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

REUNIÃO
18/05/2023 - 16ª - Comissão de Serviços de Infraestrutura

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB. Fala da Presidência.) - Minhas senhoras, meus senhores, os nossos cumprimentos.

Sejam todos muito bem-vindos e bem-vindas a esta audiência pública aqui no plenário da Comissão de Infraestrutura para tratarmos sobre um assunto premente que requer de todos nós da sociedade brasileira, das organizações, das entidades e dos Poderes as atenções devidas ao tema.

Eu agradeço a presença dos senhores convidados que se permitiram aqui estar para colaborar com este debate a fim de que nós nos aprofundemos sobre uma realidade que está entre nós presente, mas a que, a meu ver, a mim me parece, ainda não foi dada a devida dimensão pessoal pelo próprio Governo, pelas suas instituições e pela sociedade, ou seja, o sentimento é o de que estamos aguardando um infausto, um episódio de maior gravidade para que tenhamos a devida noção e dimensionemos os riscos que já nos rodeiam, que é exatamente o de estarmos submetidos aos avanços de ataques cibernéticos, de ataques aos sistemas de segurança de dados pessoais e institucionais, como já observamos. Foi essa a razão que, durante esses últimos dois, três meses, fez-nos preocupar e poder produzir, a partir desta audiência e também através de propostas legislativas, este debate que, por absoluta convicção, haverá de ser profícuo ao Parlamento e ao país.

Havendo número regimental, nós declaramos aberta a 16ª Reunião da Comissão de Serviços de Infraestrutura da 1ª Sessão Legislativa Ordinária da 57º Legislatura, que se realiza nesta data, 18 de maio de 2023.

Esta reunião destina-se à realização de audiência pública com o objetivo de debatermos a implementação de estratégias de prontidão cibernética e proteção preventiva dos bancos de dados governamentais contra eventuais ataques de *hackers*, em atenção ao Requerimento, de nossa autoria, nº 11, deste ano, que foi direcionado a esta Comissão.

Nós já temos a presença do Sr. José Luiz Medeiros, representante da Associação Brasileira de Governança Pública de Dados Pessoais. Quero desde já agradecê-lo pela atenção e por disponibilizar o seu tempo para que possa expor as suas compreensões em nome da Associação Brasileira de Governança.

Quero agradecer a presença do meu estimado amigo, com quem tive a oportunidade de estabelecer uma relação mais próxima nesses últimos meses, Dr. Fabrício da Mota, Conselheiro Titular do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

Quero cumprimentar o Sr. Luiz Fernando Moraes da Silva, Secretário de Segurança da Informação e Cibernética do Gabinete de Segurança Institucional da Presidência da República. É fundamental a sua presença. E, desde já, igualmente agradeço a disponibilização do seu tempo, pois, afinal de contas, está envolvido diretamente com todas essas preocupações.

Quero agradecer também ao Sr. Carlos Renato Araújo Braga, Diretor de Avaliação de Segurança da Informação da Unidade de Auditoria Especializada em Tecnologia da Informação do Tribunal de Contas da União. Dr. Carlos, seja bem-vindo. Eu, inclusive, me vali de um relatório, denso relatório, que foi produzido pelo Tribunal de Contas trazendo os precisos alertas a essa realidade que nos circunda. Eu agradeço ao Tribunal de Contas e agradeço pela sua presença, que muito nos honra.

Agradeço ao Sr. Arthur Pereira Sabbat, Diretor da Autoridade Nacional de Proteção de Dados; ao querido Prof. Humberto Ribeiro, Professor do Centro de Prevenção de Incidentes Cibernéticos, que tem nos munido de muitas informações e nos trazido, dia a dia, aquilo que está a nos cercar; e, por último, ao Sr. Leonardo Ferreira, Diretor do Departamento de Privacidade e Segurança da Informação do Ministério da Gestão e da Inovação em Serviços Públicos.

Antes de passar a palavra aos senhores convidados, comunicamos que esta reunião será interativa, transmitida ao vivo e aberta à participação dos interessados pelo Portal e-Cidadania, na nossa internet - o endereço, os senhores bem sabem, é senado.leg.br/ecidadania -, ou pelo telefone 0800 0612211.

Um relatório completo, com todas as manifestações, estará disponível no nosso portal, assim como as apresentações que forem utilizadas pelos senhores expositores.

Nós temos, até porque, de fato, entendíamos e entendemos que a presença de cada um dos senhores a representar as entidades...

Antes, quero saudar aqui a presença do nosso estimado Senador Prof. Esperidião Amin. Seja bem-vindo, meu Senador. Muito nos enobrece e nos enriquece a sua presença...

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - ... pela relevância da sua Presidência e pela relevância...

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - ... da sua presença!

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - ... do tema. *(Risos.)*

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Seja bem-vindo, meu querido e estimado amigo.

É evidente que, em uma audiência pública com sete expositores, nós temos que dar uma dinâmica, claro, não perdendo, para quem se permite, para quem se dispõe, abrindo as suas agendas e oferecendo-se a vir ao Senado e atender ao convite desta Comissão de Infraestrutura... Não seria, absolutamente, elegante de nossa parte diminuirmos ou limitarmos as exposições às perdas, na qualificação que cada um dos senhores expositores tem e que o tema permite, mas também não podemos nos delongar, afinal, também haveremos de cumprir, daqui a pouco, às 11h, o início das nossas atividades em Plenário. Portanto, a Presidência gostaria - penso se os senhores assim entenderem como o mais pertinente - de reservar dez minutos a cada um dos expositores para fazermos uma dinâmica, uma reunião em que possamos interagir em um debate que haverá de ser profícuo.

Definido o tempo de dez minutos para cada expositor, gostaria de passar a palavra ao Sr. Prof. Humberto Ribeiro, que terá eslaides a apresentar, municiando-nos para este início de debate.

Prof. Humberto, por gentileza. São dez minutos, que eu peço aos meus companheiros da Secretaria para... Obrigado.

O SR. HUMBERTO RIBEIRO (Para expor.) - Exmo. Sr. Senador Veneziano Vital do Rêgo, no momento em que saudamos o Senador Veneziano, saudamos todo o Senado Federal e também as autoridades presentes e os componentes da mesa. Quero saudar esta realização.

E, como diz o velho ditado, Senador, mais uma vez, esperamos que a sabedoria popular se faça presente também na frase de "prevenir é melhor do que remediar". Nós temos enfrentado, no âmbito nacional e internacional, um contexto de remediações severas do mundo digital. E elas comprometem aquilo com que eu faço uma correlação com o oxigênio para um organismo: a informação para as instituições e para o convívio social, hoje em dia. A disrupção de um sistema de um ambiente digital promove uma série de complicações na nossa sociedade. Então, o enfrentamento - aqui como egresso da Universidade de Brasília, Faculdade de Tecnologia, como pessoa que convive no setor de tecnologia há mais de 30 anos - se dá pelo modo preventivo.

E daí o conceito que vem se difundindo globalmente, que é o de prontidão cibernética. É um conceito complementar, acessório ao conceito de segurança da informação, que é um guarda-chuva mais amplo.

Preparei alguns eslaides, Senador. Serei célere. Obviamente, num momento adequado, dado o respeito ao tempo, conforme definido, não serei exaustivo em cada um dos eslaides, para que a gente possa respeitar os dez minutos.

Eu cliquei, mas não... *(Pausa.)*

Obrigado.

Como dito, a infraestrutura digital é hoje um indutor de prosperidade para a humanidade. Hoje, todos nós convivemos no dia a dia com serviços *online*, com soluções como telemedicina, trabalho remoto, comércio eletrônico e assim por diante.

E, a cada momento evolutivo, porque a gente vem numa constante exponencial nas últimas décadas, esse ambiente digital se expande, e se expande também a superfície de contato digital em que os agentes criminosos, maliciosos podem atacar essa nossa infraestrutura. Dados, sistemas e processos, então, estão ameaçados, pelos interesses das pessoas físicas ou jurídicas, de se corromperem, de serem manipulados de forma indevida.

As Nações Unidas, Senador, através do seu órgão UNODC, definem que o crime cibernético é hoje um crime transnacional. Nós não estamos mais como talvez ilustrado em filmes ou em romances utópicos, como a gente vê no cinema de Hollywood, às vezes; não são mais aqueles jovens - os "lobos solitários" - os agentes que a gente enfrenta no dia a dia. Nós estamos tratando de crime organizado, organizações transnacionais, que nos ameaçam nessa dinâmica do dia a dia. O que a ONU traz no seu... E as referências estão sempre citadas ali, Senador; sempre que é feita uma referência, há o *link*. A ONU clama por implementações de respostas urgentes, dinâmicas e internacionais.

Faço aqui um parêntese para saudar a realização desta audiência, Senador, no espírito de que eu vejo diversos colegas que têm atuado conosco no dia a dia nesta discussão, das instituições do poder público federal, do Legislativo, também do Judiciário, com diversos talentos que o Brasil tem. Então, este é um momento de facilitação dessa discussão e de orquestração desse trabalho. Saúdo, então, mais uma vez, a realização desta audiência.

O desafio contemporâneo não é apenas tecnológico; muito longe disso, ele é um desafio de governança. O risco geopolítico que o planeta vem enfrentando, na linha do agravamento, também amplia o risco cibernético. Isso é relatado naquelas duas imagens ali ao lado em que trago dois relatórios, sendo deste ano os dois. Um é do Fórum Econômico Mundial, em Davos, da perspectiva de cibersegurança global para 2023, em que se traz essa correlação entre o risco geopolítico se agravando e o risco cibernético também se agravando na mesma proporção. Esse mesmo estudo menciona que para este ano haverá US$7 trilhões de impacto para as organizações, para a sociedade mundial de prejuízos representados pelo cibercrime e antevê US$10 trilhões/ano, ou seja, são cinco PIBs brasileiros, em ordem de grandeza, como impacto para a sociedade global agora, em 2025.

Existe um outro ponto importante trazido por esse relatório, que é a evidência do efeito dominó - que a gente diz. Uma determinada instituição, em uma cadeia produtiva, que não tenha o aspecto de prevenção, compromete todas as demais envolvidas naquela sua cadeia produtiva, daí a interdependência sistêmica: todos nós temos que caminhar em conjunto. Esse é o espírito.

E o grande gargalo, o ponto fraco, no ambiente de prontidão cibernética, ainda é o capital humano; a conscientização de cidadãos, de usuários dos instrumentos digitais, porque são completamente, às vezes, expostos a más práticas de agentes maliciosos, agindo não por instrumentos tecnológicos, mas até por enganação da chamada engenharia social. É feita uma enganação do cidadão, e ele, por si só, passa a ser o ponto de fragilidade de toda essa corrente, mas, além disso, também na força de trabalho para a cibersegurança.

Daqui eu faço um apontamento, Senador, até como instituição de ensino e outras que estão aqui presentes, parceiras nossas na capacitação, para a formação do talento necessário, o talento ainda é muito escasso, para o enfrentamento desse crime organizado. Precisamos de mais profissionais especializados nesse tema.

E eu aponto, do segundo relatório que está apresentado ali do MIT (Massachusetts Institute of Technology), agora do ano 2023 também, um *ranking* global de defesa cibernética listando as 20 maiores economias do mundo, e o patamar em que o Brasil se encontra. O Brasil é o 18º dentre essas 20 economias.

As quatro linhas... Obviamente, os critérios são extensos, eu trouxe ali os quatro capítulos. Na questão de infraestruturas críticas, estamos em 17º; na questão de recursos de cibersegurança, em 16º; nas capacidades organizacionais, em 18º; e, no compromisso com as políticas públicas, no engajamento dos governos analisados, estamos em 19º.

Então, mais uma vez saudando a oportunidade dessa... Pois não.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC. Para interpelar.) - O senhor me permite uma interrupção? Porque eu acho que, senão, eu perco a oportunidade.

Eu conheço esse relatório.

O SR. HUMBERTO RIBEIRO - Pois não, Senador.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - O que eu não conheço é o grau de risco que nós representamos entre as 20.

O SR. HUMBERTO RIBEIRO - Excelente.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - Deu para entender? Ou seja...

O SR. HUMBERTO RIBEIRO - Sim. Posso chegar nesse ponto?

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - É a isso que eu queria chegar.

O SR. HUMBERTO RIBEIRO - Maravilhoso.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - Ou seja, quem somos nós em termos de alvo?

O SR. HUMBERTO RIBEIRO - Perfeito.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - E a resposta é muito importante, porque eu tenho dito aos que... Com quem eu mais tenho conversado, por exemplo, o Dr. Sabbat, que é o nosso cliente de consultas há muito tempo, que é uma sensação da sociedade brasileira, Presidente, de que nós exploramos muitas vezes, abordamos esse tema muitas vezes na Comissão de Relações Exteriores e de Defesa Nacional.

Chegamos a criar uma Subcomissão para esse assunto, fizemos visitas aos exercícios de defesa cibernética e de ataques cibernéticos simulados - eu frequentei, felizmente sobrevivi aos ataques.

Há uma noção mais ou menos generalizada da nossa desimportância, e a sua resposta é importante para abordar esse assunto.

O SR. HUMBERTO RIBEIRO - Tentarei abordá-la, Senador.

Se não for suficiente a resposta, eu fico à disposição para...

(Soa a campainha.)

O SR. HUMBERTO RIBEIRO - ... para o complemento.

(Soa a campainha.)

O SR. HUMBERTO RIBEIRO - Começando então nessa linha de resposta, eu não vou entrar em detalhes aqui, dado o respeito ao tempo, mas aqui segue um corolário temporal, em que, em 1986, houve o primeiro incidente cibernético registrado na literatura, que foi o ataque ao Berkeley Labs, nos Estados Unidos, onde um agente externo esteve infiltrado num laboratório de interesse de segurança de Estado americano, roubando os dados.

Eu faço referência aqui, de lá para cá, foram diversos incidentes. Passamos então de uma era de popularização da internet, como está descrito embaixo, a uma era de grandes incidentes, que começou com um incidente que parou o Governo da Estônia, enquanto país. O Governo ficou desfuncional no aspecto tecnológico. É o evento chamado "soldado de bronze". E aí entramos numa era de grandes incidentes globais, até em 2018 para 2019, quando dois fatos marcam a nova fase da segurança cibernética global: o primeiro é em 2018, a publicação da nova estratégia de defesa cibernética...

(Soa a campainha.)

O SR. HUMBERTO RIBEIRO - ... do Governo americano.

Posso continuar?

A nova estratégia de defesa cibernética do Governo americano, definindo que a segurança cibernética passa de um *status*, eu vou simplificar, no aspecto de dissuasão, para um aspecto de defesa ativa. Sair transperímetro das organizações e enfrentar o inimigo fora de casa.

Fica ilustrativo o exemplo hoje físico, que passa pela Ucrânia tendo que enfrentar o inimigo dentro da sua casa, não é? É muito melhor você fazer o enfrentamento do inimigo antes de ele adentrar o seu perímetro, não é?

E obviamente, com a covid, todos nós fomos forçados a abraçar a transformação digital. Todos os cidadãos. Então isso marcou uma exponencialização digital e um novo momento de defesa ativa.

Pois bem, o criminoso ataca então, o ataque começa ainda no ambiente externo, com fases. Esse é um corolário da Lockheed Martin, usado pelo Governo americano, a gente faz aqui algumas considerações a respeito disso. Sete fases-chave do ataque. Espero aqui, Senador Esperidião, trazer também insumos para a resposta.

Ainda no ambiente externo, o bandido realiza as fases de reconhecimento e de armamento. E ele então experimenta a fase de incursão, em que ele adentra o perímetro da organização. Normalmente, Senador Veneziano, no ambiente interno, as organizações tomam conhecimento de que o bandido está dentro, provocando prejuízos, entre a fase seis e a fase sete, quando o agente malicioso já está assumindo o comando e controle e realizando ações no objetivo. São diversas as ações possíveis.

(Soa a campainha.)

O SR. HUMBERTO RIBEIRO - Nesse ambiente interno, normalmente o bandido - isso são estudos do Instituto Ponemon, é um estudo já consagrado. Há mais de 19 anos fazem esse trabalho, em torno, desculpe, mais de 200 dias para se identificar o momento em que o bandido invadiu uma instituição digitalmente e a identificação do fato. E mais de 70 dias, em média, para se conseguir conter os vazamentos, a ruptura de dados que foi consagrada.

Em vários casos, Senador, o bandido atua de modo discreto e de forma perene. É um desafio persistente.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC. *Fora do microfone*.) - Ele se hospeda?

O SR. HUMBERTO RIBEIRO - Ele se hospeda e exerce o interesse dele sem que o órgão tenha conhecimento de que o bandido está lá dentro.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC. *Fora do microfone*.) - E o exemplo dos bancos...

O SR. HUMBERTO RIBEIRO - Diversos sistemas como saúde, educação, financeiro...

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC. *Fora do microfone*.) - No nosso relatório da CPI de 2016 de crimes cibernéticos, Senador Vital do Rêgo, já apontava isso, que compreendia quatro setores, no de finanças já apontava isso...

O SR. HUMBERTO RIBEIRO - Olha só...

Para o enfrentamento do ambiente interno, já temos ferramentas consagradas - instrumental, aparato - de segurança, chamadas de segurança fundacional. São diversos, são aspectos técnicos ali, de *firewall*, de antivírus, a própria gestão de *backups* e assim por diante.

O que chega, neste momento, à discussão, estimulado por este momento, como eu disse, lá de 2018, com a nova estratégia de defesa que os Estados Unidos iniciou e que diversos países vêm discutindo, é o caso brasileiro... a prontidão cibernética, então, como defesa ativa, entra nesse ambiente.

Como boa prática, temos a segregação entre as funções. Quem realiza a segurança fundacional não é o mesmo agente que realiza a prontidão cibernética. Isso traz valor agregado e elimina a chamada verticalização temerária. Quem testa, quem valida, quem elenca vulnerabilidades, não é aquele que está no muro fazendo o enfrentamento. Os dois trabalham em cooperação, mas de forma imparcial.

E, obviamente, como dissemos, a educação é a chave, a base de tudo.

Senador Esperidião, aproveitando a riqueza do seu questionamento, aqui são exemplos de serviços, obviamente o tempo vai me restringir para que entre cada um em detalhes.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - O senhor está me devendo a nossa classificação.

