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

REUNIÃO
16/10/2017 - 41ª - Comissão de Relações Exteriores e Defesa Nacional

O SR. PRESIDENTE (Fernando Collor. Bloco Moderador/PTC - AL) - Declaro aberta a 41ª Reunião, Extraordinária, da Comissão de Relações Exteriores e Defesa Nacional da 3ª Sessão Legislativa da 55ª Legislatura do Senado da República.

Hoje vamos cumprir mais uma etapa do nosso ciclo de debates, cujo tema será especificamente, dentro do painel: "O Brasil e a Ordem Internacional: Estender Pontes ou Erguer Barreiras?" O tema específico deste 14º Painel será: "Terrorismo e ameaças cibernéticas no século XXI: os inimigos sem rosto."

Passo à leitura do comunicado da reunião anterior, do 13º Painel, cujo tema foi: "Lugar do Brasil em um mundo de transformações", do qual participaram como palestrantes o Embaixador Rubens Barbosa e o Secretário de Planejamento Diplomático do Ministério das Relações Exteriores, Ministro Benoni Belli.

O primeiro palestrante, Ministro Benoni Belli, elencou três grandes desafios da ordem internacional atual:

1 - o descompasso entre as regras e as instituições vigentes e a realidade de poder, muito alterada desde o final da guerra mundial;

2 - os novos desafios à ordem mundial, derivados de um sentimento cada vez mais forte de mal-estar com a globalização;

3 - como o Brasil poderá se antecipar às tendências externas e aos cenários futuros para tentar influenciar esses processos de forma a atender seus interesses e projetar seus valores nessa ordem internacional em mudança. Segundo ele, passamos de um momento de euforia, com o fim da Guerra Fria e a ilusão do fim da história, com a vitória da democracia liberal, com unipolaridade, tendo os Estados Unidos da América como única superpotência, para uma situação complexa com polaridades indefinidas - ascensão da Ásia e dos Estados Unidos -, sem condições de resolver unilateralmente os problemas da ordem internacional.

Continuando, disse ele que, se a ascensão de novos polos representará a mudança substancial, e que mudança na ordem internacional e nas instituições será esta, é questão que continua presente. Do ponto de vista do Brasil, ressaltou o palestrante, a ascensão de novos polos não significaria necessariamente abalar os pilares da ordem instituída, mas um aperfeiçoamento positivo desta, no sentido de abrir mais espaços para países em desenvolvimento, sem minar nem revolucionar essa ordem.

O debate sobre a ordem internacional mudou um pouco de foco, disse ele, em função da própria dinâmica política, eletrônica e social das potências estabelecidas, o que gerou esse sentimento de mal-estar com a globalização. Sua origem está nas mudanças do próprio capitalismo internacional, com as mudanças tecnológicas, desemprego estrutural, deslocamentos de investimentos, que, se produziram maior eficácia da economia como um todo, afetaram muitas comunidades.

Os problemas crescentes de desigualdade e desemprego são associados, muitas vezes, de maneira simplista, ressaltou o Ministro, com a globalização, com a liberalização comercial, com a presença de estrangeiros gerando, em várias partes do mundo, ascensão de movimentos populistas contrários a qualquer tipo de projeto internacional de integração, identificado com maior abertura ao mundo.

Há uma dificuldade de entender essas mudanças. Havia no Brasil a ilusão de que a simples distribuição mundial de poder, com a ascensão de novos polos, geraria uma ordem internacional melhor, mais aberta e mais estável. O debate é mais

complexo, considerou o palestrante. Não basta haver apenas multipolaridade no sentido econômico, diplomático, político e militar; é preciso fazer dessa multipolaridade algo que corresponda a uma visão do Brasil de o que seria uma ordem internacional desejável, especialmente mais cooperativa.

A política externa não é e não pode ser um monopólio do Itamaraty, afirmou o Ministro Benoni. É uma política pública, que precisa ser debatida com a sociedade. Para responder a isso, disse ele, precisamos de um diagnóstico dessa realidade internacional, saber o que está em jogo e onde nossos interesses são prioritários. A partir daí, com base na realidade interna, devemos buscar, pela via diplomática, a construção dos caminhos pela consecução dos objetivos propostos, asseverou ele.

Em resumo, disse o palestrante, vivemos uma ordem internacional em transição, com instituições ainda antigas, porém com uma realidade de poder muito mudada. Há uma multipolaridade crescente, que não é, por si só, garantia de estabilidade e de uma ordem internacional liberal aberta a potências médias, como o Brasil. Precisamos nos precaver, não concentrando nossas fichas em alguns parceiros em detrimento de outros, o que não faz sentido em uma ordem internacional que ainda não tem uma configuração definida, concluiu o Ministro Benoni Belli.

O segundo palestrante, o Embaixador Rubens Barbosa, explicou que houve, nos últimos tempos, o desenvolvimento de uma nova geopolítica com a globalização, que se aprofunda cada vez mais com o fortalecimento do regionalismo, com o fim da bipolaridade e com o importante advento da economia, do conhecimento e da inovação.

