a melhor coordenação entre as entidades governamentais, o setor privado e os parceiros internacionais, como minha colega da CISA mencionou.

Essa agência também liderará iniciativas de educação e promoverá carreiras, construindo um *pipeline* de talento bem robusto. Além disso, uma agência nacional de segurança digital seria elevada ao mais alto nível de governo, fornecendo a direção necessária para coordenar ações e monitorar a implementação da estratégia nacional. Ela agiria como uma autoridade competente para definir, esclarecer papéis, responsabilidades, processos e atividades necessárias para implementar a estratégia e outras ações relacionadas à ciber-resiliência.

A agência também identificaria *stakeholders*, estabeleceria alvos de *performance* e criaria planos de ação para cumprir com os objetivos de cibersegurança do país. Além disso, uma agência coordenaria a colaboração intergovernamental em ciberiniciativas, garantindo que todos os esforços sejam alinhados e mutuamente reforçados. Isso inclui trabalho com parceiros internacionais para compartilhar práticas, melhorar o compartilhamento de informações e fortalecer nossas capacidades de ciberdefesa.

Recentemente, o Chile adotou uma legislação para estabelecer uma agência de cibersegurança nacional. Com mais liderança na região, o Brasil não pode ser a exceção. Como eu sempre digo, o Brasil é o maior país do mundo.

Temos que demonstrar liderança em cibersegurança e dar o exemplo para que os outros sigam. Podemos aprender lições valiosas de exemplos internacionais. Nos Estados Unidos, a agência CISA e o Escritório do Diretor Nacional de Cibersegurança têm papéis-chave na cibersegurança e na proteção de infraestruturas.

A CISA lidera os esforços federais de cibersegurança segurança e coordena a infraestrutura e a resiliência dos Estados Unidos. O escritório prevê uma estratégia para garantir que a cibersegurança continue uma prioridade. Além disso, temos o centro de cibersegurança do Reino Unido, que oferece um ponto de contato com partes interessadas, trabalhando diretamente com a lei e com parceiros internacionais. O Centro Nacional de Cibersegurança do Reino Unido traz especialistas de diferentes

agências para fornecer uma abordagem à cibersegurança abrangente. E esses exemplos enfatizam a importância de uma autoridade centralizada na gestão dos esforços de cibersegurança.

Podemos construir um ambiente mais resiliente no Brasil aprendendo com esses modelos bem-sucedidos. Uma agência centralizada acelera os esforços, melhora a coordenação e a cooperação entre diferentes partes interessadas, garantindo uma resposta mais eficiente às ameaças cibernéticas.

Eu geralmente espero que Senadores não discutam se é necessário, porque isso deveria estar claro, mas como estabelecer uma agência nacional de segurança digital. Essa agência não é só uma adição burocrática, é uma evolução necessária na nossa abordagem para garantir o futuro digital do Brasil. Nós precisamos agir o mais rapidamente possível para criar essa agência, definir seu mandato e alocar os recursos necessários para garantir seu sucesso.

Para iniciar esse processo, eu insto vocês a buscar apoio legislativo, alinhar a estrutura da agência e coordená-la com as entidades existentes. Nosso compromisso tem que ser firme e nós demonstramos isso através de ações concretas. Além disso, temos que investir em educação sobre cibersegurança e programas de conscientização para garantir que os cidadãos, negócios e agências governamentais estejam bem equipados para lidar com as ameaças cibernéticas. Isso inclui promover pesquisa em cibersegurança, desenvolver carreiras sobre cibersegurança e fomentar a conscientização sobre cibersegurança em todos os níveis da sociedade.

Para concluir, a segurança de uma infraestrutura digital é uma questão de segurança nacional. Estamos em uma encruzilhada em que ações decisivas são necessárias para proteger cidadãos, negócios e governos de ciberameaças.

Estabelecer uma agência nacional de segurança digital pode criar um ambiente digital mais seguro e resiliente para o país. Os desafios que enfrentamos são significativos, mas eles não são intransponíveis. Com a abordagem correta e o esforço unido, podemos construir uma estrutura de cibersegurança que garanta o nosso futuro digital.

Obrigado pela sua atenção e apoio.

Estamos animados para trabalhar com vocês, moldando essa agência.

Juntos, podemos construir um Brasil mais forte e mais seguro.

Obrigado.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Nos anos 70, *together we stand, divided we fall.*

Chegou a cantar esse rock?

O SR. BELISARIO CONTRERAS – Não, era muito mais jovem. (*Risos.*)

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – De 1973. Pode procurar no Google *together we stand, divided we fall*.

O SR. BELISARIO CONTRERAS (*Tradução simultânea.*) – E devemos trabalhar juntos assim como os criminosos.