O SR. HUMBERTO RIBEIRO - Perfeito.

Nós temos, então, instrumentos de aferição tanto no aspecto de conformidade dos diversos padrões já consagrados nacional e internacionalmente, quanto na verificação efetiva das vulnerabilidades. Esse é um ponto fundamental.

Ferramentas, também, de inteligência contra ameaça: as chamadas DRPS e EASM, que são as de proteção contra riscos digitais; os instrumentos de governança das cadeias produtivas. Como eu disse, o efeito dominó fica aí sob observação; e programas de cultura cibernética são exemplos. Existem outros ferramentais que podem ser agregados.

Nesse sentido, Senador Esperidião, tivemos uma experiência que será apresentada agora, no dia 23, na Universidade de Brasília, na Finatec. Trata-se de um estudo feito para o então Governo de transição, agora, no final do ano passado, na qual foi feita a avaliação de vulnerabilidades específica. Foram 34 instituições, cobriram todas. Tivemos oportunidade de interação sobre esse assunto com os colegas do GSI sobre um determinado aspecto. As contribuições foram muito ricas, como sempre, e diversos outros... cada um dos componentes dos eixos ministeriais que estavam sendo criados, alguns com mais profundidade, outros com menos, mas foi um primeiro referencial de uma ótima prática trazida, que foi a seguinte: em trocas de comando, aquele momento de aferição de risco cibernético é algo importante para o gestor que chega, para saber o que ele está recebendo enquanto risco cibernético também. Perfeito? Senador, seriam essas as informações.

Eu permaneço à disposição.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - Mas eu continuo fazendo a minha pergunta: nós, em termos de alvo, estamos entre os 20?

O SR. HUMBERTO RIBEIRO - Senador, estudos apontam o Brasil como o segundo ou terceiro maior ambiente de incidentes cibernéticos do planeta.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - Pela estatística que é divulgada de número de ataques que sofremos é que a gente...

O SR. HUMBERTO RIBEIRO - Exatamente.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - ... é classificado, não é assim?

O SR. HUMBERTO RIBEIRO - Exatamente.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - Os nossos números são exorbitantes!

O SR. HUMBERTO RIBEIRO - Exatamente.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - Já que nós falamos do sistema financeiro, não interessa ao sistema financeiro divulgar, confere?

Senador Veneziano, em matéria de indicador, o Brasil não se faz confiável. Nós já tivemos casos - eu vou mencionar um caso específico, que não envolve segurança cibernética - de incoerência entre a estatística de assalto a bancos no Estado de São Paulo, que, num determinado momento, infletiu, ou seja, revelou uma curva descendente, que não coincidia com a curva da Fenaseg, que é quem paga o seguro, deu para entender?

Quer dizer, ou havia dificuldades no número dos seguros pagos ou a curva descendente não era verdadeira.

O SR. HUMBERTO RIBEIRO - Sr. Senador, só completando a resposta...

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - Então, se nós somos segundo ou terceiro, não podemos dormir no ponto em matéria de defesa cibernética. É isso que eu... é essa a moral da história que eu queria deixar registrada, até porque tenho que ir para a CRE daqui a pouco e acho esta reunião realmente muito importante.

O SR. HUMBERTO RIBEIRO - Sr. Senador, existem métodos e protocolos já consagrados para medição de forma transparente e imparcial. É só usarmos os mecanismos que estão disponíveis.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - Todos os indicadores têm que respeitar esses 14 critérios básicos para se constituírem: univocidade, quererem dizer a mesma coisa e não ter duplo sentido, e série histórica, que é onde se assenta a política pública.

Obrigado. Desculpe a interrupção.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Em absoluto, Senador Esperidião Amin. V Exa. bem o sabe, não o faço pela sugestão protocolar, mas V. Exa sempre abrilhanta e enriquece pelo seu conhecimento, até por força do que o senhor próprio pôde dizer ao público que nos acompanha da experiência de quem vivenciou, acompanhando diretamente, ainda à época, enquanto Deputado Federal, o vasto relatório que foi...

(Intervenção fora do microfone.)

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - .... o vasto relatório que foi produzido.

Eu agradeço ao Prof. Humberto e até peço desculpas por termos que fazer esse acompanhamento com uma certa rigidez no tempo estabelecido ou pré-estabelecido para que os demais outros integrantes e expositores também possam fazê-lo.

Já convido o Sr. Luiz Fernando Moraes da Silva, Secretário de Segurança da Informação e Cibernética do Gabinete de Segurança Institucional da Presidência da República.

Apenas um parágrafo do relatório que também foi robusto do TCU:

> *A fiscalização do TCU apurou que o Brasil ocupou a 8ª posição do mundo em número de ataques a dispositivos da internet das coisas (IOT) no período de abril a junho de 2021 e o 5º lugar em ataques de sequestro de dados em meados de 2021. Em 2020 ocorreram 41 bilhões de tentativas de ataques cibernéticos na América Latina, sendo 8,4 bilhões no Brasil.*

Sr. Luiz Fernando, por gentileza.

Muito obrigado, mais uma vez, pela sua presença.

O SR. LUIZ FERNANDO MORAES DA SILVA (Para expor.) - Eu que agradeço ao Senador e, na sua pessoa, cumprimento todos aqui desta seleta audiência. É uma honra para nós aqui do GSI poder contribuir com este debate, que nós consideramos ser da maior importância nesse nosso mundo globalizado, conectado e moderno.

Eu tenho uma apresentação bem curta. Procurei obviamente e naturalmente obedecer ao intervalo de tempo que me foi concedido. Eu gostaria apenas de fazer uma colocação sobre o que nós representamos e onde nós estamos.

O GSI, além daquela atividade que é mais conhecida por todos aqui - segurança institucional da Presidência e familiares -, também tem quatro secretarias que trabalham com outros assuntos muito importantes. Dentre elas está ali a Secretaria de Segurança da Informação e o nosso departamento.

Essa Secretaria tem como atribuição principal articular, em âmbito nacional, todas as iniciativas ligadas à segurança da informação e à cibernética. É uma secretaria nova. Ela era um departamento, mas foi alçada à secretaria em janeiro, por decreto.

Isso incorporou a missão cibernética dentro dela, porque nós entendemos que a cibernética, como uma ciência do controle, da regularidade de sistemas, abarca toda atividade econômica e social do nosso planeta como um todo, não é? Então, a missão aumentou, em função justamente do impacto que todos esses acontecimentos têm na nossa realidade. Então, a administração está respondendo até organizacionalmente para responder a esses desafios.

Esse é um eslaide extraído de uma outra apresentação, que procura explicar a urgência e a relevância de dois assuntos que nós estamos gestando dentro do GSI e que já está em estágio relativamente avançado no tratamento, que é a Política Nacional de Cibersegurança e a Agência Nacional de Cibersegurança. Ambas compõem um projeto de lei que está sendo tratado no âmbito dos ministérios já há algum tempo. Já recebeu sinal verde da Casa Civil, através de uma reunião que tivemos com o Sr. Ministro Rui Costa, e estamos dando continuidade.

Esse eslaide sintetiza talvez, dentro do conceito de urgência, os três principais termômetros. Nós observamos ali que, desde 2014, com a CPI das Espionagem Eletrônica já existia a ideia de se criar uma agência, de se ter uma política, uma governança centralizada nessa atividade. Existem muitas iniciativas no país competentes; existem profissionais dedicados, porém, a articulação, a governança é fundamental para que a cooperação se realize efetivamente. A cooperação, a regulação e o controle só são possíveis com uma centralidade dessa governança. Isso já foi detectado lá em 2014.

A nossa E-Ciber (Estratégia Nacional de Segurança Cibernética), um documento de 2020, foi produzido ainda sem uma política: uma política que definisse princípios, que definisse objetivos, diretrizes e que dê norte para todas as iniciativas que têm um cunho tecnológico muito pesado. Trata-se de um cenário econômico, como um todo, muito complexo e mutante.

Então, é preciso e é urgente a existência de uma política que consiga orquestrar a academia, a indústria, os governos das esferas federal, estadual e municipal e que possa dar condições para que a educação sobre cibernética e a conscientização sobre cibernética possam ser orquestradas em políticas eficientes e que consigam chegar ao resultado.

E, por último ali, a informação do TCU, o nosso órgão de controle externo, que já vem, há algum tempo, alertando a administração pública federal sobre a necessidade desse tipo de governança.

Então, esses três talvez sejam os mais importantes na argumentação de urgência e relevância desse projeto. O eixo estruturante dessa política pode ser, digamos assim, sintetizado nesta tríade: cooperação, regulação e controle, e aí eu trago algumas analogias.

Os senhores imaginem uma atividade regulada, como talvez a atividade aérea. Os senhores observem que as aeronaves que voam pelo nosso país e que vão para o exterior e retornam, todas elas são controladas por um sistema internacional de cooperação.

Assim como a cooperação para proteção cibernética é importante, ela existe também no espaço aéreo, que é um espaço que também é regulado; existe cooperação internacional para o tráfico das aeronaves e tudo; existe regulação, como naquelas que nós observamos quando nós frequentamos um aeroporto: questões de tarifas, questões de bagagens, questões de listas; e existe o controle, que é executado pela Força Aérea Brasileira, que faz, digamos assim, a degradação controlada do processo. O que é uma degradação controlada? Nós podemos ficar presos no aeroporto, porque a meteorologia do destino não é favorável, a nossa aeronave pode ter que alternar para um outro aeroporto por uma razão qualquer. Então, toda atividade regulada exige essa tríade, e, dentro da cibernética, é exatamente a mesma coisa.

É preciso cooperação de todos os entes tecnológicos para prover a resiliência e a proteção - a corrente é mais fraca de acordo com o seu elo mais fraco -; a regulação é importante, não para restringir atividade, mas para criar requisitos mínimos, para criar padronização de equipamentos que possam regular e certificar *hardware* e *software*; e o controle para prover justamente a degradação controlada, quando isso for necessário.

Os senhores imaginem, por exemplo, um outro sistema regulado que é o da energia elétrica. Nós temos lá o Operador Nacional do Sistema. Quando nós temos um problema numa linha de transmissão, existem pessoas ali dentro que conseguem regular, que conseguem alternar o fluxo da energia de forma a garantir que o sistema como um todo se mantenha resiliente e funcionando. A mesma coisa acontece no ambiente cibernético. Pode haver necessidade de um

link de satélite ficar inoperante, de um canal de comunicação, de um cabo submarino, de uma antena importante, de um operador em telecomunicações, e nós precisamos ter essa consciência situacional para gerir esse sistema e garantir a resiliência. Então, uma agência tem essa finalidade, e é assim que nós pensamos que ela vai agir.

Sobre a audiência pública: esse projeto de lei já está disponível para consulta. Na página do GSI, os senhores encontrarão a versão dele e, no Diário Oficial de hoje, já saiu a convocação para essa audiência, que vai ocorrer no dia 15, lá no GSI.

Desde já, convido todos, as senhoras e os senhores, a comparecerem, a tomarem conhecimento do assunto, para contribuir conosco na produção de uma legislação que seja o mais inclusiva possível e que possa efetivamente ser um instrumento útil, e não mais uma peça legal que não venha a atingir seus objetivos, o.k.? Então estão todos convidados a examinar essa peça aqui, que está em estágio de avaliação.

Eu agradeço pelo tempo e estou à disposição, é claro, para perguntas e debates.

Muito obrigado, Sr. Senador.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Obrigado. Obrigado, Brigadeiro, pela sua participação.

E evidentemente, ao término das demais exposições dos convidados, nós abriremos às perguntas que já nos chegam e já são em registros feitos pela nossa secretaria.

Passo a palavra ao nosso próximo convidado, Sr. José Luiz Medeiros, que representa a Associação Brasileira de Governança Pública de Dados Pessoais. V.Sa. tem a palavra.

O SR. JOSÉ LUIZ MEDEIROS (Para expor.) - Primeiramente gostaria de agradecer ao Sr. Senador Veneziano e parabenizá-lo pela oportunidade, pelo tão importante fomento dessa discussão na nossa sociedade, tanto em organizações públicas, e que serve de incentivo também para organizações privadas.

Eu tenho uma breve apresentação, para fazer algumas exposições.

Estratégia de proteção de dados governamentais, é um tema muito atual. Então até parabenizo a apresentação do nosso Prof. Humberto, com muita propriedade abordando também temas significativos. E eu espero não ser redundante, Professor.

Dando continuidade, quero fazer uma breve apresentação. Sou um dos membros fundadores, com nosso fundador também, Fabricio da Mota, nosso Dr. Fabricio da Mota. Então essa Associação Brasileira de Governança Pública de Dados participa ativamente, fomentando iniciativas iguais a essas.

Tem um pouco aqui das minhas referências acadêmicas. Atualmente eu estou na Secretaria de Representação do Governo do Rio de Janeiro em Brasília e atuo também assessorando tomadores de decisão e partes estratégicas de empresas. E sou profissional também fazendo auditoria em sistemas de gestão.

Falaremos um pouquinho sobre cenário geral do cibercrime. Tenho alguns dados atualizados para trazer. Pena que o nosso Senador Esperidião teve que se ausentar, devido a importantes compromissos, mas eu acho que alguns dados irão responder aos questionamentos dele.

Alguns diagnósticos do TCU que foram feitos em 2020, e há alguns cenários já em 2021 e 2022; desafios atuais no setor público, e aí, de maneira geral, o que está nos ferindo aqui, qual é a importância dessa atividade, o que a gente precisa atingir, qual é a causa raiz do problema, para a gente poder ter um norte, para poder atacar e fazer uma conclusão geral, então o cenário do cibercrime.

Vamos agora conhecer no cenário mundial. Então começamos aqui por essa frase do Primeiro-Ministro da Albânia, Edi Rama: "Se o cibercrime fosse um estado, seria a terceira maior economia do mundo, depois de Estados Unidos e China, com um PIB de US$10 trilhões". É algo supersignificativo. Olha a potência desse mercado. É um mercado que não para.

Então, o incentivo ao cometimento de crime cibernético está aí: dinheiro e muito dinheiro.

Então, nós temos 360 bilhões de tentativas de ataques somente na América Latina e Caribe; 86% das organizações em todo o mundo sofreram algum tipo de ataque em 2022, logicamente isso potencializado pelo cenário de pandemia da covid-19, em que todas as organizações públicas e privadas precisaram, a toque de caixa, transformar o ambiente administrativo para o ambiente digital; 10% é o crescimento dos ataques só de 2021 para 2022.

Cenário Brasil: primeira posição entre os países mais visados para golpes por meio de LinkedIn e WhatsApp, aqueles *links* maliciosos saíram do SMS, de *e-mails*, que ainda continuam, mas já estão sendo atualizados, então, temos o WhatsApp como uma ferramenta; 103 bilhões de tentativas de ataques cibernéticos somente em 2022, ano passado; 16% de crescimento de ataques entre o ano 2021 para 2022; quinta posição é a colocação do Brasil no *ranking* global - a fonte é a Fortinet.

Aqui nós já vamos agora conversar cenário Brasil, administração pública e, sobretudo, federal, diagnóstico do TCU em 2020. Podemos ali tirar três pilares do que foi identificado, fazendo um breve resumo do excelente trabalho que foi feito pelo TCU, Senador.

Primeiro, carência de estrutura e aí envolve tudo: investimento; sistema de gestão; fomento de conhecimento dos colaboradores, de maneira geral; deficiência de atos normativos que regulem o tema - com muita propriedade o Dr. Luiz Fernando apresentou essa iniciativa, mas ainda estamos carentes disso; falta de investimentos em segurança da informação e defesa cibernética.

Então, nós temos uma governança meio capenga, meio cega, e dentro dessas deficiências identificadas, faltam políticas. Políticas de quê? Corporativas, normativos, diretrizes organizacionais documentadas e conscientização de todos os colaboradores que estão, de alguma forma, dentro daqueles órgãos, daquelas organizações; carência de profissionais capacitados. Isso aqui também é uma das causas centrais desse problema.

Nós temos aqui alguns números do TCU: mais de 70%, então, das 410 avaliadas, 306 organizações analisadas não possuíam política de *backup* aprovada formalmente pela alta gestão. O que isso significa? O documento era informal. Então, o tomador de decisão não aprovou aquela diretriz formalmente.

Quem é competente para fazer isso? Será que essa diretriz é adequada? Será que representa a parte estratégica da organização? Isso é grave. Por quê? O *backup* é o que vai dar resiliência a essa organização no ataque cibernético de *ransomware* que vai criptografar banco de dados, etc. Se a gente não tem a receita do bolo de como aquilo deve ser feito, na hora que acontece, a gente não sabe o que ocorre. Como é que vai agir?

A informalidade ou falta desse documento aumenta demasiadamente esses riscos.

E aqui também: mais de 70%, S*hadow IT*. O que é isso? São *softwares*, são sistemas, são equipamentos que estão alheios à governança da organização. Então, o que significa? A organização não sabe que aquilo está sendo utilizado. Já pode estar com vírus um equipamento igual a esse, que não é corporativo. Não há gestão efetiva desse ativo e não há uma efetiva fiscalização desse equipamento, dessa utilização, dessa informação.

Nós tratamos - órgãos públicos - de informações estratégicas e, às vezes, classificadas de acordo com a legislação. Nós temos a Lei de Acesso à Informação, que dá um rol de classificações de documentos, até documentos restritos, confidenciais, secretos, etc. Temos também que mais de 60% das organizações não aplicam controle criptográfico nesses bancos de dados. São controles adicionais. Nós podemos cair no erro de "vamos criptografar todos os bancos de dados". Não seria talvez a estratégia ideal, por quê? Porque nós temos que saber que dados estão naqueles bancos. Então, nós precisamos fazer um mapeamento desses dados para aplicar esse recurso, porque é oneroso, de maneira correta, e mais uma vez a gente fala de governança. Então, a gente está falando de governança aqui que, muita das vezes, dentro da organização, não está sendo seguida. Podem ter políticas, procedimentos internos, portarias até do próprio órgão, mas como isso não é fomentado, não é fiscalizado, não está sendo utilizado.