Estão ocorrendo grandes mudanças políticas e econômicas, com uma emergência do centro dinâmico da Ásia e da China voltando a ocupar seu lugar de destaque no contexto internacional, promovendo um reordenamento do processo produtivo global e crescendo a importância das cadeias produtivas globais.

Há a crise do multilateralismo não só nos órgãos internacionais, mas também regionais, com o fortalecimento do regionalismo no mundo. Nossa região, entretanto, ressalvou ele, caminha em sentido contrário, ocorrendo uma desintegração, segundo ele, regional na América do Sul.

Houve uma opção pela América Latina, que não é o centro do mundo, destacou o Embaixador, deixando em segundo plano políticas em relação aos países desenvolvidos, onde há novas tecnologias, inovação, dinamismo e fluxos de financiamento e comércio. O Brasil, apesar de tudo, ainda é uma das dez maiores economias do mundo, portanto, um *player* importante, que não pode permanecer isolado das negociações comerciais, como ficou nos últimos anos, assinando, em 15 anos, apenas três acordos pouco significativos, enquanto no mundo eram assinados mais de 400 acordos.

Para definir o lugar do Brasil no mundo, afirmou o palestrante, precisamos estabelecer o dinamismo da política externa, definir a estratégia em relação à integração regional, que está esgarçada, e em relação ao Mercosul. Precisamos ampliar os contatos na região, sobretudo com o México, que está marginalizado em nossas relações, com apenas 13% de tarifas preferenciais.

Na área política, avaliou o Embaixador, no médio prazo, os Brics podem ser importantes como projeção do Brasil no mundo, sendo necessário que definamos o que queremos dos Brics. Precisamos acelerar o ingresso do Brasil na OCDE, pela sua importância no estabelecimento de regras de governança global, usadas, lembrou ele, na solução de controvérsias em diversos fóruns.

Na área econômica e tecnológica, nos próximos anos, afirmou o Embaixador, vai se jogar o futuro do Brasil dentro dessa correlação de forças que se mostram no cenário internacional. Em primeiro lugar, afirmou ele, temos que resolver a situação econômica interna e ter uma política cambial e taxa de juros para a defesa da indústria e dos interesses nacionais, abandonando a visão ideológica da questão. Sem políticas claras para o câmbio, a taxa de juros, o Brasil dificilmente voltará a ter um poder industrial significativo. Não podemos continuar com a política de subsídios e incentivos, porque o Governo quebrou, e estamos questionados na OMC, da qual não podemos sair, para mudar a política industrial e de informática.

Outro fator é a questão da competitividade, o que, ressaltou o Embaixador, faz avultar o papel do Congresso, pela importância das reformas no processo de recuperação da competitividade no Brasil.

As reformas da previdência e tributária, se não forem feitas agora, disse ele, fatalmente terão de ser feitas no próximo Governo; caso contrário, em quatro ou cinco anos, estaremos na situação vivida pela Grécia.

Nossa reindustrialização não ocorrerá no setor têxtil, de calçados; ocorrerá na área de produtos que serão criados daqui para frente, produtos de inovação. E é aí que precisamos focar, asseverou o Embaixador.

Continuando, ele disse que desapareceu a fronteira entre a política econômica interna e a agenda externa. E, cada vez mais, a agenda externa influi nas decisões tomadas internamente.

Temos de incluir nas decisões e programas de governo esse componente externo, o que é um grande desafio para a classe política, porque a política externa não dá voto, mas o comércio exterior tem impacto sobre o crescimento e o emprego.

Precisamos, continua ele, rever a estratégia de negociação comercial, onde apostamos todas as fichas na negociação multilateral, e, com o fracasso de Doha, lembrou ele, o Brasil perdeu tempo.

Tudo isso, continua o Embaixador, está ligado à eleição de 2018, que será uma das mais importantes dos tempos modernos para o Brasil, um verdadeiro divisor de águas.

Ou o Brasil se ajusta ao que está acontecendo no mundo, ou volta à política que causou todos esses estragos, levando o País a uma posição delicada em termos de estabilidade econômica, de capacidade interna de pagamento, o que comprometerá o futuro da próxima geração, concluiu o Embaixador Rubens Barbosa.

Respondendo a questionamentos, o Embaixador Rubens Barbosa disse que o aspecto positivo da crise é que estamos começando a discutir o que interessa e que tem impacto na vida do cidadão, das empresas e na função do Estado no País.

Em contrapartida, ressalvou ele, é muito difícil ter um projeto, porque o País está dividido, dificultando o consenso.

A América do Sul, nosso entorno geográfico, está quase desintegrada e é o principal problema de nossa política externa, afirmou o Embaixador.

A questão da infraestrutura é exemplo da ausência de pensamento estratégico do Brasil. A China, lembrou ele, passou a ser o principal parceiro comercial do Brasil, e essa dependência tende a aumentar, pois minério de ferro, soja e milho são produtos essenciais para a China, e não temos nenhuma estratégia para acessos a portos no Pacífico.

Entre os países-membros da Aladi, o intercâmbio comercial representa em média apenas 16% do comércio dos países da região, enquanto, na Europa, são 40% e, no Nafta, 60%, comparou ele.