Obrigado, Senador.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Eu quero agradecer a todos e, antes de compartilhar as perguntas, especialmente com o Senador, eu vou mencionar aqui as perguntas feitas pelo e-Cidadania. E me permito dizer quais as que eu considero já respondidas.

Luan, de Santa Catarina: "Quais as principais ferramentas a serem instituídas pelo Brasil para garantir a segurança [e soberania] cibernética [...]?".

Acho que esse é o nó, esse é o fulcro. Nós não temos a resposta definitiva, mas há uma tendência para termos uma agência reguladora e várias formas de parceria a definir. É a resposta que eu posso dar agora.

Gostaria de saber se o Santiago Paz está disponível, porque a segunda pergunta é para ele. (*Pausa.*)

Avisa a ele que eu tenho uma pergunta do Gilson, de São Paulo, para ele rerratificar.

Igor, do Distrito Federal: "Quais são as principais estratégias propostas no Plano de Trabalho da Política Nacional de Cibersegurança?".

Estamos desenhando e teremos um resultado até o final deste ano. Naturalmente, pode ser que tenhamos outras reuniões, tipo audiência pública, mas, em função de algumas missões que nós

pretendemos cumprir, certamente o assunto vai evoluir bastante em nível de proposição do Senado. Quanto às ações do Executivo, eu espero que sejam convergentes e, para isso, temos contado com essa interlocução.

Leonardo, do Rio de Janeiro: "Como será feita a integração entre o [...] [Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, que é um suposto], o Centro Integrado de Cibersegurança e o Comando de Defesa Cibernética para gestão do ciberespaço?".

Essa pergunta eu vou endereçar ao Senador Marcos Pontes.

Ney, do Acre: "Qual é o principal desafio enfrentado pelo Brasil em termos de cibersegurança atualmente?".

Não do Brasil, mas do mundo nós tivemos aqui uma resenha muito interessante, inclusive com a participação da Sra. Patricia Soler, que trouxe... Eu peço desculpas se eu não estiver pronunciando o nome corretamente. Aqui a gente diz "Solér"; pode ser que seja "Sóler". A dúvida de minha parte continua. Mas o mundo está procurando formas de enfrentamento a esses incidentes.

Sheyla, do Ceará: "Será criada uma equipe de resposta a incidentes cibernéticos que possa atuar rapidamente em casos de ataques cibernéticos?".

É o desejável, mas eu não tenho dúvida de que vai depender muito não apenas da nossa formação de recursos humanos, mas da organização e da cooperação entre iniciativa privada e poder público. Esta última é crucial.

Renan, de Goiás: "Haverá certificações para fomento aos [...] [Grupos de Resposta a Incidentes de Segurança Cibernética] e *compliance* de ambientes públicos ou para prestarem serviços para empresas públicas?".

Acho que é uma resposta correlata à última.

Márcio, da Bahia: "Quais as garantias de que a agência não será utilizada para fins políticos? Quais as punições para os casos de utilização indevida [...]?".

Sem dúvida, esse será sempre um ponto nevrálgico, mas nós já temos experiência legislativa suficiente para tomar as cautelas legais; e, em matéria de legislação de punição, nós já temos: isso se enquadra perfeitamente como crime na administração pública.

Maria, de São Paulo: "A criação de uma Agência Nacional de Segurança Digital não [...] [aumenta] [...] os custos para o Estado? Por que não utilizar a [...] [Agência Nacional de Proteção de Dados]?".

Este foi o debate que nós travamos também aqui: criar ou não. Há quem defenda; não existe uma conclusão ainda, mas existe uma tendência. A audiência de hoje traz uma tendência de criar uma agência reguladora própria, sem perder a coordenação, cooperação e solidariedade com a iniciativa privada.

O Santiago Paz onde está? (*Pausa.*)

Aeroporto.

Tem que ser enviado para ele o seguinte – Gilson, de São Paulo –: "[...] como o [...] [Banco Interamericano de Desenvolvimento] pode apoiar o Brasil na criação e no fortalecimento de sua infraestrutura de segurança cibernética?".

Ele mencionou. Se estão recordados, ele mencionou: o quarto item é o financiamento, mas são três formas de cooperação que existem, e a quarta, mencionada por ele, é a possibilidade de financiamento. Isso é para dar uma satisfação, ainda que muito rápida e expedita, aos que nos acionaram pelo e-Cidadania.

Consulto o Senador Sergio Moro sobre se ele tem alguma indagação a fazer aos nossos debatedores: Patricia Soler, Paulo Manzato e Belisario Contreras.