Então, aqui, é a parte de recuperação de desastre (*Disaster Recovery)*, em que mais de 60% das organizações não mantêm ao menos uma das cópias sem acesso remoto. Então, tudo está conectado na rede. E o que ocorre? Está mais vulnerável. Então, ao ser vítima de um ataque cibernético, vai ficar tudo criptografado. Não tem um espelho daqueles dados separado, fora da rede, para que haja uma recuperação, para que haja uma continuidade desse negócio.

E aqui, olha, a gente já começa a ver a causa raiz do problema: maturidade organizacional. Então, mais de 80% das organizações estão no estágio inicial de capacidade de gestão e continuidade. Então, nós estamos falando aqui que dentro da implementação de seja qual for a diretriz do órgão, da organização, esses colaboradores não estão preparados para agir de forma segura, com segurança das informações e privacidade desses dados.

Basicamente, aqui a mensagem principal, o desafio principal é: é impossível proteger o que não é conhecido. E mais uma vez a gente está falando de governança...

(Soa a campainha.)

Pode continuar? *(Pausa.)*

Obrigado.

Então, os cenários mais comuns nas organizações: ausência, deficiência de gestão de riscos. A gestão de risco é o cerne de qualquer atividade, e segurança da informação é isso que subsidia a aplicação de controles para mitigar riscos. Se nós não fazemos isso, os controles serão mal aplicados, subdimensionados ou superdimensionados, gastando erário público de forma não profissional, e isso é muito complicado.

Falsa impressão de segurança. O que não é medido não tem como saber se está seguro ou se não está. Então, se nós não temos um sistema de gestão de incidente cibernético, de segurança, vai estar tudo o.k., nunca teve incidente, mas isso não está sendo medido.

Falha nas avaliações periódicas. Fiscalizações, principalmente auditorias internas. Então, as organizações públicas, de maneira geral, só se movimentam quando tem um órgão fiscalizador externo provocando, como o TCU, mas não têm ou, às vezes, não utilizam de maneira perene, de maneira contínua, as próprias fiscalizações, porque não têm profissionais capacitados para fazer isso.

E definição de indicadores e métricas. Eu tenho uma necessidade de ter um sistema de gestão de segurança cibernética dentro da organização, mas eu não sei quais indicadores eu preciso acompanhar para ver a saúde de um sistema de gestão dentro da organização.

Nós temos dados sendo tratados não somente no meio digital, nós os temos também ainda sendo tratados de forma física, sendo armazenados em microfilmes, etc. Então, isso abre ainda mais a necessidade de termos um sistema de gestão contemplando todos os meios em que aquela informação é tratada, e não somente focar na parte digital. Então, nós temos aí informações sensíveis trafegando, sendo compartilhadas, sendo encaminhadas ainda em papel.

Então, aqui, já finalizando, esse recorte. Nós temos o Sistema de Gestão de Segurança da Informação - o de privacidade é uma extensão a esse sistema -, em que ele percorre o Ciclo de Deming, que é o famoso PDCA: tem a parte de planejamento, organização, implementação, governança, avaliação e melhoria.

Então, a parte de planejamento, quando nós falamos que a maturidade ainda é muito inicial, nós paramos ali na organização; a gente consegue planejar, consegue estabelecer normativos, diretrizes, legislações, mas nós paramos ali na organização - definições de papéis e responsabilidades, talvez até treinamentos e conscientização -, e nós paramos aqui. Então, atividades iguais à implementação ficam carentes, inclusive por causa de *turnovers* de autoridade, de representante de determinados órgãos. Então, há um determinado... É natural, mas precisamos ter isso como políticas de estado.

Investimentos, por vezes, carentes, isso foi falado e diagnosticado pelo TCU.

A governança. Gestão de ativos. Ativos são equipamentos, *softwares*, até pessoas especialistas - então, nós não temos, essa identificação está meio carente -, acessos, operações, incidentes, gestão de fornecedores, muitos ataques visam aos fornecedores devido à resiliência ou ao porte da organização; quando ela é muito grande, não consegue diretamente, vai pelo fornecedor. Então, é preciso ter *assessments* de segurança cibernética para esses fornecedores para ver se eles têm o mínimo de capacidade, de adequação à legislação.

Avaliação e melhoria, principalmente por análises críticas, auditorias, primeira, segunda e terceira partes, parte de *due diligence*, para ver se todos os parceiros, cocontroladores, controladores, operadores de dados estão atendendo às legislações, e há o mínimo de resiliência cibernética, e *gap analysis*, que é essa análise de lacuna, o que está faltando para alcançar um nível mínimo de adequação às boas práticas trazidas pelo mercado.

Então, basicamente, é isso.

Deixo os meus contatos aqui.

Muito obrigado a todos.

Parabéns, mais uma vez, pela iniciativa.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Somos nós que agradecemos, inclusive pedindo a V. Sas. e perguntando-lhes se nós poderemos disponibilizar os eslaides que já foram trazidos e expostos? É importante, porque sempre, ao término, nós somos requisitados por aqueles que nos acompanham.

Passemos ao Sr. Arthur Pereira Sabbat, Diretor da Autoridade Nacional de Proteção de Dados.

Por gentileza, Arthur.

O SR. ARTHUR PEREIRA SABBAT (Para expor.) - Sr. Presidente, Sr. Senador Veneziano, Sras. e Srs. Parlamentares, senhoras e senhores aqui presentes e os que nos acompanham pela internet, eu gostaria de abordar, primeiramente, algo sobre o poder público e, depois, passando em termos mais gerais, inclusive falando do que a Lei Geral de Proteção de Dados Pessoais pode corroborar na busca de um cenário mais adequado de proteção de dados pessoais e de segurança cibernética.

Bem, o poder público é o maior detentor de dados do país hoje. Ele é assim não porque ele deseja ou por um mero capricho, mas porque ele precisa de dados pessoais para prestar serviços melhores e mais adequados aos cidadãos.

Segundo o Portal GovBr, 84% dos serviços públicos oferecidos pelo Governo Federal para a população estão digitalizados, isso no âmbito federal. Entretanto, ao tempo em que a crescente digitalização de serviços públicos tornou mais célere o atendimento às necessidades dos cidadãos brasileiros, também apresentou uma superfície de ataque valiosa aos criminosos digitais, que passaram com maior intensidade a ver as plataformas, *sites* e bancos de dados, inclusive bancos de dados do Estado, como potenciais fontes de ganhos. Inclusive tivemos dados alarmantes, como resultado da situação de pandemia que tivemos, da situação da covid-19, que impôs uma obrigatoriedade de migração em tempo recorde de trabalhos que eram presenciais - de grande parte do setor público e, inclusive, do privado - para *home office* e para teletrabalho. Essa migração em tempo recorde representou uma vulnerabilidade imensa de diversos sistemas, o que fez com que ataques cibernéticos nesse período crescessem mais de 250% e levou a perdas imensas e a vazamentos de dados pessoais também.

Agora, a LGPD, é interessante ver que ela possui diversos dispositivos que tratam de segurança, que são voltados também para os órgãos públicos. A segurança é tão relevante para a LGPD (Lei Geral de Proteção de Dados Pessoais) que se constitui em um capítulo específico, o Capítulo VII, que trata de medidas de segurança técnicas e administrativas, sendo que, ao longo da lei, existem outros tipos de abordagem para os entes regulados, no sentido de tratarem suas bases de dados com segurança. Destaco, em especial, o art. 46 da lei, que exige de órgãos públicos e de entes privados a adoção de medidas de segurança que protejam "os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

Poderíamos citar aqui uma série de ações também que poderiam preservar ações mais operativas - a parte de segurança cibernética. Mas essas ações todas, acredito, devem fazer parte de uma iniciativa maior, que, a meu ver, deve ser capitaneada pelo Estado, para evitar que a fragmentação de ações seja ainda maior, essa fragmentação que hoje temos no país, em que o Estado, hoje, se defende dentro de suas possibilidades e o setor privado faz o que pode. Então, nós temos aquela situação em que quem tem mais recursos se defende mais, quem tem menos recursos se defende menos e espera que nada aconteça com ele, mas essas ações poderiam ser, certamente, mais coordenadas. No âmbito do setor produtivo, essa fragmentação de ações, portanto, no campo cibernético, vejo-a ainda em um grau ainda maior. Então, é claro, quem tem mais ativos, mais valiosos a proteger se defende mais, e aqueles que não têm tantos recursos torcem - perdoem meu coloquialismo -, torcem para não sofrer ataques cibernéticos ou para que esses ataques não produzam tantos danos.

No caso da administração pública federal, o Executivo conduzia algumas boas ações nos últimos anos. Aí os colegas que me antecederam citaram também o Decreto 9.647, de 2018, que instituiu a Política Nacional de Segurança da Informação, mas é claro que uma política nacional por decreto, na verdade, representa uma intenção, uma coordenação macro do Executivo federal, mas uma intenção do Executivo, que ele passa para a sociedade. É uma intenção, não é? Um protocolo de intenções, na verdade. O Decreto 10.222, que aprovou a Estratégia Nacional de Segurança Cibernética, e o Decreto 10.748, mais recente, que instituiu a Rede Federal de Gestão de Incidentes Cibernéticos.

Mas embora sejam iniciativas muito boas e salutares, elas alcançam somente o Executivo federal. Falta um instrumento em âmbito nacional que estabeleça ditames essenciais e macrodiretrizes para a segurança cibernética nacional. E por isso, eu louvo essa iniciativa do GSI, que está em gestação, de uma política nacional.

A ideia é levar o tema ao nível estratégico, que é onde ele merece estar e como ele deve ser tratado pelo país, ou seja, falta, de fato, uma política nesse sentido, um grande instrumento, um diploma legal dessa envergadura, como uma grande concertação, porque a política nacional é isso, ela é uma grande concertação, diferentemente de uma lei geral, que tende a normatizar um tema do seu início ao seu fim. A política nacional é mais uma grande concertação; ela congrega a sociedade em torno desse tema, em torno de um sistema dinâmico e eficaz, em que todos os instrumentos, em que tenhamos instrumentos que levem à proteção dos crescentes ataques cibernéticos, que mitiguem essas perdas imensas que eles acarretam.

A criação de um grande sistema, portanto, nacional de segurança cibernética, obrigando o setor público e facultando o privado, o que é algo que funcionou em países na Europa, como a Inglaterra, por exemplo, terá efeitos certamente muito benéficos para elevar o nível de segurança cibernética de todas as instituições do país.

Agora, é claro que isso não é de todo suficiente, mas é uma grande iniciativa e é um grande direcionamento, considerando que todos os países que têm uma boa taxa de sucesso no combate aos crimes cibernéticos investiram em três grandes frentes.

A primeira frente é uma implementação de macrodiretrizes em âmbito nacional. Alguns países chamam de estratégia, outros de política, dependendo do ordenamento jurídico local. Mas esse foi o primeiro pilar de sucesso.

O segundo é compreender a mente do atacante, para estabelecer ações eficazes para combatê-lo. É interessante isso, não é? Eu vejo o Dr. Malaguti, um grande especialista, não é?

Agora, um ataque cibernético tem, via de regra, um ataque cibernético bem-sucedido, cinco vertentes, todas elas relativas ao atacante: motivação, conhecimento, habilidade, ferramentas e oportunidade. Todos os ataques cibernéticos bem-sucedidos têm esses cinco elementos.

A motivação varia muito, do atacante. Pode ser política, ideológica, financeira, religiosa. Podem ser diversas. Pode ser um Estado-nação perpetrando um ataque cibernético a mando do próprio Governo. Mas ele tem que ter também conhecimento para lidar com aquele ataque. E ele tem que ter habilidade em lidar com as ferramentas. Não adianta, às vezes, o conhecimento, se ele não é hábil. Ele tem que ter ferramentas a sua disposição para perpetrar um ataque cibernético. E por último, ele tem que ter a oportunidade.

E é claro que, quando um país atua de modo único, como no esforço como nação, o primeiro reflexo é que o país inteiro consegue reduzir essa vertente de oportunidade, começa a negar ou reduzir ao máximo a oportunidade que um atacante tem que ter. Que oportunidades são essas? Ou seja, são sistemas vulneráveis, é a cultura muito reduzida de segurança, são sistemas mal dimensionados, é a arquitetura computacional mal-elaborada, com recursos de segurança muito pífios, e isso faz com que aumente a oportunidade de um atacante atuar.

E a terceira vertente para uma taxa de sucesso como país - e já foi mencionado aqui também pelos colegas que me antecederam - é a obrigatoriedade do ensino de segurança cibernética de proteção de dados e privacidade que são um conjunto; é muito difícil segmentar um do outro, dicotomizar um do outro...

(Soa a campainha.)

O SR. ARTHUR PEREIRA SABBAT - Posso continuar? Só determinando.

... ou seja, a obrigatoriedade do ensino de segurança cibernética de proteção de dados e privacidade desde o nível fundamental, porque foi nas mentes mais tenras, na criança que outros países fizeram isso, conscientizando as crianças, conscientizando os jovens, os adolescentes dos riscos que eles diariamente enfrentam quando utilizam os recursos da internet, e isso, claro, aliado à capacitação de adultos, tanto no âmbito público como no âmbito privado.

Eu acredito que essas iniciativas, se adotadas, poderão levar o país a alcançar, em um cenário futuro, Senador, a tão almejada maturidade em segurança cibernética. Ela é difícil de alcançar mesmo. Nenhum país alcançou isso facilmente, alcançou ao longo de tempos, mas sempre teve o primeiro passo em uma ação coordenada como país, um esforço como nação. É isso que nós temos que ter com os três Poderes da União unidos, servindo de exemplo ao setor privado, e aí poderemos alcançar essa maturidade, que nada mais é do que um tripé formado de conhecimento, cultura e experiência.

Isso dito, só tenho a agradecer a oportunidade, Senador, e tenho certeza de que conseguiremos sucesso.

Muito obrigado.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Somos nós que agradecemos.

Antes de convidar o Dr. Fabrício, eu estava observando que nós estamos aqui diante de convidados que mais detidos estão à esfera governamental, mas estamos a tratar de um tema que está diretamente enredado com a iniciativa privada.

Vamos lá. Avancemos tecnologicamente. Criemos e implementemos todas as abordagens, as identificações. Estabeleçamos sistemas protetivos. Cheguemos, como muito provavelmente não haveremos de chegar, porque, da mesma forma como evoluímos aqui, as mais mentes evoluem igualmente, às vezes, até mais, mas, se nós não levarmos à iniciativa privada, às plataformas, ao indivíduo como pessoa, estaremos continuamente em uma situação de fragilidade. Ou não? Ou é uma abordagem indolente a que eu faço? Porque eu estava ouvindo a Luiz, como ouvi a Arthur, enfim, ouvindo a todos e me perguntava exatamente sobre isto: ou seja, avançamos nas instituições, nas esferas de governo e, se aqueles que estão com o propósito, qualquer um desses móveis, seja o financeiro, seja o político, enfim, qualquer um desses, mas eu quero por outro caminho, esse outro caminho é acessível? A mim me parece que sim.

Depois, eu quero ouvi-los, pretendo ouvi-los, até para dirimir essa minha ignorância.

Convido o Dr. Fabrício Mota para fazer uso da palavra.

O SR. FABRÍCIO MOTA (Para expor.) - Sr. Presidente, Senador Veneziano do Rêgo, cumprimento, na pessoa de V. Exa., os colegas palestrantes, painelistas, os que estão por vir também para participar. Agradeço imensamente o convite.

Eu sempre registro que, muito embora eu seja Conselheiro lá no CNPD, um órgão de auxílio à ANPD, um órgão consultivo, eu não falo em nome do conselho, mas me sinto muito confortável para compartilhar minha opinião e meus pensamentos a respeito deste tema, que é um tema que muito nos interessa já de longa data.

Eu vou me valer da fala inaugural do Prof. Humberto - utilizando-se de uma linguagem bastante acessível, como é típica dos brilhantes professores que temos -: prevenir sempre é melhor que remediar.

E percebo, Senador, que nós estamos, cada vez mais, enfrentando um ambiente social - e talvez seja desnecessário dizer - digitalizado. Acho que isso é óbvio, isso é evidente, mas nós temos uma necessidade de enfrentar a instrumentalização do Estado com as ferramentas adequadas para lidar com essa realidade. E essas ferramentas passam também por uma estruturação normativa. O Estado é refém - um Estado democrático de direito, constitucional como o nosso - da ordem jurídica. Este é o pressuposto básico de uma democracia constitucional: nós somos reféns da ordem jurídica. Nós não temos monarcas, nós temos leis. Elas regem a sociedade, elas são produzidas pela vontade da sociedade. O Parlamento é o elemento de vocação dessa vontade média da população, e nós estamos passando por uma sociedade cada vez mais embrenhada nos elementos cibernéticos, mas que não está acompanhando uma evolução normativa que seja suficiente para fomentar e dar condições para que o Estado possa reagir.

Algumas normas vêm surgindo ao longo do tempo. Eu faço uso também da fala do Sr. Luiz Fernando, quando ele nos trouxe diversos instrumentos, diversas políticas que já vêm sendo construídas ao longo do tempo, mas nós talvez tenhamos que enfrentar com uma percepção melhor de planejamento de regulação e de condições normativas para que o Estado possa atuar. A Lei Geral de Proteção de Dados, que foi citada com muita propriedade aqui pelo nosso Diretor Arthur Sabbat, já é uma norma que representa essa modernização do pensamento do legislador, já traz um elemento de governança, já traz um elemento, inclusive, principiológico de prevenção e já traz - o que é o mais importante entre todos esses elementos para garantir eficácia - a responsabilidade.

Todos podemos observar que a ANPD vem iniciando o seu processo de fiscalização e o processo de sancionamento. As responsabilidades já estão postas, as obrigações estão postas e talvez, não por acaso - também não quero constranger o nosso Diretor aqui com perguntas que ele não queira responder ou não possa -, a primeira listagem de agentes de tratamento, agentes regulados, que estão enfrentando processo sancionador sejam órgãos públicos, a primeira leva, digamos.

Isso talvez seja um fator de muita relevância para pensarmos na necessidade de dar ao Estado condições de atender a esse cenário a ponto de que não seja levado à responsabilização. Isso envolve, como foi dito por todos os que nos antecederam, o elemento principal da prevenção, mas o que é prevenção? Como é que materializamos a prevenção? Não é apenas um conjunto de boas ideias ou de boas práticas, mas essencialmente um conjunto de práticas, de ações, de realizações. E, no âmbito público, realização depende de condição, de orçamento e de previsão, inclusive normativa.