Na década de 80, a indústria, que é quem dá emprego, destacou ele, representava cerca de 25% do PIB, e hoje representa apenas 9%. Precisamos buscar a reindustrialização, focando os novos produtos que estão sendo criados. Há dez anos, o Governo fala em inovação, mas nada fez de prático para atrair investimentos.

Segundo o Ministro Benoni, respondendo também a indagações dos nossos internautas, a visão estratégica do País não é uma visão dos gabinetes de Brasília; é uma visão que precisa passar pelos Estados, pelos Municípios e pelas realidades regionais, que é onde os problemas estão dados, as oportunidades são identificadas e as soluções se apresentam. Não há como o Brasil resolver seus problemas sem pensar a inserção como parte dessa agenda de busca de soluções. Se nada fizermos para defender nossos interesses e valores, asseverou o Ministro Benoni, acabaremos tendo de aceitar regras internacionais que irão moldar a dinâmica internacional em nosso desfavor.

O desenvolvimento do Brasil está atrelado e precisa ser compartilhado com o desenvolvimento regional, pois há uma interdependência enorme que exige um projeto de integração regional. O Brasil, por seu tamanho, precisa ser um esteio desse processo, mas a defesa dos nossos interesses não pode deixar de considerar os interesses dos demais países.

O crescimento dos investimentos chineses é visto no Itamaraty como algo positivo. O importante, independentemente da origem do investimento, é que tenhamos uma visão estratégica do que queremos e sejamos capazes de carrear, carrear os recursos para atender nossos maiores interesses e necessidades, a exemplo da área de infraestrutura, finalizou o Ministro Benoni Belli.

Peço à Secretaria da Comissão que dê como lido todo o relato que acabo de ler em suas partes principais.

Como disse inicialmente, a nossa reunião de hoje destina-se à discussão de um tema extremamente atual e muito polêmico. O tema é "Terrorismo e Ameaças Cibernéticas no século XXI - os inimigos sem rosto".

Participam da reunião, como palestrantes, o General de Divisão Paulo Sérgio Melo de Carvalho, Diretor de Relações Institucionais da Rede ANSP (An Academic Network at São Paulo); o Prof. Dr. Jorges Mascarenhas Lasmar, da Pontifícia Universidade Católica de Minas Gerais; o Dr. Marcus Vinícius Reis, Coordenador-Geral de Defesa da Secretaria de Assuntos Estratégicos de Presidência da República; e o Prof. Dr. Gills Vilar Lopes, da Universidade Federal de Rondônia, os quais gostaria de cumprimentar, em nome de todos os presentes, de todos os integrantes desta Comissão, e convidá-los para fazer parte da Mesa, agradecendo antecipadamente a presença de todos. *(Pausa.)*

Gostaria, mais uma vez, de agradecer a todos os senhores palestrantes que nos honram com suas presenças na noite de hoje.

Os senhores terão 20 minutos disponíveis para fazer a explanação que desejem. Naturalmente, um tempo extra será concedido para a conclusão do raciocínio e o fecho das suas explanações. A marcação do tempo é feita naquele relógio digital ali, com os algarismos em vermelho. O tempo será dado em ordem decrescente, começando com 20 minutos e indo até ao zero.

O tema de hoje é: "Terrorismo e ameaças cibernéticas do século XXI: os inimigos sem rosto." Nós apresentamos os seguintes tópicos para serem abordados, caso os senhores palestrantes julguem conveniente: o atual terrorismo e suas ameaças; as chamadas ameaças híbridas com a utilização de redes sociais e a invasão de redes de internet; terrorismo

na era digital: segurança cibernética; o ciberespaço como um novo campo de batalha: guerra cibernética, terrorismo e segurança internacional; reações das potências e possibilidades de ações brasileiras.

Para dar início ao nosso painel, concedo a palavra ao Dr. Gills Vilar Lopes, Professor da Universidade Federal de Rondônia.

O SR. GILLS VILAR - Boa noite a todas e todos aqui presentes, aos Exmos Senadores e Senadoras, na presença do Presidente da Mesa, e demais amigos, colegas e irmãos também.

Como foi falado, eu venho da Universidade Federal de Rondônia, na Floresta Amazônica. Esse é um tema que, aparentemente, diz respeito às tecnologias muito avançadas, mas, a partir do momento em que não conseguimos criticar a forma com que essa tecnologia é aplicada, sobretudo a assuntos estratégicos nacionais, deixamos de ganhar muita força naquilo em que somos bons, que é na análise de conjectura e, consequentemente, na sua própria resolução.

O tema específico de que vou tratar aqui é um desses vários temas que, nos últimos anos, sobretudo no último lustro deste século, vem acalentando não só discussões acadêmicas, não só discussões parlamentares, a exemplo desta Comissão, mas, sobretudo, no *modus operandi* das nossas próprias agências de combate a esse tipo de ameaça, as ameaças cibernéticas e, mais especificamente, as ameaças terroristas, que bebem também desse novo ambiente que é o ciberespaço.