O SR. SERGIO MORO (Bloco Parlamentar Democracia/UNIÃO - PR. Para interpelar.) – Primeiro, gostaria de congratular os expositores, Sr. Belisario, Sr. Paulo, Sra. Patricia, pela exposição. Eu achei bastante interessante a referência que foi feita sobre *mandatory reporting* de incidentes de ataques cibernéticos, inclusive pelo que eu entendi ali sobre regulação no âmbito da CISA.

E, já que essa legislação de criação da agência teria que vir pela legislação brasileira, de iniciativa do Executivo federal, sem prejuízo de depois nos debruçarmos sobre esse texto, uma sugestão que faria – até porque existem membros do Executivo aqui presentes – é que já fosse analisada essa colocação de uma obrigação legal de que empresas, setor público e setor privado, façam comunicados, *reporting*, como diz a lei, de incidentes de ataques cibernéticos, pelo menos em algumas circunstâncias.

A minha dúvida, e aí posso indagar a todos, é se *mandatory reporting* abrange a informação quanto ao ataque, mas também quanto à solução, se uma solução for encontrada. E, nesse último caso, se não existe, eventualmente, pelo menos para o setor privado, para as empresas, algum obstáculo no que se refere a direitos intelectuais, de proteção intelectual da solução encontrada para os ataques.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Eu vou endereçar a pergunta do Senador Sergio Moro à Sra. Patricia "sóler" ou Soler, que ainda está, pelo que me informam, *online*, para que ela, por favor...

A SRA. PATRICIA SOLER (*Por videoconferência*. *Tradução simultânea*.) – Sim, estou aqui.

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

A SRA. PATRICIA SOLER (Para expor. *Por videoconferência*. *Tradução simultânea*.) – Em relação a reportar ataques, há diferentes modelos de diferentes países. Tem o modelo americano, que estamos colocando, que ainda não está finalizado. Há outros países que já o têm completo, têm o mecanismo de fazer valer, também, e a obrigação – se são penalidades financeiras, se vão relatar, se são criminais... Então, realmente depende do país e da relação com o setor privado.

Eu diria que a recomendação é olhar várias formas diferentes de relatórios obrigatórios. Quanto tempo a empresa tem para relatar? Em alguns países, elas têm que ligar para o Governo em até quatro horas e têm 72 horas para dar um relatório escrito. A ideia é que a gente quer que eles respondam ao incidente. Vai parecer diferente em diferentes países – quanto tempo, quanta informação... –, e a nossa lei ainda não está finalizada nos Estados Unidos.

Em termos de propriedade intelectual, ela é protegida pela nossa legislação. Então, algumas das autoridades que criaram isso em 2015, empresas e outras entidades, podem compartilhar informação para motivos de ciberdefesa. Não nos importamos com como eles chegaram a um certo resultado, com qual *software*; é mais nos resultados em que estamos interessados, e não no *software* único que os permitiu derivar algum resultado.

Nas nossas páginas, temos uma página para advogados. Isso é algo que eu recomendo para qualquer ciberentidade em qualquer país. Inevitavelmente, outras agências federais, o público, o setor

privado vão querer saber quais são as proteções que estão no local e, tendo isso no *website*, eles podem investigar e fazer suas perguntas.

Obrigada.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Consulto o Senador Sergio Moro se tem alguma consideração a fazer. (*Fora do microfone.*) Considera satisfatória?

O SR. SERGIO MORO (Bloco Parlamentar Democracia/UNIÃO - PR) – Muito obrigado.

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

O senhor tem alguma indagação a fazer aos nossos Belisario Contreras e Paulo Manzato?

O SR. SERGIO MORO (Bloco Parlamentar Democracia/UNIÃO - PR. Para interpelar.) – Acho que vale aquela pergunta sobre o que as suas respectivas entidades e instituições poderiam fazer, eventualmente, para ajudar o Brasil na criação de uma agência nacional, como uma pergunta final, mas também deixo a V. Exa., querendo...

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

O SR. PAULO MANZATO (Para expor.) – Bom, com relação a essa última pergunta, eu tenho alguns eslaides, mas eu não queria colocá-los aqui, porque talvez com tempo que eu... A Cloudflare tem como missão, como um *statement* nosso, ajudar a construir uma melhor internet. E essa palavra ajudar é uma palavra absolutamente importante, porque ela fala de cooperação. Nenhuma empresa pública e privada pode guerrear nessa guerra sozinha. É assim que a Cloudflare tem feito com a iniciativa privada e com o poder público.

Ela fez acordos com... A gente acabou citando aqui várias agências, mas todas elas, com exceção da de Israel, têm *partnership* com a Cloudflare, a CISA e a correspondente em UK, para fazer a proteção do DNS autoritativo. Acordos de cooperação de inteligência, de troca, baixo memorando de *understanding*, mas a Cloudflare é uma empresa absolutamente transparente, sem revelar informações de propriedade intelectual, mas, todas as vezes que ela encontra uma vulnerabilidade, isso é criado, registrado, os famosos CSEs, e reportado como se chegou ao resultado, mais ou menos como a Patricia Soler acabou de dizer. A gente está preocupado no como, na resolução.