Eu digo tudo isso, Senador, justamente para oferecer uma visão da necessidade de evoluirmos esse ordenamento. Eu faço menção - já tive oportunidade de falar com V. Exa. sobre algumas ideias a esse respeito - a uma proposta de emenda à Constituição que tramita hoje no Senado e que estabelece uma visão de organização legislativa, fixando competência legislativa na União federal para organizar o ordenamento jurídico com relação a esse assunto, ou seja, entre as várias competências legislativas da União, que já são previstas hoje na Constituição, passaria a ter a previsão de norma sobre segurança cibernética, que é um elemento também relevante. Para além disso, como a gente fala sobre ações, sobre práticas, precisamos também que haja um dever do Estado de zelar pela segurança cibernética. Hoje, esse dever existe numa percepção de responsabilidade que parte essencialmente do Poder Executivo, como vetor de ação do Estado, e do Legislativo, como vetor de discussão, mas talvez tenhamos que pensar em um conjunto federativo, em uma organização federativa, União, estados, Distrito Federal e municípios, pensando e agindo efetivamente no sentido de garantir a segurança cibernética e a defesa cibernética, que são conceitos que não se confundem, mas que são conceitos essenciais.

O objetivo desta audiência pública, Senador, é tratar da prontidão cibernética em relação a bancos de dados governamentais. Prontidão cibernética - aprendi com o Prof. Humberto - está relacionada com estar preparado, estar pronto. Ora, essa prontidão depende essencialmente de um planejamento, mas de um conjunto de ações, que têm que ser implementadas, até para se dimensionar a responsabilidade. Eu só posso responsabilizar aquele que efetivamente deveria ter a obrigação de fazê-lo e não o fez ou o fez de maneira insuficiente. Então, esse planejamento de ações depende de condições.

Mais que isso, aqui fazendo um pouco de coro ao que o José Luiz Medeiros representa aqui como representante da GovDados, até mesmo para se buscar a responsabilidade do Estado, é preciso compreender as condições que o Estado tem para responder à altura. O Estado deve responder? Deve, mas nós precisamos criar condições financeiras, orçamentárias, humanas para isso. Precisamos de servidores capacitados, precisamos de investimento em aculturamento. Hoje, qualquer dos senhores aqui, que têm muito mais competência do que eu para falar sobre mecanismos de segurança, sabe que um dos elementos mais efetivos para intrusões e ataques cibernéticos é a engenharia social, é o mecanismo da engenharia social, que lida com fragilidades humanas. Como é que você combate fragilidades humanas? Com conhecimento, com

cultura. Talvez alguns anos atrás, o golpe do WhatsApp fosse uma coisa recorrente e fácil, mas, hoje, já é um pouco mais difícil, porque temos a consciência de que existe um mecanismo de fragilidade que é emocional.

Todas essas questões nos apresentam um senso de responsabilidade republicana. Pensar pela perspectiva da prontidão cibernética é fundamental como vetor de planejamento, mas, além disso, é desenhar as maneiras de concretização. A prevenção depende do planejamento, mas ela depende de ação. Eu não consigo me defender perante a ANPD apresentando uma política de boas práticas que eu não executo. Um papel isolado ou presente no meu *site* da internet não é suficiente. Eu preciso demonstrar perante o órgão de controle, inclusive outros, como o TCU também, que eu implementei e sigo implementando essas medidas que estão ali previstas. Se elas forem falhas ou insuficientes, eu também tenho a obrigação de revisar e aprimorar. Então, é um ciclo infindável de percepção a respeito dessa temática, Senador.

Eu vejo que o Senado Federal - em particular o Senado Federal - tem estado extremamente atento e parabenizo V. Exa. pela sensibilidade e liderança em provocar um debate dessa natureza aqui na Comissão. Temos a percepção compartilhada por todos que lidam com esse assunto, de alguma maneira, seja por dever de ofício, por aspectos doutrinários, acadêmicos e até mesmo por dever de profissão no âmbito da iniciativa privada, nós temos a percepção clara de que...

(Soa a campainha.)

O SR. FABRÍCIO MOTA - ... os próximos incidentes que envolverão o aspecto cibernético estarão no centro das fragilidades democráticas. Nós estamos falando aqui não de guerras ou ataques no sentido físico, mas essencialmente cibernético.

Toda essa percepção e esforço que têm sido promovidos pelo Poder Executivo, através de seus diversos órgãos, inclusive do Gabinete de Segurança Institucional, no sentido de perceber essas necessidades são fundamentais. Isso precisa reverberar entre todos os Poderes.

Tivemos um incidente gravíssimo no Superior Tribunal de Justiça há cerca de dois anos, e me recordo muito bem de um evento do qual participamos, vários dos colegas aqui presentes, pois foi um evento que teve um enfrentamento inédito. Ora! Temos que superar o ineditismo de realização desse enfrentamento e passar a estar preparados para aquilo que, de fato, seja inédito e que não possamos ter vivido, mas que temos que estar preparados para não viver.

Então, penso, Senador, que a iniciativa é excelente e espero que desta audiência surjam propostas concretas, propostas ativas, no sentido de fomentar e, inclusive, de proteger as instituições públicas, porque é o Poder Público que será, de fato, o vetor de direcionamento desse assunto na sociedade.

Muito obrigado.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Obrigado, Dr. Fabrício Mota, pela participação.

Antes de convidar para sua explanação o Sr. Leonardo Ferreira, Diretor de Privacidade e Segurança da Informação do Ministério da Gestão, eu quero registrar aqui, para nossa alegria também, as presenças dos senhores representantes do Conselho de Justiça Federal: Sr. Renato Solimar Alves, Subsecretário de Segurança da Tecnologia da Informação, seja muito bem-vindo; e o Sr. Kleb Amâncio da Gama, na condição de Assessor Institucional, seja igualmente muito bem-vindo.

Convido, e já está ao nosso lado, o Sr. Leonardo Ferreira, que é o Diretor de Privacidade e Segurança da Informação do Ministério da Gestão e da Inovação em Serviços Públicos.

V. Sa. dispõe de dez minutos, por gentileza.

O SR. LEONARDO FERREIRA (Para expor.) - Sr. Senador, muito obrigado pelo convite. Cumprimentando o senhor, cumprimento meus colegas palestrantes que me antecederam. A todas e a todos, um bom dia.

Vou tentar ser o mais objetivo possível aqui nessa exposição.

Sou Diretor de Privacidade e Segurança da Informação do Ministério da Gestão e da Inovação em Serviços Públicos, um dos nossos ministérios do Poder Executivo Federal.

O nosso departamento é responsável, no âmbito do Governo Federal, no âmbito da Secretaria de Governo Digital, pelas pautas de proteção de dados pessoais e segurança da informação.

Sobre alguns pontos que foram trazidos aqui, Senador, logo no inicio desses debates, nós entendemos que as temáticas de proteção de dados pessoais e segurança da informação precisam ser trabalhadas de maneira conjunta. E, assim, nós direcionamos todo o nosso esforço no âmbito da Secretaria de Governo Digital. Então, as temáticas são tratadas de maneira

conjunta, tanto é que acabo acumulando os papeis de gestor de segurança encarregado pela proteção de dados dentro da nossa organização. Acho que esse é um primeiro ponto.

Um segundo ponto que eu acho que vale um esclarecimento - o Sabbat trouxe uma informação importante - é que hoje a Secretaria de Governo Digital... O Brasil é um dos países mais digitalizados, que mais avançou na transformação digital no âmbito mundial. Hoje nós temos 148 milhões de brasileiros que já utilizam nosso acesso gov. A gente está falando de uma população de 220 milhões e a gente está dizendo que quase 150 milhões de brasileiros têm acesso, utilizam as plataformas do Governo, o gov.br. Isso é muito interessante, porque a gente tem mais de 4 mil serviços digitais - a pandemia foi esse elemento que acabou acelerando a necessidade dessa migração para o digital -, mas nós temos uma preocupação muito grande com um elemento basilar, que é manter a privacidade, a proteção de dados e a segurança da informação dessa população que acessa as plataformas governamentais. Como é que a gente faz? Como é que a gente trabalha?

O Fabrício trouxe aqui um ponto na fala dele: ele usou três vezes a palavra "prático", um aspecto prático. Ele usou "prático", "ação". Então, a minha fala é um pouco diferente dos colegas que me antecederam e que acabam trazendo um diagnóstico do que acontece no mundo. No Brasil, em específico, em órgãos governamentais, nós temos uma abordagem bastante pragmática. Hoje, o Governo Federal, capitaneado pela Secretaria de Governo Digital, é órgão central de um sistema para 251 órgãos. Então, quanto a todos os órgãos que se possa imaginar agora, nós somos responsáveis por endereçar, em coordenação com a Autoridade Nacional de Proteção de Dados e com o Gabinete de Segurança Institucional, o olhar para esses 251 órgãos.

E hoje, pessoal, de maneira bem pragmática, nós temos o Programa de Privacidade e Segurança da Informação. É um aspecto prático, é um aspecto bastante pragmático. Nós já temos dois anos de programa. Senador, no ano de 2022, nós fizemos um piloto com esses 251 órgãos, olhando para 57 órgãos. Nós utilizamos como critério o Acórdão 1.889, do TCU, que deixava muito claro aqueles órgãos que teriam ali sistemas críticos para o Governo. E, assim, nós fizemos um trabalho voltado para esses órgãos.

Mas o que é o PPSI? O Programa de Privacidade e Segurança da Informação tem o objetivo de melhorar a postura de segurança desses 57 órgãos. E assim nós fizemos ao longo de 2022. Olha só que interessante. O programa conta com cinco torres, cinco disciplinas. A gente olha para aspectos de governança, maturidade, tecnologia, pessoas e metodologia. Hoje existe, pessoal, e está disponível para vocês, um *framework* de privacidade e segurança da informação com um conjunto de 32 controles. São mais de 300 medidas, ligadas aos aspectos de privacidade e segurança da informação. Mas como é que se dá esse aspecto prático?

No ano de 2022, nós conduzimos uma autoavaliação com esses 57 órgãos. Fizemos uma nova avaliação no mês de julho e concluímos o ano de 2022 com uma terceira avaliação.

Essa avaliação... Existe um ciclo em que se passa por uma autoavaliação, é feita uma *gap analysis*. A partir daí, eu construo um plano de trabalho e o órgão, a unidade começam a fazer essa implementação.

Tivemos ganhos substanciais, tivemos um implemento de mais de 90% nessas medidas de segurança. Optamos por trabalhar com aquilo que a gente chama de o básico bem feito, é aquela segurança da informação e privacidade basilar. Então, nós escolhemos sete conjuntos de medidas cibernéticas e, a partir daí... O colega trouxe a questão de *backup*, que era uma dessas disciplinas, outra era controle de gestão de acesso, gestão de vulnerabilidades à parte, não é? Como é que você vai proteger algo que você não sabe? Então, a gente focou muito em inventário, tanto olhando para a parte de proteção de dados pessoais, quanto da segurança da informação. E também trabalhamos com a parte de *logs*. Caso você passe por um incidente de segurança, é importante que você tenha elementos para que os colegas aqui, que estão presentes, da Polícia Federal possam fazer o seu trabalho de investigação. Então, hoje a gente tem um olhar, eu diria, privilegiado desse movimento. Esse grande movimento, no ano de 2022, Humberto, nos trouxe segurança e convicção.

Agora, dia 28 de março, nós publicamos uma portaria - para quem tiver curiosidade, é a Portaria 852 do Ministério de Gestão - que tornou obrigatório esse programa para os 251 órgãos do Poder Executivo Federal. Então, hoje, quando a gente fala de pessoas... No ano passado, nós fizemos a 1ª Semana CyberGov, que foi uma semana, uma imersão de mais de 30 horas para órgãos de governo, discutindo boas práticas. Fizemos a 1ª Semana de Proteção de Dados Pessoais, em parceria com a ANPD e com o GSI. Tivemos mais de 4 mil inscritos. Então, é bastante prático. A gente acredita que o Governo precisa realmente ter essa liderança, sinalizar para o privado. Então, a gente fica totalmente à disposição, o Poder Executivo Federal.

Tem acontecido um movimento, Senador, muito interessante, em que alguns estados e municípios têm nos procurado e adotado a nossa metodologia e o nosso *framework*, a nossa forma de capacitar, porque o *framework* se torna o coração. Eu falo de 32 controles na área de privacidade e segurança, mas, quando eu penso uma capacitação, eu vou capacitar nessas competências que estão no *framework*; quando eu penso em comprar uma tecnologia, está ligado a esse *framework*. Então, tudo começa a fazer sentido e você começa a ter sinergia.

Então, o Governo, hoje, o MGI trabalha na Estratégia Nacional de Governo Digital, que é uma estratégia que se pensa para sinalizar para estados e municípios como o Governo Federal pensa. Por óbvio, respeitando as autonomias dos entes federados, é uma sinalização. Já existe hoje a Estratégia de Governo Digital, e um dos pilares dessa Estratégia Nacional de Governo Digital é exatamente a parte de privacidade e segurança da informação.

Se o senhor me permite, sobre essa dúvida que o senhor trouxe, essa questão em relação à preparação do privado, a gente interage muito no dia a dia, existe muita solidariedade nesse ambiente cibernético. Se você tem lá um banco passando por incidente de segurança, o GSI presta algum tipo de apoio. Mesmo não sendo um órgão governamental, há muita troca, muita inteligência, trocas de informação. Eu vejo, como o Sabbat trouxe, que aquelas estruturas, aqueles órgãos, as organizações que são mais estruturadas e contam com recursos realmente conseguem se defender em alto nível, mas a gente sabe que a gente tem uma gama de empresas privadas de pequeno e médio porte que demandariam apoio e suporte do Estado.

Então, hoje, na Secretaria de Governo Digital, no Governo Digital, a gente tem convicção de que é possível fazer esse movimento. A nossa, digamos, ambição de 2023 a 2026, no Poder Executivo Federal, é estar presente nesses 251 órgãos do Governo Federal.

Ministério da Saúde, Ministério da Educação, Banco Central, Exército, Marinha, Aeronáutica, qualquer órgão desses que vocês pensarem, provavelmente, vai ser um órgão da nossa área de responsabilidade. Então, existe uma troca muito ativa com esses órgãos, existem estratégias de a gente estar presente.

A gente criou uma estrutura, Senador, de governança em que a gente tem o encarregado pela proteção de dados, a gente tem um gestor de segurança...

(Soa a campainha.)

O SR. LEONARDO FERREIRA - .... o responsável pela auditoria interna e mais o diretor de tecnologia dentro de cada um desses 251 órgãos, que são responsáveis por esse programa. Então, assim, é como se fosse um pedacinho da SGD dentro de cada órgão, discutindo essas temáticas.

Então, hoje, eu diria, a gente está bastante animado com os resultados que a gente obteve no ano de 2022. Temos um marco legal para expandir e com possibilidade de sinalizar para estados e municípios o que a gente pensa no Governo Federal.

Fico à disposição lá na Secretaria de Governo Digital.

Muito obrigado.

Eu acho que essas são as nossas considerações, Senador.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Eu que agradeço, Leonardo, pela exposição feita, e já comentando sobre a indagação que nós fizemos, *a posteriori*, os senhores também, demais outros, se sintam à vontade se desejarem tecer qualquer outro comentário.

Como o último expositor... Antes disso, eu quero saudar a presença do nosso querido Flávio Silveira da Silva, representando a Polícia Federal, perito criminal que é na Diretoria de Combate aos Crimes Cibernéticos. Os meus cumprimentos e o meu agradecimento também.

Nosso último palestrante, o Sr. Carlos Renato Araújo Braga, Diretor de Avaliação de Segurança da Informação da Unidade de Auditoria Especializada em Tecnologia da Informação do TCU (Tribunal de Contas da União), que já foi por nós aqui mencionado no trabalho vasto e robusto que apresentou recentemente.

O senhor é muito bem-vindo e coloco à disposição o microfone para a sua exposição por dez minutos.

Obrigado.

O SR. CARLOS RENATO ARAÚJO BRAGA (Para expor.) - Muito obrigado, Senador Veneziano, pela oportunidade dada ao Tribunal de Contas da União de estar aqui podendo trazer a palavra a todos num assunto que nós consideramos bastante relevante. Cumprimentando-o, cumprimento todos os Parlamentares eventualmente presentes, os palestrantes que me precederam e que colaboraram muito com o que eu vou poder falar agora. Já que o trabalho do TCU já foi bastante mencionado, isso vai me permitir trazer outros elementos, elementos adicionais, para a reflexão dos senhores.

E eu já vou começar pela minha conclusão, que é a de que o Estado brasileiro, se pretende ser soberano, precisa colocar a defesa cibernética como tema prioritário na sua agenda. Essa é a conclusão da minha apresentação e vou começar complementando a sua inquietação. O setor privado, do nosso ponto de vista, é parte fundamental na defesa cibernética do país, e vou trazer alguns argumentos para a reflexão dos senhores com respeito a isso.

Por favor.

O.k. Obrigado.

Não, avança, avança... Bom.

Começo apresentando.... Eu vou me centrar num tipo de ataque para exemplificar o que acontece na prática, trazendo elementos mais práticos. O Brasil - essas informações são de 2022 - já era líder em ataques na América Latina e o segundo maior país afetado por ataques de *ransomware* - eu vou falar o que é isso, é um tipo de ataque da moda, vamos dizer assim. E agora a informação mais recente - essas são de 2022 -, de 2023, é agora do dia 10/5.

Essas são agências que compilam informações de inteligência. Esses são relatórios de inteligência que as empresas produzem, e nós já somos o país que mais paga resgate de *ransomware* no mundo. Então, isso aí responderia talvez uma pergunta de Senador Esperidião Amin sobre que lugar que nós estamos. Nós estamos em um lugar bastante desconfortável.