O objetivo aqui não é dar aula, como professor, mas ser o mais didático possível para demonstrar-lhes que a teoria que pretendo mostrar aqui um pouco na primeira parte se coaduna com a nossa prática, a nossa práxis. E, ao final - eu quero deixar muito bem claro isso -, a minha fala serve justamente para fortalecer ainda mais os órgãos, democraticamente estabelecidos, de proteção contra essas ameaças, sobretudo os órgãos de inteligência de Estado. O órgão principal do nosso sistema brasileiro de inteligência é a Abin.

Como os senhores e as senhoras podem perceber, o título da palestra é "Terrorismo e Ameaça Cibernética". Consequentemente, eu vou mesclar esses dois objetos no que a gente comumente tem chamado de terrorismo cibernético, sobretudo o terrorismo cibernético deste século XXI, já que o terrorismo cibernético é algo que já vem sendo estudado academicamente e nos âmbitos dos estudos de segurança internacional de atividade de inteligência desde os anos 80 nos Estados Unidos, por exemplo.

Então, aqui, brevemente, vou tentar demonstrar que a natureza do terrorismo, que é propagar o terror, o temor social, não é algo recente; remonta a idos e idos, mas podemos falar em termos modernos desde a Revolução Francesa. A Al-Qaeda tomou para si também um desses meandros que é levar o terror aos seus objetos, às pessoas que eles achavam que eram suas principais ameaças, muitas delas no Ocidente.

Mas, em 2001, algo muito interessante aconteceu para os estudos sobre ameaças cibernéticas. Se, depois do fim da Guerra Fria, do debruçar da cortina de ferro, em 1989, 1991, os Estados começam a ter novas ameaças que não são aquelas simplesmente que advêm do Estado, mas também dos grupos terroristas e não estatais, nós percebemos que, com o 11 de setembro de 2001, os Estados Unidos, com sua guerra ao terror, tentam buscar novas fontes de ameaça ao seu Estado, a sua soberania nacional. Dentre essas novas ameaças, está justamente a internet.

Não vamos diferenciar aqui tecnicamente internet de ciberespaço, mas digamos que a internet é o carro forte do ciberespaço. Nós temos as redes de telefonia móvel também fazendo parte dos ciberespaços. Então, a internet é apenas a ponta desse grande *iceberg*, que logicamente esconde outros locais ocultos e outras formas de possibilidade de bens e de malefícios para a humanidade.

Com o 11 de setembro, o ciberespaço começa a ser um objeto, digamos assim, de securitização por parte dos Estados. Há perguntas como: até que ponto uma organização terrorista pode se organizar no âmbito da internet e o Estado não ser capaz de identificar? Até que ponto uma célula, um indivíduo, um lobo solitário, nos dizeres das agências de inteligência, consegue se utilizar das mesmas tecnologias que nós, civis, utilizamos, como o GPS, um aplicativo de geolocalizador para identificar uma infraestrutura crítica?

Da mesma forma que utilizamos essas benesses da internet, consequentemente aqueles cuja natureza humana nos dizeres hobbesianos é imutável, no sentido de, se ele vai fazer o bem, ele também é propenso a fazer o mal... E utilizar também a internet demonstra que há muitas possibilidades para que isso ocorra.

O terrorismo, se percebemos, até o 11 de setembro e, consequentemente, com a criação do que nós convencionamos a chamar de Estado Islâmico ou Daesh ou Isis, mas sobretudo, em 2003, 2004, o *modus operandi* era o mesmo: homens-bomba, explosões, decapitações. Eu me lembro disso lá na Revolução Francesa: guilhotina e decepamentos em público para chocar, para levar o terror. Então, o *modus operandi* continua o mesmo.

O que acontece é que, em 2013, 2014, o Estado Islâmico surge com uma nova proposta, um novo *modus operandi*: vamos levar, sim, o terror, continuar fazendo com que a natureza do terror persista, mas vamos impulsionar nossa mensagem,

vamos nos utilizar das redes sociais, da internet para que isso ocorra. A utilização das redes sociais com fins terroristas, digamos assim, é um novo mote desses estudos de terrorismo cibernético.

Só que, ao analisar também lá na Floresta Amazônica, em literatura e ao visitar algumas instituições dentro e fora do Brasil, nós percebemos que o conceito de terrorismo cibernético está muito defasado para o século XXI, sobretudo para esta segunda década do século XXI, ainda mais com o Estado Islâmico, porque terrorismo cibernético, na literatura... Quando eu falo em literatura, o conceito, teoria, são esses conceitos que são colocados em políticas públicas, porque é a partir de discussões como essa que isso é positivado, que isso vira lei. Mas, se o conceito, de certa forma, não está se encaixando com a realidade, consequentemente, a política pública e as ações dos órgãos competentes também não vão estar.

E o conceito de terrorismo que até então se tinha, e durante o próprio advento do Estado Islâmico vem ocorrendo, no meu ponto de vista, é muito defasado, porque pensem aí: como é que pode um terrorista talibã ou qualquer que seja, na sua pequena caverna encrustada lá no Paquistão, no Irã, ou no Iraque, que mal sabe mandar um *hello, mommy,* vai conseguir acessar redes protegidas e altamente criptografadas de um sistema informatizado do Pentágono ou daqui mesmo do Brasil?