A Cloudflare tem total interesse de participar e discutir uma criação de uma agência nacional de cibersegurança, mas o que eu gostaria de dizer é que, por exemplo, a Cloudflare, para o Brasil, não é alguma coisa nova...

(*Soa a campainha.*)

O SR. PAULO MANZATO – Só para complementar. Há três anos, foi criado o GovShield, que é um programa do Serpro. E o GovShield, é público isso, é um produto Cloudflare e está disponível para todos os municípios e estados fazerem adesão a ele. Então, a cooperação da Cloudflare com o Governo brasileiro não é recente. Talvez, não seja um nome tão conhecido como o Google, mas a Cloudflare, em cibersegurança, é uma empresa super-respeitada. Além de ter outros projetos na área de eleições, iniciativas públicas...

Então, respondendo à sua pergunta, Senador, a Cloudflare pode contribuir com tecnologia, com inteligência e no modelamento da agência.

Obrigado.

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

Sr. Belisario.

O SR. BELISARIO CONTRERAS (Para expor. *Tradução simultânea.*) – Muito obrigado.

Um dos meus papéis era o de coordenador da aliança. E um dos propósitos era crescer a segurança ciber e digital na região. Agora, temos mais ou menos 20 membros e muitas organizações que cá estão, Google, Cloudflare, Apple e outras, muitas outras; ambos, Estados Unidos, América Latina, com CISA, Alumo, e europeias, como Telefônica ou Santander.

O que podemos oferecer é colocar *expertise* e habilidade de todas as empresas multinacionais, e os interesses que eles têm em apoiar vocês, o Legislativo e o Governo. Temos feito esses engajamentos em outros países. Por exemplo, com a Colômbia fizemos um engajamento próximo com o Legislativo e o Executivo, organizando uma mesa redonda no palácio presidencial para discutir o que é necessário para avançar nisso. Na Colômbia, eles estão em um processo similar, não só com uma lei, mas com dois projetos de lei para criar... Propomos isso ao Brasil, esperamos fazer isso em breve, e, novamente, estamos prontos para trabalhar com vocês, para conectar vocês com todas as

organizações, e não por motivos nossos, mas para garantir que vocês tenham os *insights*. Tem dezenas de programas de educação, pesquisa, recursos que estão disponíveis para vocês a nenhum custo.

(*Soa a campainha.*)

O SR. BELISARIO CONTRERAS (*Tradução simultânea.*) – Podemos oferecer muitas coisas para o Governo, para o Legislativo, até para o povo, que, no fundo, são os que vocês querem proteger.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Agradeço a todos os participantes (*Fora do microfone.*) e indago se alguém gostaria de acrescentar alguma coisa.

Agradeço especialmente a participação dos companheiros, colegas Senadores, aqui na pessoa do Senador Sergio Moro, pelas suas inestimáveis colaborações.

Agradeço muito aos representantes do GSI, que, com a sua presença, preservaram esse espírito de cooperação que existe entre o Parlamento, especialmente o Senado, e o GSI, na busca dessa formulação da maneira menos surpreendente possível, e, sim, da maneira mais cooperativa possível.

Agradeço muito à equipe da Comissão de Relações Exteriores e Defesa Nacional. Agradeço ao Presidente da Comissão, o Senador Renan Calheiros. Sem essa colaboração, esta reunião seria impossível. Agradeço ao pessoal do nosso gabinete, que deu a infraestrutura e nos ajudou aqui a conduzir esta reunião. São quase três horas de reunião, com muitas informações interessantes e absolutamente proveitosas e úteis para essa tarefa de fazermos uma avaliação da política nacional de defesa cibernética e dar os próximos passos que nos levarão à apresentação de um relatório até o fim deste ano.

Agradeço finalmente aos palestrantes, ao Santiago Paz; à Sra. Patricia Soler – agora, eu vou alterar para completar a possibilidade de entonação do seu sobrenome –; ao Rafael Gonçalves; ao Paulo Manzato; ao Belisario Contreras; e o Sr. Jorge Blanco. Acho que foram esses os nossos participantes, indispensáveis à realização desta reunião.

Com isso, declaro encerrada a reunião e, eventualmente, teremos convocação de nova reunião, a ser proximamente divulgada.

Muito obrigado. (*Palmas.*)

(*Iniciada às 14 horas e 15 minutos, a reunião é encerrada às 16 horas e 52 minutos.*)