O que é um ataque de *ransomware*? É quando o atacante, o agente de ameaça, domina todo o ambiente da organização, criptografa e faz uma extorsão. Mas isso não acontece de uma hora para outra. Ele não entra, aperta o botão e domina. Então, ele entra, tradicionalmente, por uma dessas quatro portas. É uma maneira de classificar como o ataque acontece. Ou ele acontece por meio do *fishing*, que é aquele *e-mail* enganoso no qual o usuário clica e, a partir daí, decorrem algumas ações; ou ele entra porque há uma falha de configuração ou vulnerabilidade em algo que a organização coloca de frente para a internet - aí estão os serviços de *e-mail*, as páginas e as aplicações *web* que nós temos -; ele entra por conta de uma invasão de *malware*, que é aquele *pendrive* que alguém achou no estacionamento e coloca no computador para, por curiosidade, saber o que tem ali dentro, e, aí, o *malware* se instala; ou ele entra - e esse quarto elemento vai ser bem explorado ao final, para gente falar da iniciativa privada - por um terceiro, um parceiro que eu tenho e com quem, em princípio, eu tenho uma relação de confiança. Então, se ele invade o parceiro, ele vai conseguir chegar a mim, e o primeiro passo do atacante é ganhar o acesso inicial, que, no mundo da cibersegurança, é chamado de *foothold.* Ele entra na minha rede e ganha uma conta. Lá no TCU, ele consegue a conta do Renato Braga para fazer todas as operações que o Renato Braga faz, e eu não sou capaz de dominar a rede do TCU. Mas, com base na minha conta, abre-se para ele um leque maior de oportunidades, que, no mundo da cibersegurança, a gente chama de superfície de ataque. Ele começa a enxergar mais coisas que ele não enxergava antes de ser o Renato Braga dentro da rede do TCU.

E há um viés cognitivo de que a gente deve fortalecer mais e ter mais defesas no perímetro das organizações. Então, é como se eu fechasse a porta da portaria do meu condomínio e pensasse que está tudo bem, eu estou seguro aqui dentro. E isso não é verdade, porque o atacante pode passar as barreiras do condomínio; e aí, depois, ele precisa encontrar a porta da minha casa fechada; e, depois, se ele entra na minha casa, ele precisa encontrar o cofre da minha casa fechado. Ou seja, eu tenho que ter proteções em camadas ao longo do tempo. Isso porque o primeiro movimento que ele faz após entrar na minha rede se chama movimento lateral. Aí, ele começa a pular de máquina em máquina até ele encontrar uma máquina especial. E ele vai andando e vai dominando todas as máquinas, até que ele encontre essa máquina especial, que é a máquina que tem o comando de toda a rede e, a partir daí, ele pode, sim, fazer o que ele quiser. Aí, o que ele faz? Ele pode pegar todos os dados, inclusive e especialmente os dados pessoais, fazer a exfiltração, pode destruir tudo, dependendo da motivação, como foi comentado pelo Presidente da ANPD, ou pode fazer a encriptação dos dados, criptografar tudo, ou pode fazer essas três coisas em qualquer combinação que ele tenha vontade.

Essas linhas todas sugerem que a maneira que eu tenho que fazer para me defender é colocar essas várias barreiras. Eu tenho que ter o porteiro do condomínio, eu tenho que ter a minha porta fechada, eu tenho que ter a porta do meu quarto fechada, eu tenho que ter o cofre fechado e eu tenho que ter a empregada vigiando o que está acontecendo. Quanto mais camadas de proteção eu coloco, mais seguro eu vou ficando.

Por que essa explicação um pouco mais técnica talvez? Para mostrar que isso não é fácil de fazer, isso é uma coisa complexa. E é uma coisa complexa para quem defende e é uma coisa, muitas vezes, fácil para quem ataca, porque quem defende tem que fechar todas as portas e quem ataca só precisa achar um caminho desses aberto para chegar lá.

Então, nós estamos diante de um cenário que é bem semelhante a um cenário de guerra: ataques e defesas, ataques e defesas. E, nesse cenário atual, eu vou apresentar para os senhores alguns elementos que mostram que os atacantes estão em vantagem, e a gente precisa reverter o jogo.

Esses números ajudam a gente a entender que, do lado de lá - foi uma outra fala mencionada -, não temos mais aquele *hacker* isolado, aquele adolescente que é revoltado com o mundo e que está querendo explorar as coisas. As coisas hoje são profissionais nesse mundo. O último número que a gente tem ali... Esses relatórios todos, como eu disse, são produzidos por empresas de inteligência com base nos seus clientes. É um relatório da IBM do ano passado.

Vamos pegar a linha superior, que mostra que um atacante fica, em média, 207 dias dentro da sua rede antes de começar a atacar, ou seja, ele ganha o acesso inicial e fica fazendo esse movimento lateral, entendendo e conhecendo toda a sua

rede, sabendo todas as contas, quais os privilégios que elas têm, onde estão os dados mais valiosos, tanto do ponto de vista de dados pessoais, quanto de ponto de vista financeiro; no caso do governo, onde é que estão os documentos estratégicos, aqueles documentos que têm maior relevância e que, se vazados, podem expor a segurança nacional do país - e, por isso, eu disse que nós estamos diante de uma questão de soberania nacional. E, depois que ele consegue executar o ataque, na média, a organização leva 70 dias para conter o ataque. Conter significa não o deixar continuar se espalhando; não quer dizer a recuperação. Existe mais uma quantidade "x" de dias para que ele possa, depois de conter o ataque, erradicar, sumir com os vírus, com os *softwares* do atacante, conseguir pegar o *backup*, botar no ar e voltar à normalidade.

Esses números ali, se eu somar, só para eu poder me recuperar, significa meio ano - meio ano potencialmente. Portanto, eventualmente, esses ataques que nós tivemos nos órgãos governamentais, de cerca de um mês, dois meses, não espelham o que esses adversários, esses agentes de ameaça são capazes de fazer. Eles podem fazer muito mais do que fizeram conosco. Eles fazem muito mais com as empresas da iniciativa privada.

Continuando - e agora eu vou aprofundar um pouco -, o agente de ameaça, o adversário, o atacante, o *hacker* do mal, seja qual for o nome que os senhores desejem usar, ele não é amador. O nome técnico que se usa na cibersegurança é APT(*advanced persistent threat)*, ameaça persistente avançada. São verdadeiras organizações estruturadas, empresas, como uma organização empresarial, com hierarquia entre as pessoas, com funções definidas, financiadas para custear essas pessoas, ferramentas e equipamentos à sua disposição, da melhor qualidade possível, para atacar os adversários. Alguns relatórios de inteligência, inclusive, sinalizam que esses grupos podem ser financiados por países, tem orçamentos governamentais direcionados a esse tipo de coisa...

(Soa a campainha.)

O SR. CARLOS RENATO ARAÚJO BRAGA - ... com pessoal competente, motivado e com tempo prolongado, como a gente viu anteriormente, para executar as ações. Se ele pretende tirar um sistema crítico nosso do ar, ou seja... Vamos pegar um exemplo - e aí já vou iniciar a sessão de apresentar por que a iniciativa privada está envolvida. Se ele deseja tirar o Brasil do ar, ele tira o sistema elétrico do ar. O sistema elétrico está na mão, é operado pela iniciativa privada. E ele tem tempo para fazer isso, porque, quando ele fizer o estrago e a gente levar seis meses sem energia elétrica, para onde é que vai o nosso país? É uma reflexão. Então, eles são preparados para isso e têm tempo para fazer isso.

Já existem coisas como C*ybercrime-as-a-Service*. O que é isso? São esses atacantes profissionais disponibilizarem vídeos tutoriais, ferramentas na internet, e com isso eles ampliarem a quantidade de pessoas que vão promover aqueles ataques iniciais, para ganhar o *foothold*, ou o pé inicial, e vender eventualmente depois esse ataque inicial para que eles possam prosseguir. Os senhores estão percebendo que é uma coisa muito organizada. Nós não estamos falando de coisas esporádicas. Isso já está relatado em vários relatórios dessas empresas de segurança. É contra isso que o Estado brasileiro tem que lutar.

O TCU ainda não chegou ao ponto de mapear tudo isso. O TCU até agora fez trabalhos mapeando o que seriam as fragilidades de um pedaço pequeno do cenário brasileiro, que são a administração pública, os acórdãos que foram falados aqui. A nossa conclusão é que o jogo está desequilibrado. Nós estamos mais fracos do que eles.

E aí vêm os nossos desafios. Então, não adianta falar do problema, vamos ver por onde a gente começa as soluções. Já foi mencionado por praticamente todos os palestrantes: gente, o profissional dessa área não é um profissional *trainee*. O profissional de segurança começa a dar resultados três ou quatro anos depois de treinado. Ele não é um profissional de programação. Ele não é um profissional que entende de rede. Ele não é um profissional que entende de uma ferramenta chamada Active Directory. Ele é um profissional que entende de tudo, que entende das fragilidades que ocorrem nas várias áreas e que sabe entender os sinais que vêm dessas várias áreas, para compor os caminhos de ataque pelos quais o adversário vem. Naquele caminho que eu mostrei, vários ativos são atacados em sequência e só a percepção de que isso está acontecendo é que permite ao defensor entender: "Opa, tem alguém entrando aqui e tentando fazer um *ransom*". E aí naqueles 207 dias, ele consegue identificar o camarada lá para o dia cem, por exemplo, e consegue estancar o ataque antes de chegar ao final.

Então, recursos humanos em qualidade, qualificação necessária para a área de tecnologia no setor governamental é um tema que o TCU já botou em pauta desde 2008, com o primeiro relatório. Em especial, em 2014, um relatório do Ministro Raimundo Carreiro apontou isso de maneira muito clara: falta gente na TI do Governo. Agora, se eu olhar para a segurança, falta gente na segurança, na TI da segurança do Governo, para fazer segurança no Governo. Isso é muito grave. Isso falta no mundo, é um problema mundial. E quando a gente conseguir capacitar alguém, esse alguém vai ser comprado para trabalhar para fora, em dólar. Tem que se pensar em uma política de Estado para tratar com isso.

Segundo item: pelo menos em parte do Poder Executivo, em 250 organizações, esse problema já está sendo endereçado, como o Leonardo colocou aqui antes. É a fragilidade da implementação dos controles. Então, é o relatório que foi

apresentado pelo TCU em 2022, relatoria do Ministro Vital do Rêgo. Se a gente somar ali... Aqui tem uma síntese. Já foram falados sobre vários aspectos - *backup*, controle de acesso -, mas, quando a gente faz uma síntese, se a gente somar o pessoal que está no vermelhinho e o pessoal que está no azul, é o pessoal que está no nível que nós chamamos de inexpressivo e nível inicial, são os mais suscetíveis a ataque da administração pública, a gente vai ver que o número chega próximo a 80%, esse número já foi mencionado aqui agora. Então, tem que se implementar esses controles e as organizações estão correndo atrás de fazer isso, pelo menos no Poder Executivo, os 251 na liderança da unidade do Leonardo. E aí nós precisamos incentivar que socorra nas outras organizações públicas e na iniciativa privada também. Como é que nós vamos chegar lá? Nós vamos falar um pouco mais adiante. Liderança para governança e articulação. Outro trabalho de 2020, também de relatoria do Ministro Vital do Rêgo, apontou as fragilidades. Nós temos fragmentação nas políticas. Então, eu estou mencionando ali três políticas: duas do Executivo e uma do Judiciário. O Ministério Público está estudando como vai fazer a sua. E aí nós temos quatro políticas direcionando, dando o comando central, que não é central. Nós temos lacunas, porque não há direcionamento algum para a iniciativa privada, e nós temos ainda sobreposição. Então, como o Executivo apresenta duas diretrizes, nós temos ali uma sobreposição que pode ou não trazer algum tipo de conflito. Então, essa liderança, em princípio, está sendo endereçada pelo GSI, com essa nova proposta de diretriz nacional. E aí nós vamos participar. Tomamos conhecimento agora da audiência pública e minha equipe já está providenciando as informações para que a gente possa contribuir no aperfeiçoamento desse documento. Os desafios que nós pretendemos confirmar este ano. Este ano nós temos um grupo de fiscalizações que nós chamamos de Protege-TI, um grupo integrado. E aí nós vamos agora a campo, porque aqueles trabalhos iniciais antes, aqueles números são autodeclarativos. Então, eles tendem, segundo a nossa experiência, a serem piores na realidade. Então, se nós temos 80% de fragilidade, a prática anterior de outros trabalhos diz que esse número é maior. Então, este ano nós vamos a campo para ver se as coisas estão acontecendo por causa de uma premissa que tem que entrar na agenda do Governo também: papel não para ataque. Não é política que vai parar ataque. O que vai parar ataque é a configuração adequada no *firewall*, é a configuração adequada no Active Directory, é o usuário nosso consciente, recebendo ação de conscientização, que ele não deve clicar em *link* de *e-mail de* quem ele não conhece, que ele não pode usar o *e-mail* corporativo no LinkedIn, não pode usar o *e-mail* corporativo para fazer compra na Amazon. Nós vamos fazer seis trabalhos este ano para verificar o que está acontecendo e, na sequência, contribuir com ações de capacitação para os agentes do setor público poderem implementar de fato os controles que param os ataques.

O segundo ponto que nós queremos trazer, que foi mencionado pelo Diretor da ANPD, é incorporar uma visão de segurança ofensiva para a defesa. O que quer dizer isso? Nós estamos trazendo para cá princípios do milenar livro *A Arte da Guerra*. Se você quer saber defender, você tem que saber como é que o seu atacante ataca; se você quiser atacar, você precisa saber como é que o seu adversário se defende. Então, nós precisamos que os nossos técnicos de segurança de TI entendam como o ataque acontece, que eles entendam aquela figurinha que eu mostrei ali, que tem muito mais detalhes, tecnicamente falando. E posso presenciar aos senhores, eu não sei defender. Vou citar um exemplo claro agora: eu não sei configurar um serviço Active Directory. Mas eu sei invadir um serviço Active Directory e tirei uma certificação no início do ano, atacando sem saber defender, para evidenciar aqui com um depoimento real para os senhores que é possível fazer isso, é muito mais fácil atacar do que defender. Nós temos que estar muito mais preparados. Os militares sabem isso de largo tempo.

A terceira diretriz desse nosso trabalho é trazer a alta administração das organizações para o jogo. Os líderes dos órgãos têm que ter consciência de que isso é uma realidade e incorporar isso à sua agenda. E aí eu posso também trazer um depoimento real: dois anos atrás, eu coordenei um trabalho, que não tem a ver com segurança da informação, em que nós participamos de reuniões do que seria o comitê digital de mais de vinte organizações. Somente em duas delas eu ouvi os altos dirigentes tratarem de temas de segurança da informação. O que mais se trata é de colocar sistemas em produção para apoiar a execução das políticas. Então, cada vez mais, a gente quer fazer políticas, a gente quer digitalizar essa política, para ela ser eficiente, mas a gente não está preocupado em colocar segurança desde o início da concepção da solução. Aí a gente vai ter, cada vez mais, milhares e milhares de serviços aumentando a superfície de ataque e aumentando o risco de a gente ser atacado. Onde a iniciativa privada... Aqui, vem esta tela. O risco vai aumentar. Então, se os senhores acham que está ruim, a visão do TCU vem sempre alarmante, trazendo problemas, mas é o nosso papel. É o nosso papel! Graças a essa visão alarmante, a gente tem hoje uma política, em audiência pública, sendo conduzida. É o nosso papel fazer isso!

Aí eu chamo a atenção, agora, Senador, para responder à sua pergunta. Ali está a iniciativa privada. A iniciativa privada é um terceiro em relação ao setor público. Cento e cinquenta milhões de cidadãos brasileiros podem acessar o Governo pelo celular. Nós temos 150 milhões de portas de entradas para os atacantes. Se o atacante dominar o meu celular, e ele conseguir a minha conta gov.br, ele vai entrar dentro do portal e vai enxergar um monte de serviços de alguém que tem acesso ouro para acessar serviços que exigem uma autenticação maior. Portanto, ele tem um espectro maior de lugar para procurar todas as outras vulnerabilidades e começar a entrar dentro do sistema do Governo. Se uma empresa que faz

exportação, pequena, média ou grande, for invadida, essa empresa tem acesso ao Siscomex para interagir com o Governo. Portanto, o adversário tem acesso ao Siscomex e entra dentro dos sistemas do Governo.

Essa rede, esse sistema de proteção de segurança é uma coisa em que tem que haver uma proteção coletiva. Se a gente não fizer uma proteção coletiva no Brasil, no Estado brasileiro, o Estado brasileiro fica vulnerável.

Vou pegar um outro exemplo: a Secretaria Municipal de Saúde precisa interagir com o Ministério de Saúde. Então, os sistemas dela falam com o Ministério da Saúde. Se o sistema da prefeitura é invadido, o agente de ameaça ganha uma superfície de ataque maior para invadir o Ministério da Saúde. Nesta figura, a gente representa isso mostrando que a administração pública federal é um pedaço pequeno da administração pública. E o pedaço maior não é esse. O pedaço maior é do outro lado. É a sociedade brasileira. Dentro dela, o setor produtivo.

Eu coloquei ali, pequenininho, o que mais nos assusta. E a gente, já, já, vai chegar lá, porque a nossa equipe tem um mato alto tão grande para atuar, mas nós vamos chegar lá no que a gente chama de infraestrutura crítica...

(Soa a campainha.)

O SR. CARLOS RENATO ARAÚJO BRAGA - ... que é endereçada por uma das políticas do GSI. É aquilo que para o país, como eu falei, e que, em sua grande maioria, está nas mãos da iniciativa privada.

É nós começarmos a refletir o seguinte: o que acontece se o sistema de pagamento brasileiro, esse está na mão do Governo, do Banco Central, se ele for atacado e parar? Para o sistema financeiro. O que acontece se o Operador Nacional do Sistema - que não é do Governo, é privado - for atacado e parar? Acaba a energia elétrica do país. O que acontece se as operadoras de telecomunicações forem atacadas? Para a comunicação do país. Todas essas infraestruturas críticas estão tão vulneráveis quanto... A gente não sabe, porque a gente não tem informação de qual é o nível. Aqueles números que nós apresentamos são números do Governo, do setor público federal. Nós não sabemos quais são os números dos governos estaduais, distrital e municipais. E não sabemos quais são os números e a vulnerabilidade do setor privado. Portanto, quando a gente está cego, por prudência, a auditoria joga o risco lá para cima. Só por não saber, simplesmente não saber.