Então, quando se falava em terrorismo cibernético, que eu chamei de 1.0, é justamente essa imagem de um terrorista altamente didático, altamente patrocinado pelo seu grupo, que vai trazer danos físicos a uma rede de computador ou um roubo de senhas, que, enfim... Se a gente pega os dados oficiosos das redes do Pentágono, vamos perceber que eles têm milhões de tentativas de acesso a suas redes altamente protegidas. Uma ou duas talvez sejam de alguma pessoa que se diga pertencente a algum grupo terrorista. Mas, sistematicamente, atribuir uma tentativa ou mesmo aferir algum dano a uma rede altamente protegida de um Estado? Acredito que esse conceito não se aplica tão bem ao conceito de terrorismo cibernético. E é esse conceito que nos vem sendo trazido à baila para aplacar as políticas públicas, sobretudo as políticas de defesa nacional e as políticas de segurança cibernética de vários países. Não vou citar países, mas, fazendo uma análise comparativa, a gente percebe que o conceito de terrorismo cibernético é justamente atrelado a ataques cibernéticos.

E é aí que surge, como eu falei para vocês, esse conceito de infraestrutura crítica, ou seja, algumas usinas, alguns serviços oferecidos pelo Estado, cuja interrupção colocaria em risco a sobrevivência do próprio Estado ou a sobrevivência de determinada parte idiossincrática do próprio Estado. Então, um terrorista cibernético seria capaz de fazer esse dano bem avulso.

E aqui, como nós não temos - pelo menos até onde eu saiba - uma definição de terrorismo pelas próprias Nações Unidas, o que a gente tem é uma tentativa de epitetar determinadas ações como terroristas. Com base nisso, temos percebido que a nossa lei antiterrorismo bebe também um pouco dessa fonte do terrorismo cibernético 1.0.

Não vamos ler a lei aqui, logicamente, mas eu queria só enfatizar algumas partes da lei antiterrorista brasileira como a questão da teoria da literatura, que se coaduna com a prática. Então: "Terrorismo consiste na prática de atos previstos neste artigo com a finalidade de provocar o terror", ou seja, a natureza é a mesma: provocar terror, temor. "São atos terroristas sabotar o funcionamento, apoderar-se com violência, grave ameaça à pessoa ou [e aí entra o nosso caso mais específico] servindo-se de mecanismos cibernéticos". Ou seja, o ciberespaço aí não é um fim em si mesmo, mas é um meio pelo qual o terrorista irá se utilizar para levar o seu temor, o seu terror. E, no final do inciso IV deste art. 2º, ele vai nos falar sobre as infraestruturas críticas ou estruturas estratégicas, que são aquelas estruturas essenciais para os serviços públicos do Brasil. Esse entrelaçamento entre teoria e prática a gente continua vendo não só no Brasil, mas pelo mundo afora.

O que eu poderia chamar de Terrorismo Cibernético 1.0? Ou seja, já é um avanço em relação a essa questão de atrelar terrorismo cibernético a um ataque cibernético feito por um *hacker* superdotado ou um grupo de *hackers* superdotados. E esse exemplo eu trago justamente da mais do que necessária e recém-aprovada, digamos assim - isso foi em 2016 -, Política Nacional de Inteligência.

A gente percebe que, em 2013, com as revelações lá do Edward Snowden de que o Chefe de Estado brasileiro foi espionado... Em que medida isso fere a soberania nacional? Lanço essa pergunta para vocês. Mas, em 2013, a PNI não existia ainda, estava engavetada. O que acontece é que, de 2016 para cá, do ano passado para cá, com a PNI em pauta, os órgãos de inteligência, a nossa Agência Brasileira de Inteligência tem um respaldo legal muito maior para agir naquilo que a gente chama de terrorismo cibernético.

Quando eu falar aqui em atividade de inteligência, em órgãos de inteligência, estamos falando hoje no regime democrático de direito, uma organização que se pauta pela dignidade da pessoa humana, por outros conceitos, abertos ou não, elencados pela carta das Nações Unidas.

Mas a Política Nacional de Inteligência, que já estava pronta há mais de dez anos, previa justamente, como coloquei ali, algumas das principais ameaças ao Estado brasileiro. Ela faz uma análise de conjuntura.

Logicamente que nós temos outros problemas tão importantes quanto: a questão da Amazônia Azul; a questão da Amazônia Verde, de onde eu venho mais uma vez falando; e a questão do terrorismo. E a PNI traz o conceito de terrorismo mais amplo, que se coaduna, de certa forma, com o inciso XXXIII do artigo 5º da nossa Constituição. Mas o que é mais interessante é que há dez anos, mais ou menos, a PNI já trazia os ataques cibernéticos como ameaça à soberania nacional.