Aí eu volto à tela da conclusão, que foi por onde eu comecei. Se a gente pensar num Estado brasileiro soberano, a segurança da informação tem que ser priorizada na agência do Estado. E eu imagino que, nesta audiência, o senhor está inaugurando algo neste sentido: tentar colocar na agenda do Estado brasileiro a segurança da informação.

Agradeço a paciência de todos.

Muito obrigado.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Eu me ponho a dizer que não tomamos como alarmismo gratuito, absolutamente não. É uma participação e uma colaboração efetiva que o Tribunal de Contas, como também os demais outros órgãos, faz - faz o Tribunal, e fazem os demais - em relação a este tema, que é instigante. Eu falava com o Brigadeiro e dizia o quão complexo, o quão difícil de você contornar, porque, afinal, nos tornamos suscetíveis a cada dia que passa.

Enfim, quero saudar a chegada do meu querido parceiro, companheiro de Casa Senador Wellington Fagundes.

Como bem antecipei aos senhores e às senhoras, em face da agenda que se inicia em Plenário, às 11h, nós vamos aqui dar seguimento à participação daqueles que são fundamentais às audiências públicas e, como nós, têm dúvidas a apresentar-lhes.

Eu recebo, nós recebemos pelo Portal e-Cidadania, perguntas.

Sr. Newton Moraes, de Rondônia: "Quais os principais desafios enfrentados na implementação de estratégias de proteção cibernética de bancos de dados governamentais?".

Eu vou fazer a leitura, e os senhores podem, têm a liberdade de pedir a palavra para comentar. Perfeito? *(Pausa.)*

Então, a primeira delas: "Quais os principais desafios enfrentados na implementação de estratégias de proteção cibernética de bancos de dados governamentais?".

Estou olhando aqui, ao lado do Dr. Arthur e do Dr. José Luiz Medeiros.

Manu Silva, do Estado da Bahia: "Pretende-se estabelecer um protocolo mínimo a ser adotado pelos gestores para prevenção de ataques cibernéticos?".

Sra. Camila Vale, do Estado de São Paulo: "Quais os próximos passos para combater ameaças cibernéticas no Brasil?".

Sr. Felipe Chagas, do Distrito Federal: "Como o Governo pensa [Brigadeiro] em permitir uma autenticação multifator para a população de baixa renda para acesso aos serviços públicos?".

Sra. Josianne Sant'Ana, do Estado do Amazonas: "O que o Governo tem feito para combater ataques cibernéticos? Quais as ameaças para a população brasileira?".

Sra. Bruna Almeida, do Estado do Paraná: "Garantia dessas estratégicas? Quais são?".

Sra. Nathaly Santos, do Estado de Pernambuco: "De que forma a análise de comportamento de usuários pode ser usada para detectar atividades suspeitas em bancos de dados governamentais?".

Interessante.

Sr. Silvio Bonilha: "Está dentro da governança o tratamento do avanço da inteligência artificial, considerando até onde é o limite para obtenção dessas informações?".

Sra. Crystine Joranhezon, do Distrito Federal: "Uma vez que medidas de segurança englobam o processo de ferramentas, qual é a estratégica: foco no processo, na ferramenta ou nos dois?".

Por fim, Leticia Luche, de São Paulo: "Além da fiscalização pela ANPD, o Poder Judiciário pode atuar em conjunto na aplicação de medidas preventivas e coercitivas?".

Bem, eu não poderia pretender que os senhores tivessem memorizado todas as perguntas, mas, enfim, eu as coloco para que os expositores possam, de acordo com os temas abordados pelos nossos internautas, fazer algumas considerações.

O brigadeiro deseja fazê-lo em relação a como o Governo pensa em permitir uma autenticação multifator para a população de baixa renda.

O SR. LUIZ FERNANDO MORAES DA SILVA (Para expor.) - Do ponto de vista tecnológico, a autenticação multifator se baseia naquela tríade: o que você tem, o que você sabe e o que você é.

Imaginem, num acesso a uma instalação segura, é importante que a pessoa tenha o conhecimento de uma senha, o que ela sabe; o que ela é pode ser, por exemplo, uma identificação digital, uma íris; e o que ela possui, um cartão, algo assim. Então, é uma tríade.

Para a gente implementar isso na sociedade onde haja uma desigualdade, com pessoa com baixos recursos para utilizar esse serviço, nós não temos como escapar dessa realidade tecnológica. Nós precisamos realmente levar essa tríade, mesmo que incompleta, para essa pessoa, seja pelo celular que ela sua. Se ela não tiver, pela digital ou por uma senha. É uma questão da tecnologia.

Nós precisamos adotar a tecnologia possível dentro da realidade da sociedade.

Essa é a questão. Não se pode fugir do que existe no mundo real. A realidade é essa.

Quanto a mais um assunto, sobre a inteligência artificial, há um assunto interessante.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Só para creditar ao Sr. João da Silva, do Estado do Rio de Janeiro. Foi ele quem fez a pergunta ou não? A pergunta da inteligência artificial.

O SR. LUIZ FERNANDO MORAES DA SILVA - A inteligência artificial, pelos estudos que vêm sendo feitos, tende a ser - isso, afortunadamente, para o nosso lado - mais benéfica para a defesa do que para o ataque, porque a inteligência artificial, quando ela é circunstanciada ao que você está defendendo, ela conhece muito mais o que ela está defendendo do que uma inteligência artificial que está atacando.

Então, o que se tem hoje é que a inteligência artificial é, felizmente, um aliado da proteção cibernética. Ela tende a ser aplicada isoladamente ou já dentro de outras ferramentas, de forma a dar mais robustez e capacidades a todos esses *softwares* e essas soluções de TI que se apresentam para proteção.

Então, é um bom horizonte a aplicação da inteligência artificial.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Na verdade, foi o Sr. Sílvio Bonilha, de São Paulo, que fez esta indagação: "está dentro da governança o tratamento do avanço da inteligência artificial?".

Obrigado, brigadeiro.

O SR. LUIZ FERNANDO MORAES DA SILVA - Obrigado.

O SR. LEONARDO FERREIRA - Senador...

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Pois não.

O SR. LEONARDO FERREIRA - Seria possível um complemento...

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Claro. Fique à vontade.

O SR. LEONARDO FERREIRA (Para expor.) - ... sobre como lidar com esta temática?

Hoje, já existem em curso, no acesso Gov.br, na conta desses 148 milhões de brasileiros, níveis de segurança associados - níveis bronze, prata e ouro - em que nós associamos um conjunto de serviços de acordo com o avanço nessa jornada de segurança.

Então, a conta ouro, hoje, por exemplo, habilita que a pessoa, eventualmente, por exemplo, faça a declaração do Imposto de Renda utilizando esse tipo de autenticação.

Para além dessa questão de bronze, prata e ouro que habilita serviços, nós já utilizamos o reconhecimento facial para que você vá de prata para ouro.

Então, você consegue ter esse reconhecimento como uma chave, como um fator de segurança.

Existe em curso hoje, já, um percentual desses 148 milhões de brasileiros que utiliza um segundo fator de autenticação por meio, por exemplo, de SMS, que eles recebem no seu celular diretamente.

Então, pensando o Acesso GovBR, quando a gente olha para dentro de Governo, para unidades de Governo, existe uma diretriz da Secretaria de Governo Digital, em que se iniciou uma discussão muito forte em relação a essa questão de segundo fator.

Só para dar um exemplo aqui para as senhoras e os senhores: hoje no MGI - o Ministério de Gestão e Inovação -, nós baixamos uma diretriz da nossa Ministra de que todos os usuários dos nossos sistemas governamentais deveriam habilitar um segundo fator de autenticação.

Na Secretaria de Governo Digital, hoje, quando vou acessar o sistema corporativo, eu necessariamente preciso receber, em um outro dispositivo, um fator de autenticação. Caso as minhas credenciais sejam comprometidas, roubadas, muito provavelmente esse atacante não vai ter esse segundo dispositivo, então, não teria grande utilidade, porque ele não conseguiria fazê-lo.

Então, a gente inicia um movimento, olhando para todos os 251 órgãos da nossa área de responsabilidade, fomentando a adoção desse múltiplo fator de autenticação como uma medida muito importante.

Conectando com a parte de inteligência artificial, hoje já existe no gov.br uma solução que vem sendo construída com as empresas de Governo, Serpro e Dataprev, que é exatamente essa análise comportamental. É quando você consegue perceber que o Senador, por exemplo, acessou a sua conta gov.br, mas, historicamente, ele sempre acessa essa conta num período noturno, localizado aqui em Brasília, e, geralmente, em dias de semana. Qualquer coisa diferente disso já gera um bloqueio automático em sua conta.

Então, a gente está indo para uma solução antifraude com essas empresas de Governo para incorporar nesse serviço aos 148 milhões de brasileiros. Assim, nos próximos meses, a gente vê o amadurecimento dessa tecnologia, porque ela é muito importante.

Se uma pessoa loga da sua conta, por exemplo, lá do Rio Grande do Sul, imediatamente essa conta é bloqueada, considerando que as suas atividades, essa inteligência artificial, os processos de *machine learning*, conseguiram mapear que o seu trabalho, a sua base territorial é Brasília e, no máximo, Goiânia - são dois locais que você consegue...

Então, a gente tem avançado muito nesse sentido, como um fator de proteção - respondendo aos cidadãos.

Muito obrigado.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Obrigado, Leonardo.

O Sr. Silvio...

O SR. CAIO LEONARDO RODRIGUES - Sr. Presidente...

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Pois não.

O SR. CAIO LEONARDO RODRIGUES - Posso fazer uma sugestão?

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Pois não.

O SR. CAIO LEONARDO RODRIGUES (Para expor.) - Meu nome é Caio Leonardo Rodrigues, eu sou advogado em Brasília, Consultor da Aware e Conselheiro da OAB do Distrito Federal.

Assisti, tenho acompanhado, esse debate por dentro e estou de acordo com as preocupações, especialmente aquelas trazidas pelo TCU, que elevaram um pouco, indevidamente, a barra de preocupação.

Nós estamos, no Brasil, com uma visão de defesa cibernética ainda preocupada com direitos individuais, com o interesse e a defesa do cidadão e da cidadã, mas, definitivamente, nós estamos em uma quadra diferente da história.

Nós estamos em uma quadra diferente, nós não estamos mais só em Sun Tzu, nós estamos na quadra da doutrina Gerasimov, que é aquela que tem nutrido a guerra na Ucrânia, que é a guerra não mais como em Clausewitz, a guerra que é a continuação da política por outros membros, mas a guerra tendo a política como um dos seus meios. Então, a guerra sempre, a guerra todo o tempo.

E o Brasil hoje está se... eu vou usar aventurando, no melhor sentido, em apresentar-se como um *player* internacional importante numa das mudanças mais estratégicas e mais sensíveis da história da humanidade, que é a mudança do padrão dólar dentro da discussão sobre Brics e a entrada dos países produtores de petróleo nos Brics. E tudo isso em busca de um enfraquecimento do padrão dólar e uma alternativa a isso que nós todos estamos acompanhando, etc.

Eu digo isso para lembrar a pergunta que foi feita aqui pelo Senador Esperidião: qual é a relevância do Brasil no grande cenário internacional? A relevância do Brasil há um ano era nenhuma. O Brasil não tinha a menor importância no quadro geral das coisas. Só que agora nós nos colocamos, mais uma vez, como uma nação de importância substancial...

(Soa a campainha.)

O SR. CAIO LEONARDO RODRIGUES - ... no debate sobre o avanço geopolítico do planeta. E isso faz com que nós sejamos alvo do conflito de interesses em que nós nos metemos. E esse conflito de interesses não vai ser mais realizado através de "*boots on the ground*"; não é bota no terreno brasileiro, não é ataque com bomba no Brasil. O Brasil é grande demais para isso. É mais fácil destruir a capacidade de gestão e de articulação econômica por ataque ao sistema.

Então, com isso, e colocando também nesse contexto, é que eu, tendo ouvido o que os senhores falaram e considerando os *gaps* de legislação, de normativização, etc., é que eu instaria V. Exa., Presidente, a constituir um grupo de trabalho para pensar numa legislação nacional com esse viés de prontidão cibernética - não só de defesa, mas de prontidão -, para que nós nos adequemos à necessidade de defesa nacional, diante dos desafios que nós estamos enfrentando ou podemos enfrentar de agora em diante.

Muito obrigado.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Obrigado, Dr. Caio, pela sua participação oportuna. Efetivamente, inclusive - até porque o convite foi formulado pelo GSI, pelo Brigadeiro Luis Fernando -, fatalmente, fundamentalmente, o Senado também se permitirá, através de orientação do Presidente Rodrigo Pacheco, participar, colaborar e ouvir, até para que haja essa interação, esse processo de formulação legislativa e de discussão e debates no Congresso Nacional.

É o que penso ser, também, oportuno, para que nós instrumentalizemos isso.

Eu gostaria de ouvir - antes de repassar, aqui, algumas perguntas que já foram formuladas e ouvir os expositores - o Senador Wellington Fagundes, que pede pela ordem.

Senador Wellington Fagundes, por gentileza. Muito obrigado pela sua presença.

O SR. WELLINGTON FAGUNDES (Bloco Parlamentar Vanguarda/PL - MT. Pela ordem.) - Senador Veneziano, primeiro quero parabenizar pela oportunidade dessa audiência pública extremamente importante.

Como já foi falado aqui - isso já foi dito, mas eu quero repetir -, o Brasil passou do 71º para o 18º lugar no Índice Global de Segurança Cibernética. Isso foi divulgado pela União Internacional de Telecomunicações, que é da Organização das Nações Unidas. Aqui, no nosso continente, o Brasil situa-se atrás apenas dos Estados Unidos e do Canadá - é isso mesmo?

O índice, como os senhores bem sabem, é baseado em um balanço das intervenções de segurança cibernética na estrutura legal do país.

Eu tenho duas perguntas aqui, perguntas essas, inclusive, feitas pela consultoria, já que eu não sou um especialista na área: Na visão dos senhores, qual é a posição do Brasil e como ela reflete, com precisão, o estágio das políticas públicas de segurança cibernética no nosso país? E ainda, em nova edição dessa estratégia, quais aprimoramentos os senhores julgam mais importantes e necessários, claro, na legislação?

Eu quero também, aqui, registrar, Sr. Presidente... V. Exa. está propondo até a criação de uma comissão ou de uma subcomissão de inteligência artificial. Eu acredito que tudo tem a ver, tudo está conectado hoje. Eu também julgo extremamente importante o Senado... Quem sabe até uma Comissão, uma Comissão temporária...

Eu quero aqui... Na minha cidade, nós tivemos lá um evento criminoso, que aconteceu...

A assessoria está me trazendo aqui: "Comissão de Juristas responsável por subsidiar elaboração de substitutivo sobre inteligência artificial no Brasil"; seria esse o nome, não é?

Bom, tivemos a situação, lá, de um jovem de trinta e poucos anos, que, ao nosso ver, não era um bandido, mas que, talvez, o desespero o tenha levado a uma situação em que ele conseguiu montar uma bomba por controle remoto, num supermercado, e provocou uma explosão, fazendo uma chantagem

Felizmente, ele foi rapidamente... a polícia atuou muito bem e conseguiu prendê-lo. Eu, conversando com o Secretário de Segurança do estado, ele trazia a preocupação sobre o que fazer com a situação de um jovem como esse, que tem muito preparo na área, desse cidadão ficar lá, digamos, daqui a pouco, "refém" do crime organizado.

Tem alguma sugestão de vocês também? O que a gente poderia fazer, em termos de legislação? Como tratar uma situação como essa? Deve ser, no dia a dia, muito grande o crescimento dessa situação. Têm alguma sugestão? Porque imaginem um jovem, com muita capacidade, muita inteligência, domínio, e esse jovem, amanhã, está dentro de uma penitenciária a serviço do crime organizado. E a própria Segurança, o Secretário de Segurança, sem ainda uma definição do que fazer, de como tratar uma situação dessas. Claro que ele procurou colocá-lo separado, mas falou da fragilidade do sistema para controlar uma situação como essa.

E aí, claro, eu gostaria, do comentário de vocês, principalmente para os leigos que estão lá, para as famílias que, às vezes, veem seus filhos submetidos a essa questão. E, no caso do Mato Grosso, como nós temos um problema muito sério de faixa de fronteira, são 720km de faixa contínua, seca, mais trezentos e poucos... Esta semana mesmo, a segurança do estado conseguiu apreender lá mais de 1 tonelada de cocaína. Então, o Pantanal, aquela nossa região, é muito suscetível a essa condição do narcotráfico. O Pantanal é uma área muito grande, uma planície e pouco habitada.

O que nós podemos fazer exatamente numa questão de faixa de fronteira? Vocês teriam alguma sugestão para um melhor controle numa situação como essa? Claro que nós estamos falando de segurança. Então, acho que como hoje a gente não fala mais nem em rodovia, nós estamos falando em infovia, para tudo isso o Estado precisa se preparar.

Eu ouvi aqui a afirmação do Carlos dizendo que nós estamos perdendo o jogo. Foi mais ou menos essa situação. Eu gostaria de um comentário mais, digamos, popular sob esse aspecto porque, como a gente vê vocês falando, se o Estado demonstrar, também, que não tem a capacidade de estar à frente, isso traz uma temeridade muito grande para todos nós, principalmente na condição de legislador, às vezes, nos sentindo até, em certo momento, impotentes naquilo que podemos fazer.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Meu querido Senador Wellington, só para reavivar as duas primeiras questões que o senhor levantou, franqueando de imediato os expositores. O senhor falou sobre... Só para reavivar.

O SR. WELLINGTON FAGUNDES (Bloco Parlamentar Vanguarda/PL - MT. *Fora do microfone.*) - Posso ler de novo.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - É a posição do Brasil...

O SR. WELLINGTON FAGUNDES (Bloco Parlamentar Vanguarda/PL - MT) - A visão dos senhores palestrantes é genérica.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Sim.

O SR. WELLINGTON FAGUNDES (Bloco Parlamentar Vanguarda/PL - MT) - A posição do Brasil reflete com precisão o estágio das políticas públicas de segurança cibernética no país? E a outra é: na nova edição dessa estratégia quais aprimoramentos os senhores julgam mais importantes? Aprimoramento em termos de legislação, necessários. Eu acho que aí o comentário é bem amplo.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Perfeito. É só para trazer já franqueada a oportunidade de dar fala aos nossos convidados.