Diante das alegações do Snowden, o que será que a Abin poderia ter feito? Não sei. Ela pode fazer tudo aquilo que a lei permite. Então, o fato de positivar algo como terrorismo e especificamente como terrorismo cibernético - e um dos meus objetivos aqui é demonstrar a vocês a necessidade de se positivar o que é terrorismo cibernético, sobretudo para uma era que se chama "era da informação", para uma sociedade em que vivemos chamada de "sociedade da informação" -, no meu ponto de vista, é fulcral, logicamente, levando-se em conta os ditames do Direito Internacional, dos direitos humanos e dos direitos fundamentais da nossa Constituição.

É um passo muito grande dado pela PNI, mas, ao mesmo tempo, ela atrela as questões de terrorismo e ciberespaço com as questões de infraestrutura crítica, ou seja, de algo físico que vá ser danificado.

O meu segundo grande objetivo aqui, o que eu quero demonstrar a vocês é que o Terrorismo Cibernético 2.0 não perde a essência da proteção às infraestruturas críticas ou estruturas estratégicas nacionais, mas leva também em conta uma das partes muito relegadas pela literatura, enfim, que é a questão do terror, do temor e do dano não só físico, mas também psicológico.

O que é um avião caindo no panteão da economia mundial, senão um símbolo? Além das mortes e tudo mais. Então, a questão simbólica por trás do terrorismo, que por si só é um fenômeno internacional - e, no nosso caso, transnacional -, enseja também um temor psicológico. E essa essência é que, no meu ponto de vista, algumas discussões, algumas políticas públicas, algumas leis não têm levado em consideração.

Então, em 2014, quando o Estado Islâmico se autoproclama Estado Islâmico da Síria e do Iraque, ele começa a se utilizar da internet para propagar... Vejam só, pensem só comigo: utilizando a internet, você não vai causar nenhum dano a rede nenhuma, você não vai roubar dado nenhum. Você vai simplesmente propagar um terror que é psicológico, que tem um efeito psicológico muito forte.

Nesse quesito, os objetivos do Estado Islâmico, quer queiramos ou não, foram alcançados. Eles ficaram notórios para todo mundo. Esse rapaz aqui, o Bradley Manning, um dos que se utilizou do WikiLeaks para vazar documentos e tudo o mais, traz um dos relatos mais interessantes sobre a atuação do Estado Islâmico que eu já vi. Ele trabalhou no Afeganistão e na Síria e falou: Olha, os Estados Unidos estão saindo daqui e estão deixando um monstro. E esse monstro está sabendo se utilizar dos artefatos do século XXI, das superproduções videográficas por meio das redes sociais, da promoção de vídeos e tudo o mais.

O Bradley Manning, como um agente de inteligência que lutou *in loco* onde o Estado Islâmico nasceu, coloca que um terço do poder do Estado Islâmico, ao contrário da Al Qaeda, do Boko Haram, até então era justamente se utilizar das redes sociais de uma forma bem sedutora, tanto para os jovens que queriam uma aventura quanto para um adulto de consciência já formada que não estava satisfeito com o sistema no qual estava vivendo.

Nesse sentido, o Terrorismo Cibernético 2.0 tem a mesma natureza de todos os terrorismos: levar o terror social, o temor, o pavor a um determinado indivíduo, a um grupo de indivíduos, etnias, etc. O seu *modus operandi* continua sendo o mesmo: explosões, decapitações, todas aquelas coisas que vemos e abominamos, mas eles se utilizam sobretudo do ciberespaço para se comunicar, para propalar uma ideia, enfim, para se esconder atrás daquilo que as forças policiais, as forças de inteligência não conseguem ver. E o principal veículo, ao contrário dos antigos terrorismos, que era o jornal e o rádio... Hoje temos uma coisa totalmente diferente para impulsionar ainda mais esse terrorismo cibernético, que são as redes sociais e a internet. Se, no rádio, temos uma pessoa falando para várias; na TV a mesma coisa; na internet, todos falam para todos. É um fenômeno social que até então não se via, e isso foi utilizado de maneira muito pragmática por esse tipo de grupo terrorista. Por conseguinte, acabou transbordando para outros grupos, como o Boko Haram, o Al-Shabaab e por aí vai. Esse é mais ou menos o conceito de Terrorismo 2.0 que eu queria trazer aqui e que a literatura, pelo menos da minha área, ainda não tem debatido a fundo.

Aqui nós podemos ver como uma breve análise de redes sociais nos demonstra que alguns *tweets*... No caso específico, o mais escuro é sobre o Estado Islâmico, e o cinza mais claro é sobre os outros, Al-Shabaab, Boko Haram e tudo o mais, para demonstrar o patamar de quase 100 mil *tweets* por dia. Ou seja, se antigamente as pessoas não sabiam nem o que era terrorismo, hoje nós estamos começando a falar sobre esses assuntos de uma maneira muito corriqueira, os noticiários mostram que o Estado Islâmico decapitou, etc. Então, se tornou muito "natural" saber que esse tipo de grupo existe e saber que eles existem no âmbito das redes sociais.

Aqui já é uma forma de contra-argumentar e contra-atacar justamente a principal característica do Estado Islâmico e dos grupos terroristas que se utilizam das redes sociais. Trago um exemplo, para não dizerem que eu venho aqui dizer que temos que invadir todas as redes sociais, todas as contas de Twitter. Nada disso! Basta, no meu ponto de vista, um sistema de vigilância sistematizado por meio do Estado, pautado por respaldos legais, jurídicos, quando for o caso, mas para demonstrar até que ponto pode agir um órgão de inteligência; se ele vai ficar o dia todo fazendo análises em fontes abertas, em jornais abertos para subsidiar a tomada de decisão estratégica, ou se ele pode ser mais proativo, no sentido de ir atrás de onde as conjecturas, as análises que eles têm feito os levam a atuar nas redes sociais.

E um exemplo muito simples dessa cultura de combate ao terrorismo cibernético foi feito na França.

(Soa a campainha.)

O SR. GILLS VILAR - Na França, nós pudemos ver que houve uma campanha muito forte, sobretudo depois das mortes lá em relação ao Charlie Hebdo e, consequentemente, depois daqueles atentados. E o governo francês lançou-se dos próprios meios que o Estado Islâmico estava utilizando. Criava redes sociais oficiais para demonstrar o outro lado também: "Você vai ficar matando pessoas, os seus próprios companheiros, compatriotas?" "Seus familiares moram aqui. Você vai para lá para lutar contra aqueles que lhe criaram?" Enfim, é uma certa cultura antiterrorismo cibernético que a França fez por meio desse *site*, colocando *links*, telefones, para que as pessoas que estão pensando em seguir o Estado Islâmico, em servir o Estado Islâmico ligassem para lá e também pudessem obter orientações.

No âmbito do exército britânico, criou-se um departamento específico para atuar nas redes sociais.

E, aqui no Brasil, o que eu tento fazer um pouco lá no Norte do País é trazer essas questões de ameaças cibernéticas para serem discutidas com estudantes não só da Ciência da Computação, de Ciências Exatas e da Informação, mas, sobretudo, com estudantes de Ciências Sociais, Ciência Política, Relações Internacionais e Direito. É o que a gente chama aí de Relações Internacionais Cibernéticas.

Agradeço pela fala e estou à disposição de todos.

O SR. PRESIDENTE (Fernando Collor. Bloco Moderador/PTC - AL) - Muito obrigado ao Dr. Gills Vilar Lopes, Professor da Universidade Federal de Rondônia, pela sua exposição.

Gostaria, antes de passar a palavra para o nosso próximo palestrante, de agradecer as presenças sempre honrosas de S. Exªs o Embaixador da Itália, Sr. Antonio Bernardini - muito obrigado pela presença de V. Exª -; o Embaixador do Catar, Sr. Mohammed Alhayki - muito obrigado a V. Exª pela presença -; o Embaixador da Angola, Sr. Nelson Manuel Cosme; o Embaixador do Azerbaijão, Sr. Elkhan Polukhov - seja muito bem-vindo -; o Embaixador da Polônia, Sr. Andrzej Braiter - seja muito bem-vindo -; a Srª Embaixadora Gisela Padovan, do Ministério das Relações Exteriores, Chefe da Assessoria de Assuntos Federativos e Parlamentares do Ministério; o Ministro Conselheiro da Embaixada da Espanha, Sr. José Manuel Pascual García; o Ministro Conselheiro da Embaixada da Itália, Sr. Filippo La Rosa; o Ministro Conselheiro da Embaixada do Irã, Sr. Morad Ali Gholami Nohouji; a Engenheira de Sistemas de Informática da Embaixada do México, Srª Cynthia Margarita Herrera; e, sobretudo, a presença de S. Exª a Srª Presidente da Comissão de Relações Exteriores e Defesa Nacional da Câmara dos Deputados, Deputada Bruna Furlan, que sempre nos brinda com a sua presença na apresentação dos nossos painéis.

Passo a palavra agora ao Prof. Dr. Jorge Mascarenhas Lasmar da Pontifícia Universidade Católica de Minas Gerais.

O SR. JORGE MASCARENHAS LASMAR - Exmo Senador Fernando Collor, em nome do qual eu cumprimento a todos da Mesa. Srs. Senadores embaixadores, oficiais e demais convidados aqui presentes, boa tarde.

É extremamente importante discutirmos um assunto tão atual como esse, e meu papel aqui será de dar uma visão um pouco mais geral e ampla sobre o fenômeno.

Inicialmente eu gostaria de começar com o entendimento de o que é o ciberterrorismo. Essa é uma discussão extremamente longa, em que não há um consenso. Nós podemos classificar conforme as intenções ou conforme as ações que acontecem, mas, para efeitos da apresentação, vamos entender o ciberterrorismo como o uso politicamente motivado de computadores como instrumentos ou alvos de grupos ou indivíduos terroristas engajados em violência para influenciar uma audiência.

É importante entender bastante bem essa definição, porque ela vai além do simples ciberataque. O que nós temos de entender é que a internet se desenvolve, a partir das décadas de 80 e 90, como um meio de comunicação extremamente dinâmico, que também, por sua vez, é capaz de oferecer anonimidade, rapidez e amplo alcance através do globo, a um custo de acesso extremamente baixo. O problema é que essa mesma tecnologia não só pode como tem sido explorada para o caso de terrorismo.