O SR. LEONARDO FERREIRA - Senador...

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Pois bem, Dr. Arthur.

O SR. LEONARDO FERREIRA - Não Arthur, por favor.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Leonardo.

O SR. LEONARDO FERREIRA (Para expor.) - Eu posso trazer uma contribuição sobre o segundo ponto que o Senador Wellington nos trouxe, sobre essa preocupação com a questão de jovens. O senhor utilizou o termo jovens.

A gente tem feito algumas trocas de informação com países como Dinamarca, Israel, só para citar alguns, Espanha, Estados Unidos, nesses últimos dois, três anos. Há uma preocupação muito grande, eles trabalham muito o termo "*hacker* do bem". São esses jovens, algo até natural, essa geração digitalizada, que já nasce tendo acesso aos meios tecnológicos muito cedo e que, a partir disso, vai desenvolvendo um conjunto de conhecimentos e habilidades ligados à parte de tecnologia que, muitas vezes, a habilita a montar dispositivos como esses que o senhor citou aí, no Estado de Mato Grosso.

Eu acho bem interessante citar aqui uma iniciativa da RNP, talvez seja útil até aprofundar, conhecer um pouco mais, mas eles iniciaram um projeto recentemente, foi coisa de uma semana o lançamento, que eles chamam Hackers do Bem. É uma iniciativa da RNP junto com o Senac ou Senai - tenho que aprofundar, só para checar essa informação - para capacitar, no Brasil, pelos próximos anos e neste ano de 2023, 30 mil jovens. Exatamente trazendo uma formação voltada para a questão de segurança cibernética, segurança da informação, mas, mais do que isso, trazendo os valores, porque é como você está falando, existem essas ferramentas e elas podem ser utilizadas para o bem.

Então, eu acredito muito em educação, muito em treinamento, conscientização, tanto é que o nosso programa de privacidade tem uma torre de pessoas que a gente olha o tempo inteiro. É a fronteira. A gente vai conseguir virar esse jogo exatamente capacitando, e os jovens são um elemento muito importante que não pode ser esquecido.

Então, estou tentando trazer aqui esse trabalho dos Hackers do Bem, iniciativa essa da RNP que rapidamente o senhor consegue localizar na internet e que é muito interessante, muito relevante. Isso pode ser expandido e está no *roadmap* aqui do nosso programa de olhar para os jovens, dentro dessa perspectiva.

É só uma pequena contribuição.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Obrigado, Dr. Leonardo.

Dr. Arthur.

O SR. WELLINGTON FAGUNDES (Bloco Parlamentar Vanguarda/PL - MT. Pela ordem.) - Só mais um comentário, Sr. Presidente.

Inclusive agora eu estava vendo uma matéria, o Japão está fazendo uma revolução na área da educação, e é exatamente isso o que eles estão tentando fazer: que as crianças entrem para a área do bem. Uma educação já da criança na pré-escola, para que ela possa, então, estar preparada para utilizar toda essa tecnologia para o lado do bem, fase em que, infelizmente, nós sabemos que as nossas crianças também estão extremamente suscetíveis.

Talvez um comentário sobre esse aspecto também fosse importante.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - E que foi feito no início ou em uma parte da exposição do Dr. Arthur. Ele pode gentilmente trazer de volta.

Dr. Arthur.

O SR. ARTHUR PEREIRA SABBAT (Para expor.) - Muito obrigado, Senador, muito obrigado pelo questionamento, Senador Wellington.

A primeira pergunta sobre a posição de 18º no *ranking* da UIT, se apresenta, de fato, na atual situação do país, risco cibernético.

Eu creio que não, nós ocupávamos a 71ª no ranking da UIT em termos de segurança cibernética, e a União Internacional de Telecomunicações leva em consideração uma série de fatores para esse posicionamento, esse *ranking*, em termos de maturidade cibernética. E o que fez a diferença foi a publicação do Decreto 10.222, da estratégia nacional de segurança cibernética, que fez o país sair da 71ª para a 18ª, mas é claro que... Por quê? Porque o país não tinha nada que apresentasse, para a sociedade brasileira ou para o mundo, uma iniciativa ou um conjunto de esforços que significasse que o Brasil queria progredir nesse terreno mais assertivo.

Por isso, a ONU leva muito em consideração quando um país estabelece políticas, macro ou diretrizes, porque isso significa que o país sinaliza para as outras nações que está preocupado com um tema estratégico, como é a segurança cibernética.

No caso do segundo ponto, desses recrutamentos que acontecem com os nossos jovens, esse é um recurso bastante antigo utilizado inclusive pelo Estado Islâmico, que utilizava a *darknet*, a *deep web*, para poder fazer os seus recrutamentos, inclusive com vistas não somente a ações de cinéticas, ações físicas, como integrantes do exército deles, mas, também, como ações de cibersabotagem, ciberespionagem e ciberterrorismo.

Na legislação brasileira, nós temos mais de 40 crimes cibernéticos tipificados, só que, como o nosso ordenamento jurídico concentra tudo - nós não temos uma legislação específica de cibercrimes - no Código Penal e em outros códigos, de atuação

do servidor público e em vários outros diplomas, então esses crimes cibernéticos estão pulverizados. Eles existem, foi uma opção estratégica jurídica nossa e assim temos feito.

Agora, o ideal, como pontuei há pouco, no caso dos países que estão vencendo essas crises cibernéticas e vencendo a luta contra o crime organizado, vencendo a luta contra ataques cibernéticos e reduzindo seus prejuízos morais ou financeiros, comerciais, mercadológicos e reputacionais, é exatamente o incentivo na parte educacional de crianças e adolescentes.

Há os moldes como já estamos acostumados a fazer com o Código de Trânsito. Então, a professora pinta ali no chão a estradinha, bota os semáforos, às vezes de papelão, bonitinho, ou desenha ali. Isso já vai instruindo a criança no que é certo, no que é errado em termos de trânsito. A mesma coisa temos que fazer em termos de segurança cibernética e proteção de dados, porque a criança passa a valorizar desde a tenra idade aqueles princípios e já os vai enraizando, e elas vão crescer como cidadãos conscientes e cidadãs conscientes.

Nas instituições públicas e privadas, a gente fala muito: "Ah, porque temos que combater, temos que incentivar as instituições públicas e privadas". Mas, às vezes, nos esquecemos de que essas instituições são feitas de pessoas e pessoas que têm essa cultura desde a tenra idade tendem a ser, claro, cidadãos conscientes, cidadãs conscientes. E o índice de erros, como bem pontuou o Dr. Fabrício Mota, na parte de engenharia social, a pessoa que vulgarmente cai em golpes, isso tende a reduzir fragorosamente, assustadoramente com a cultura em proteção de dados e em segurança cibernética.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Pois não.

O SR. MARCELO MALAGUTTI (Para expor.) - Eu gostaria de agradecer a oportunidade oferecida pelo Sabbat.

Meu nome é Marcelo Malagutti, eu sou Assessor Especial do Ministro do GSI e um dos responsáveis junto com o nosso Secretário pela proposta da política em andamento.

Eu gostaria de fazer um complemento, Senador Wellington, com relação à questão do jovem que já se desviou, porque a proposta da educação é extremamente relevante, é fundamental do ponto de vista da preparação do jovem que ainda não se desvirtuou, mas nós temos que pensar no futuro e também no agora.

Alguns países - eu tive a oportunidade de passar dois anos fazendo a minha pesquisa na Inglaterra - recrutam os *hackers* já incriminados, já indiciados ou até já condenados e passam a utilizá-los para reforçar o lado público na repressão a outros criminosos.

No Brasil, infelizmente, o nosso marco legal ainda é um pouco complexo com relação a essa situação, mas nós já encontramos evidências hoje de, por exemplo, no mercado financeiro, no qual eu tenho bastante experiência, de utilização de *hackers* que se infiltraram nos sistemas dos bancos, alguns com intenção criminosa e outros como *hackers* do bem, como disse o Leonardo, e aí os bancos os contratam para fazer parte da sua equipe de prevenção. Naquela lógica que o Dr. Carlos Renato colocou com relação a aprender as técnicas ofensivas para poder preparar as defesas.

Então, caberia, talvez, Senador, nos prepararmos, num grupo de trabalho, nesses debates aqui do Legislativo, e trabalharmos com a perspectiva de fazer alterações no nosso marco legal para que, por exemplo, os juízes, quando condenassem criminosos que perpetrassem crimes cibernéticos, pudessem aplicar penas alternativas do tipo: auxiliarem as polícias estaduais, a Polícia Federal, eventualmente, ou outros órgãos como uma medida de punição, ajudando a sociedade.

Obrigado pela atenção.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Obrigado, Dr. Malagutti, pela participação.

Dr. Carlos.

O SR. CARLOS RENATO ARAÚJO BRAGA (Para expor.) - Com respeito à educação para a preparação para o futuro, não é a minha área na educação, mas eu sei da existência de pontos, dentro da base curricular nacional, que já tratam desse tema de educação cibernética, prevenção, como lidar com notícias falsas e outros assuntos correlatos à segurança da informação.

Então, é questão de implementar essas coisas que já estão previstas na base curricular nacional e tornar isso realidade para os nossos jovens.

O SR. WELLINGTON FAGUNDES (Bloco Parlamentar Vanguarda/PL - MT) - Sr. Presidente...

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Pois não, Senador.

O SR. WELLINGTON FAGUNDES (Bloco Parlamentar Vanguarda/PL - MT. Pela ordem.) - Apesar de todos aqui, eu acho, conhecermos, eu gostaria que alguém, ao fazer o comentário, explicasse o que é um crime cibernético, porque muitos dos que estão nos assistindo, às vezes, não têm nem noção do que é um crime cibernético.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Qual dos senhores?

Inclusive, a sua exposição, meu querido Malagutti, é a pergunta da Sra. Letícia, que foi mais ou menos nesta linha: "Além da fiscalização pela ANPD, o Poder Judiciário pode atuar em conjunto na aplicação de medidas preventivas e coercitivas?".

José Luiz falava sobre a pergunta que fora feita: quais os principais desafios enfrentados na implementação de estratégia de proteção cibernética de bancos de dados governamentais?

Em seguida, a questão que foi feita, inclusive, com o propósito de levar, pedagogicamente, aos nossos telespectadores o que foi pontuado pelo Senador Wellington.

O SR. ARTHUR PEREIRA SABBAT (Para expor.) - Muito obrigado, Senador.

Um crime cibernético pode ser perpetrado de duas formas: ele é uma conduta ilícita que pode ser perpetrada com o uso de computador, com o próprio fim de fraudar algum sistema eletrônico - e aí ele seria chamado crime cibernético próprio -; ou com o uso de computador para atingir algum outro sistema ou para fazer algum outro mal a alguma pessoa ou a alguma organização, que seria o crime cibernético impróprio, sempre com o uso de meios computacionais, mas, às vezes, ou para atingir um próprio sistema eletrônico, que aí é o próprio, ou para angariar recurso ou atingir outros sistemas que não computacionais, propriamente computacionais, como, por exemplo, *revenge porn* ou, então, *cyberbullying*, que não atinge o computador, mas é um crime impróprio, mas tipificado.

Obrigado.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Sua vez, por gentileza, ao comentário que foi feito em forma de pergunta do Sr. Nilton Moraes, do Estado de Rondônia.

O SR. JOSÉ LUIZ MEDEIROS (Para expor.) - Sim.

Bom, os principais desafios - nós verificamos aqui durante as exposições -, basicamente, estão concentrados na governança de um sistema de gestão de segurança da informação e privacidade de dados. Nós verificamos que há planejamento, sim, robusto, implementação, definição de diretrizes e de legislações, mas, na fase de implementação, a gente vê uma carência, e na continuidade desse sistema de gestão. Então, a estratégia tem que se voltar para a manutenção dessa implementação de um sistema de segurança, resiliência cibernética, definição de papéis e responsabilidades, obrigatoriedade de times de segurança cibernética, segurança da informação, que pega toda a parte mais governamental ali dentro do órgão - de governança, melhor dizendo -, mas também dotado daqueles profissionais mais especializados, *red teams*, *blue teams*, que estão aptos a testarem os sistemas de que atualmente dispõem o órgão, mas também podem fazer a devida contrarresposta em um caso de incidente, de um ataque cibernético.

Obrigado, Presidente.

O SR. LUIZ FERNANDO MORAES DA SILVA - Senador?

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Pois não, Sr. Luiz Fernando.

O SR. LUIZ FERNANDO MORAES DA SILVA (Para expor.) - Em relação a esse posicionamento que o Brasil vem angariando nessas estatísticas mundiais, o que tem um peso específico muito grande é justamente a digitalização da nossa economia. Ela tem um peso específico muito grande nesses *rankings*.

É verdade, o Brasil só fica atrás do Canadá e dos Estados Unidos na digitalização do seu Governo. Foram grandes vitórias, de muitos anos para cá, como quando, por exemplo, houve toda aquela inclusão digital para o pagamento de auxílios emergenciais. Foram mais de 40 milhões de benefícios digitalizados em pouquíssimo tempo. Foi um grande feito tecnológico na área do Governo digital no Brasil. Esse tem sido o carro-chefe que tem levado o Brasil a aumentar nesses *rankings*, mas, como já foi dito aqui também, a segurança cibernética tem que caminhar em conjunto com isso daí. É uma estatística que precisa ser examinada sobre outros aspectos. O Governo pode se digitalizar, mas a população precisa também ter condições de fazer uso, as economias precisam se potencializar com essa digitalização. É um contexto bem maior.

Quanto ao uso das tecnologias, também já foi dito aqui, há a doutrina de defesa por camadas em profundidade. Nós mencionamos aqui várias tecnologias para proporcionar a defesa dos nossos sistemas, mas elas precisam ser arquitetadas. Existem muitas ferramentas e muitas tecnologias, mas elas precisam ser aplicadas em diferentes camadas e é preciso precificá-las, porque há tecnologias que são muito caras e que não podem ser aplicadas em grande número. Há tecnologias mais simples que podem ser aplicadas em grande número.

Então, existe a necessidade do conhecimento de um arquiteto de soluções cibernéticas. É como já foi dito aqui: o profissional não é um programador, não é um analista, não é um profissional específico, é alguém que conhece a tecnologia, que conhece o cenário e as fragilidades e que é capaz de arquitetar essa solução. Agora, o senhor imagina isso a nível nacional. É uma arquitetura nacional que vai englobar altos níveis de cooperação, até de coragem, de propósitos, de reconhecimento das próprias fragilidades que cada setor tem.

Cada setor da nossa economia conhece a sua área, conhece o que sabe defender melhor. Não vai existir um único arquiteto defensor de toda a economia brasileira. Vai existir um conjunto setorial de *experts* naquela área que precisa conversar com *experts* de uma outra área para que se consiga uma resiliência razoável em nível nacional.

Agora, a digitalização é uma atividade mais direta. É o emprego de tecnologia no serviço ou na atividade industrial. Ela tem interesses bem mais simples, bem mais factíveis de gerar esse consenso. Ninguém está pensando na fragilidade. Essa é a grande visão que eu, pelo menos, tenho dessas estatísticas que são publicadas sobre o Brasil.

O SR. RENATO SOLIMAR ALVES - Presidente, poderia falar aqui?

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Pois não.

O SR. RENATO SOLIMAR ALVES (Para expor.) - Gostaria apenas de trazer à reflexão... Me apresentando, sou Renato Solimar Alves, do Conselho da Justiça Federal. Trabalho na área de segurança cibernética lá e também participo do Comitê Gestor de TI do Poder Judiciário, do Comitê Gestor de Segurança da Informação do Poder Judiciário, e também, na academia, como pesquisador. Para quem não conhece, a UnB possui um mestrado profissional em segurança cibernética, que alguns órgãos já tiveram a possibilidade de ter turmas; e também faço parte desse time de pesquisadores, digamos assim.

Dentro das inovações possíveis sobre as quais esta Casa talvez pudesse refletir, com relação a, como o colega se posicionou ali, essa possibilidade de trazer penas alternativas em que se possam usar esses conhecimentos, eu já vi estudos no sentido de que as empresas possuem programas públicos de recompensa por descobertas de vulnerabilidades. São os programas Bug Bount, como eles chamam. Então, grandes empresas, como Facebook e Google... Eu já vi estudos relacionados ao Governo de Portugal sobre a possibilidade de se ter alguma forma de recompensar aqueles que descobrem vulnerabilidades. Então, de certa forma, você vai usar o conhecimento público das pessoas que atuam nessa área não atuando diretamente no Governo e já o auxiliando a identificar os problemas mais críticos, aquilo que você poderia tratar.

Hoje, confesso que seria muito difícil algo acontecer nesse aspecto, mas gostaria de trazer à reflexão a possibilidade de possuir programas públicos de recompensas pela descoberta e indicação daqueles problemas para os *hackers* que estão aí pelo mundo. Então, é algo a se pensar.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Obrigado...

O SR. WELLINGTON FAGUNDES (Bloco Parlamentar Vanguarda/PL - MT) - Presidente, só para contribuir.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Pois não, Senador.

Só para agradecer, meu querido amigo Senador Wellington Fagundes, ao Sr. Renato Solimar Alves, que é Subsecretário de Segurança de Tecnologia da Informação.

Por gentileza.

O SR. WELLINGTON FAGUNDES (Bloco Parlamentar Vanguarda/PL - MT. Pela ordem.) - Era exatamente isso que eu ia pedir, para cada um se identificar, porque depois nossa assessoria vai poder ter acesso, fazer alguma consulta. Acho que é muito importante que cada um se identifique...

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Sem sombra de dúvidas.

O SR. WELLINGTON FAGUNDES (Bloco Parlamentar Vanguarda/PL - MT) - ... para a gente buscar depois...

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Claro, efetivamente.

Quero saudar a chegada do Senador Izalci Lucas.

E passo a palavra ao Sr. Flávio Silveira da Silva, que é Perito Criminal na Diretoria de Combate aos Crimes Cibernéticos na Polícia Federal.

Sr. Flávio.

O SR. FLÁVIO SILVEIRA DA SILVA (Para expor.) - Bom dia a todos.

Agradeço o convite para participar desta audiência, em nome do Diretor de Combate, o Dr. Otávio, e da Coordenadora-Geral da Diretoria de Combate aos Crimes Cibernéticos, a Dra. Cassiana, que está aqui neste momento.

Esse tema vem ganhando importância, nos últimos anos, todo mundo sabe disso, e a Polícia Federal vem sofrendo transformações relacionadas a essa importância. Eu trabalho nessa Diretoria desde 2009 e passei por várias etapas que sinalizam a importância que vem ganhando esse tema de segurança cibernética no Brasil e na Polícia Federal. Inicialmente, uma unidade informal, que não tinha nenhuma chefia formal definida, se transformou e hoje, desde janeiro, ela foi transformada em uma diretoria própria. Ainda bem. Para a nossa surpresa e felicidade, a gente se tornou uma diretoria e a gente também teve a nossa criação, na Polícia Federal - tendo em vista a importância, e a quantidade de crimes, e esse aumento que a gente vem presenciando nos últimos anos -, a criação, além da diretoria, das delegacias regionais nos estados, nas superintendências, para a investigação dessa matéria de crimes cibernéticos.

Dentro da nossa diretoria, a gente tem três coordenações temáticas que são relacionadas a crimes, como falado pelo Dr. Sabbat, crimes próprios específicos cibernéticos. Temos ali investigação de crimes de pornografia infantil, então tem uma coordenação para esse tipo de investigação. Temos a coordenação de investigação de fraudes bancárias eletrônicas, que é um crime muito comum, e o Brasil é um celeiro desse tipo de crime, e a nossa tecnologia, infelizmente, é exportada e os nossos *hackers*, nessa matéria, são muito bons. E tem a coordenação em que eu atuo como coordenador substituto, que é a coordenação de crimes de alta tecnologia, que atua com esses novos crimes de alta complexidade, como crimes de *ransomware*, que têm se tornado o novo crime padrão nessa área de ataques a órgãos e a instituições privadas.

Hoje em dia, é mais fácil você sequestrar o dado de uma pessoa - que vai ter muita importância para ela, econômica ou organizacional - do que você sequestrar uma pessoa. Então, você consegue sequestrar aquele dado, pedir um resgate em relação àquilo e, se a pessoa não pagar, você pode até a extorquir para ameaçá-la de que o dado vai ser divulgado e conseguir um resgate maior. Então, é esse tipo de situação que não só o Brasil, mas o mundo vem enfrentando, e há uma tendência de aumento, infelizmente. A gente vê que esse tipo de crime vem aumentando. E a ideia da cooperação e da atuação em parceria com outros órgãos, não só com a administração pública, mas também com a iniciativa privada, é um caminho fundamental a ser seguido.

A Polícia Federal tem aumentado a sua participação de uma maneira preventiva, nessa área. Então, a ideia não é só de atuar depois que o incidente ocorreu - você muitas vezes não tem muito o que fazer, se todos os dados estão criptografados, se você não tem um *backup* daquilo ali, isso muitas vezes se torna irremediável.

Para você atuar de uma forma preventiva, como seria essa forma preventiva? Em cooperação com outros países, essa troca de informações de vulnerabilidades ou de credenciais vazadas que muitas vezes são vendidas em fóruns, em mercados, com esse tipo de informação, a gente pode agir de forma proativa, como a gente vem atuando, para uma comunicação com órgãos públicos que possam ser alvos de ataques ou de instituições privadas, para evitar que danos maiores aconteçam. Então, um vazamento de credencial que hoje está sendo noticiado em um fórum da *dark web*, por exemplo, daqui a um mês, pode se tornar um incidente de *ransomware* naquela mesma instituição. Então, a nossa atuação com essa ideia da cooperação internacional, aprofundando esses mecanismos, tem essa finalidade de evitar esses danos maiores.

Eu gostaria de agradecer aqui o convite. A audiência, o debate, tem sido muito enriquecedor.

Obrigado.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Nós é que agradecemos - em nome do Senado e desta Comissão de Infraestrutura - a sua presença representando a Polícia Federal.

Eu, evidentemente, gostaria... Pergunto ao Senador Izalci se V. Exa. deseja fazer participação para, logo em seguida, encerrarmos esta audiência pública.

Senador Izalci Lucas, querido companheiro.

O SR. IZALCI LUCAS (Bloco Parlamentar Juntos pelo Brasil/PSDB - DF. Para interpelar.) - Sim, Presidente.

V. Exa. sabe que nesta Casa a gente bate o escanteio e tem que cabecear. Então, eu gostaria muito de estar aqui desde o início, é uma matéria super-relevante, mas nós tivemos a reunião de Líderes, e depois, na sequência, ainda mais outras atividades. Mas, Presidente, rapidamente, eu não quero, até porque esse assunto já deve ter sido abordado aqui, eu vou direto para algumas questões sobre que você já deve ter feito a apresentação.

O gabinete lá, o GSI, estaria elaborando uma Política Nacional de Defesa Cibernética para fornecer diretrizes com relação a essa questão. Então, eu perguntaria, não sei, não vou fazer direto, mas quem puder responder: como a Política Nacional de Defesa Cibernética vai responder aos desafios apontados pelo Tribunal de Contas da União? Em qual estágio de elaboração

está a referida política? E haverá a criação ou uma proposta de criação da Agência Nacional de Segurança Cibernética como já vimos aventado pela mídia? Essas são as colocações.

Com relação a... Estava direcionado, mas para todos aqui: quais as medidas já adotadas em outros países que deveriam ser implementadas pelo Brasil para evitar ataques como o do dia 10 de dezembro de 2021? E qual é o impacto em termos de previsão de um impacto orçamentário dessas medidas que já acontecem lá fora e que poderíamos aplicar aqui? E com relação ao ministério da gestão, quais as ações do Ministério da Gestão e Inovação estão sendo implementadas para aumentar a segurança da informação da gestão pública? Acabei de ouvir do nosso representante da Polícia Federal que o que a gente mais tem com relação a segurança, mas de forma especial, da Polícia Federal é uma carência muito grande de pessoas. Há algum tempo, já não tem concurso, não chama os profissionais. E essa área é uma área que tem que se atualizar sempre, não é? Como é que está a situação, inclusive, lá da Polícia Federal, mas de outros órgãos do Governo com relação a essa questão? Porque isso não é totalmente terceirizado; tem gente da própria polícia que desenvolve e acompanha tudo isso.

Então, de fato, parabenizo a audiência pública. É fundamental, é um assunto superimportante. Nós que participamos do marco regulatório da internet, agora essa questão aí, uns chamam de *fake news*, outros de medida restritiva, no sentido de censura, então tem toda essa polêmica que está sendo votada aí. Mas o que percebemos, já marcamos três reuniões, três audiências estão previstas agora, com relação à inteligência artificial, porque, no Brasil, normalmente você já quase que proíbe tudo antes de acontecer, não é? O brasileiro é muito criativo, mas, por exemplo, essa primeira audiência trata da questão jurídica. Então, já querem fazer toda uma regulamentação, algumas dificuldades para você implementar a inteligência artificial, mas não podemos esquecer o aspecto tecnológico, de inovação. Nós temos que dar a essas audiências exatamente esse foco também, porque o Brasil não pode ficar na dependência de outros países.

Então, eram as minhas considerações. Eu não sei se já foi tocado, eu depois vou dar uma olhada também nas notas taquigráficas, mas, se puder responder a essas indagações, agradeço.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Nós que agradecemos, Senador Izalci, a V. Exa., que é tão intrinsecamente, na sua história parlamentar, vinculado às questões de inovação, de ciência e de tecnologia. Eu faço sempre questão de registrá-lo como uma das referências envolvidas nesse debate, desde a oportunidade que tive, acompanhando-o na Câmara Federal e agora, mais ainda, podendo observar e abeberar-me da sua sensibilidade em todos os espectros, mas notadamente na área de ciência e tecnologia.

Eu passo a palavra ao Sr. Luiz Fernando, porque V. Exa. pontuou sobre uma questão do GSI, e, em seguida, franqueando também aos demais outros a oportunidade da fala, já nos dirigindo derradeiramente às nossas despedidas.

Sr. Luiz Fernando.

O SR. LUIZ FERNANDO MORAES DA SILVA (Para expor.) - Bem, a política que está sendo gestada é a Política Nacional de Cibersegurança, não necessariamente de defesa cibernética, que é o conceito mais do âmbito militar. É uma política que estudou, já há longo tempo, as melhores práticas internacionais, a organização dos governos das nações mais avançadas, procurando adaptar isso à nossa realidade. E o item mais importante que nós observamos é justamente a existência de uma governança, seja através de um centro, de uma agência ou de um outro ente estatal que possibilite o que já foi dito aqui, justamente a atividade de governança através da cooperação, da regulação e do controle da segurança cibernética nacional.

Então, o projeto de lei de uma política traz um conjunto de princípios, entre eles, por exemplo, o combate ao cibercrime, o uso ético dos meios tecnológicos e tudo mais. Há também um conjunto de diretrizes, há também a própria proposição da agência, a sua estruturação, o seu conjunto de atores.

E, dentro do que o senhor perguntou sobre custos, essa agência, pelos nossos cálculos, que já estão praticamente terminados, demandará pouco mais de R$500 milhões em cinco anos. Isso representa uma parcela ínfima, digamos assim, dos prejuízos que a cibernética tem causado. Só para dar um exemplo ao senhor, recentemente foi publicado o resultado de uma investigação realizada no INSS que, se não me engano, registrou R$1 bilhão de prejuízo. E nós estamos falando de R$500 milhões em cinco anos, isso envolvendo não só a parte de pessoal, mas também a atividade de custeio e a estrutura.

Então, é uma iniciativa que nós constatamos claramente a sua relevância e a sua urgência, porque ela vai propiciar, justamente, o que o senhor está perguntando: como é que nós vamos conseguir consertar tudo isso? Como é que nós vamos conseguir resolver ou melhorar todos esses problemas que já são prementes e já estão contabilizados, já estão presentes em estatísticas? Parte daí, da governa centralizada.

Então, a nossa esperança é que esse projeto possa encontrar eco nas Casas Legislativas e que, rapidamente, nós possamos nos instrumentar, porque se tornaria uma lei de aplicação em todo o país. O que nós temos, hoje, são decretos de aplicação

restrita à administração pública federal apenas. Então, o nosso modelo atual já apresenta uma deficiência intrínseca: nós não conseguimos concertar essa ação em nível nacional.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - A propósito, só para renovar, porque fatalmente haveremos e faremos questão de estar presentes, qual é o dia da audiência que o senhor...

O SR. LUIZ FERNANDO MORAES DA SILVA (Para expor.) - A audiência será realizada no dia 15 de junho, no auditório do Anexo I do Palácio do Planalto. Ali, na descida da N1, tem um auditório. Ela ocupará toda a parte da manhã, de 8h30 a meio-dia, e todos estão convidados para, a exemplo daqui, trazerem suas observações, suas sugestões e críticas, para que nós possamos melhorar esse projeto de lei e conseguir a aprovação aqui nas Casas Legislativas.

O SR. IZALCI LUCAS (Bloco Parlamentar Juntos pelo Brasil/PSDB - DF. Pela ordem.) - Presidente, se me permite só um complemento.

Eu acompanho essa questão da tecnologia e inovação e o que eu percebo é que nós temos sistemas que são tripartites, por exemplo, o SUS (Sistema Único de Saúde), que é União, estado e município, como o Suas também, que é área social, educação também. O que a gente percebe - eu acompanhei isso e cheguei a colocar inclusive emenda para o Ministério da Saúde para implementar ações de tecnologia, inovação, etc. - e vejo é que não há essa integração. Então, por exemplo, informações, porque o cidadão está lá no município, não está aqui na União, muito menos no estado, as pessoas moram no município, então esse sistema tem que estar bastante integrado com o dos estados e dos municípios. Nessas políticas todas, eu vejo que não acontece isso. Aqui, por exemplo, está dizendo que o Governo, quase 80%, 61% já está digital, etc., mas não adianta fazer só na União se não chegar à ponta, lá no cidadão. Essas medidas que vocês estão tomando, que são importantes, têm que levar em consideração essa integração de informação, para que haja também a proteção cibernética como informação de todos, desde o município até o estado. Eu sei que não é fácil, mas acho que esse é o nosso objetivo, principalmente na área pública.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Perfeito, Senador Izalci. Foi uma das abordagens trazidas esse ponto que V. Exa. faz com muita percuciência.

Meu querido Prof. Humberto, para que nós finalizemos.

O SR. HUMBERTO RIBEIRO (Para expor.) - Muito obrigado, Senador Veneziano.

Quero reiterar aqui o que o senhor trouxe, quer dizer, ilustrando, aproveitando a oportunidade. O Senador Izalci é um defensor dos assuntos de inovação, ciência e tecnologia. Nós e vários dos nossos colegas, interagindo sobre esse aspecto, estamos tratando de uma moeda de duas faces: existe a face da prevenção, do combate ao crime, mas há outra face, a bela face, que a nossa sociedade nunca pode esquecer, que é a face da inovação, da prosperidade trazida pela transformação digital. Transformação digital muda a relação de tempo e espaço para a sociedade. A gente produz mais, a gente agrega valor, a gente se torna mais competitivo pelo lado produtivo e a gente traz bem-estar para a nossa população através dos mecanismos digitais. Eu falo também com outro boné neste momento, na prerrogativa de diretor do Deseg, o Departamento de Segurança da Federação das Indústrias do Estado de São Paulo (Fiesp), do qual participo com muita honra.

Dois pontos, Senador, na sua pergunta que eu gostaria de agregar ao que o Brigadeiro brilhantemente já trouxe: um ponto necessário para a nossa discussão em nível de Brasil que a gente identifica, no âmbito acadêmico da Universidade de Brasília, é a questão de métrica. Que régua estamos usando? E essa questão apareceu em vários dos questionamentos e das interações. Que régua estamos usando para dizer se estamos bem ou mal? E se indeterminado, saindo do nível macro nacional ou do poder público, também no nível individual de cada instituição: qual régua usamos, qual régua usaremos?

Nesse sentido, também aqui quero repercutir um trabalho muito bem estruturado - o Dr. Carlos, do TCU, o mencionou na apresentação -, quando o TCU, através do seu Ministro Relator Vital do Rêgo, coloca um dos modelos de métrica já como um balizador, que é o CIS 8, que, se eu não me engano, é o que está vigente neste momento. É um padrão internacional muito bem-vindo. Existem outros, sob outras diferentes perspectivas, que podem complementar esse primeiro passo brilhante que já foi trazido. Esse é um ponto.

E um outro ponto também, finalizando, Senador, sobre o aspecto do papel do setor privado. Nós, inclusive, enquanto setor privado organizado, através da nossa federação, estamos anunciando na próxima semana, agora, dia 24, um laboratório de prevenção a incidentes cibernéticos na Fiesp, através do Senai, que é um dos nossos braços no Sistema S, justamente com a preocupação de iluminar a trilha do nosso jovem, da juventude brasileira. O *hacker* ético, trabalho em que podemos, Senador, não só fortalecer nossas estruturas de combate, mas prestigiar o papel, inclusive, de exportação de produtos brasileiros, cujo selo de segurança, confiabilidade, trazido pela segurança cibernética, pode nos posicionar em arenas muito mais competitivas.

A União Europeia, por exemplo, lançou agora, em fevereiro passado, um novo protocolo de exigência quanto à importação de produtos para a Europa. Já, como foi dito pelo Dr. Sabbat, a barra, quer dizer, estabelecida já num outro patamar, em que não vai ser mais simplesmente a qualidade intrínseca do produto, mas também o invólucro, o envelope, em especial, na exportação de serviços: como é que isso chega e não expõe a vulnerabilidades ou a riscos o cidadão europeu? Ou seja, se quisermos exportar precisamos estar atentos também a isso.

Como disse, são dois lados da mesma moeda. Então, corroborando, e já aproveitando para agradecer pela riqueza dessa nossa audiência pública de hoje, parabéns, Senador Veneziano, ao Senado Federal e a todos os colegas.

O SR. PRESIDENTE (Veneziano Vital do Rêgo. Bloco Parlamentar Democracia/MDB - PB) - Somos nós que agradecemos pelas participações qualificadíssimas dos senhores, a representar as entidades, enfim. Esse tema é palpitante e merece todas as nossas permanentes e reiteradas atenções.

Em nome do Presidente desta Comissão, nosso companheiro Senador Confúcio Moura, eu agradeço pela oportunidade que ele nos permite, ao lado desta equipe de excelência que nos secretaria, em nome também dos meus companheiros, Senador Izalci Lucas, Senador Wellington Fagundes e, mais cedo, o Senador Espiridião Amin, pela participação. São companheiros que, dia a dia, trabalham, como os demais outros, e estarão a deter-se nesse tema.

Quero saudar o Brigadeiro Luiz Fernando; quero agradecer à representação do nosso Tribunal de Contas, o Dr. Carlos Renato; quero agradecer ao José Luiz Medeiros, ao Dr. Arthur Sabbat; cumprimentar o Dr. Caio, o Dr. Malagutti, o Prof. Humberto, o Leonardo Ferreira, o Flávio, representando a Polícia Federal, o querido amigo Renato, correto? Eu gosto de memorizar - não estou lendo não, viu? *(Risos.)*

Enfim, quero agradecer a todos os nossos companheiros e companheiras, cidadãos brasileiros, ao Newton, Manu Silva, Camila do Vale, Felipe Chagas, Sílvio Bonilha, Crystine e Joranhezon, Letícia Luche, João da Silva, Josiane Santana, Bruna Almeida, Nathaly Santos e tantos outros que fizeram perguntas, que participaram e que demonstram as devidas preocupações, porque, de fato, aquilo que foi exposto aqui nos requer uma participação, uma interação para diminuirmos, quanto mais possamos, as fragilidades e os acessos daqueles que "terminam", entre aspas, valendo-se e se beneficiando de atitudes nada condizentes.

Eu agradeço a todos.

Muito obrigado pela distinção da presença, pela aceitação dos convites.

Estaremos muito proximamente vinculados, porque - repito - esse é um tema que requer de nós toda uma atenção especial.

A todos o meu boa-tarde.

(Iniciada às 9 horas e 15 minutos, a reunião é encerrada às 12 horas e 08 minutos.)