E aí precisamos entender que o terrorismo é muito mais do que simplesmente o ataque terrorista ou o ataque cibernético. A ação terrorista compreende uma série de atos interconectados que acontecem tanto antes quanto depois do ataque.

É importante entender que todas essas fases também podem acontecer dentro que nós chamamos de ciberespaço. Por isso, o ciberterrorismo deve ser entendido como um fenômeno mais amplo do que simplesmente a sua relação com ciberataques específicos. Por exemplo, os terroristas têm utilizado, os grupos terroristas têm utilizado a internet para atos de comunicação, coordenação, propaganda e financiamento, radicalização, recrutamento, planejamento, coleta de informação, treinamento, incitamento à violência, ataque, e mesmo apoio material ao próprio ataque.

Como o nosso tempo é curto, eu vou centrar em seis pontos principais: a propaganda, compreendendo aqui também a instância de recrutamento; o financiamento do terrorismo; o treinamento virtual; o planejamento através da internet; a execução dos ataques; e a questão da comunicação.

Quanto à propaganda, ela pode assumir diversas formas. Ela se dá através de comunicações e instrumentos de multimídia, que podem dar instrução ideológica, explicação e justificativas para atos, ou mesmo promoção da atividade terrorista, sempre com conteúdo que promove a violência e a promoção de retórica extremista. Ela se dá através de revistas eletrônicas, tratados, arquivos de vídeo e áudio, e mesmo jogos eletrônicos desenvolvidos para esses grupos. O seu conteúdo é distribuído em *websites*, *chat rooms*, fóruns, revistas *online*, redes sociais, distribuição de vídeos e arquivos, entre outros.

É preciso entender que a produção desse material é extremamente profissional e, além de ser direcionada em audiências gerais, também costuma ser desenhada para audiências específicas e pode ser usada como instrumento de manipulação psicológica.

O que nós vemos aqui na imagem é a maneira pela qual os recrutadores virtuais do Estado Islâmico costumam atuar. Em um primeiro contato, eles buscam os seus alvos e os recrutadores respondem àqueles que tentam encontrar o grupo terrorista. Em um segundo momento, criam-se microcomunidades em que se mantém um contato mais constante e direto com aquele alvo, e ele é encorajado a se isolar de influências externas; evitar, por exemplo, que ele procure um *share*, procure outras pessoas para discutir as suas ideias. No terceiro momento, então, aquilo restringe ainda mais para comunicações em canais privados. E, finalmente, quando os recrutadores estão satisfeitos, eles identificam e encorajam aqueles alvos que eles julgam estarem aptos para realizar atividade terrorista, seja promovendo ativismo nas mídias e redes sociais, seja participando de viagens para se ingressar ao grupo e suas atividades, ou até para cometer atos de terrorismo.

É importante destacarmos que nós não estamos longe dessa ameaça. Por exemplo, aqui, no Brasil, nós tivemos o caso de uma adolescente do Pará em que há uma suspeita forte de que ela foi recrutada através da internet e teria viajado ao Estado Islâmico, via Marrocos e Istambul, para se juntar ao grupo. Ou podemos pensar também na própria Operação Hashtag aqui, no Brasil, em que, pelos autos do processo, verificamos que vários dos indivíduos foram recrutados e passaram por um processo bastante semelhante ao de recrutamento.

O financiamento na internet acontece de diversas maneiras diferentes. Ele pode se dar tanto por maneiras legais ou ilegais e é centrado principalmente em dois pontos: a coleta de fundos, que pode ser feita através de pedidos diretos de ações humanitárias, comércio ONGs, exploração de ferramentas de pagamento *on-line;* ou mesmo por meio de meios fraudulentos - fraudes em cartão de crédito, roubo de identidade, fraudes no eBay etc. Mas o ponto importante também é o uso da internet para transferência de fundos terroristas. Um caso interessante é o uso de jogos eletrônicos, como o Second Life, para fazer a transmissão de fundos sem detecção.

O treinamento. Dada a distância do mundo ocidental para regiões de conflito, esses grupos têm incentivado o treinamento dentro dos próprios territórios em que os indivíduos são nacionais, e esses instrumentos são encontrados na internet com plataformas que distribuem guias práticos, vídeos e áudios com instruções, informações e conselhos.

Existem, por exemplo, programas de *fitness*, programas de exercício, programas de como manusear armas de fogo e até mesmo confecção de artefatos explosivos. Esses materiais chegam a contar, inclusive, com materiais de contrainteligência, criptografia e técnicas de anonimato na internet.

O planejamento. O planejamento tem encontrado na internet uma fonte enorme para a coleta de informações em fonte aberta, mas também tem sido usado como apoio e direção aos atentados. Um exemplo é o *software* Mujahideen Secrets, que usa uma criptografia avançada de 256 bits, chaves de criptografia variáveis de *stealth cipher* e sistemas de mensagem instantânea.

Aqui também nós relembramos que o Brasil não está imune a esse tipo de ameaça. Há alguns anos tivemos, em São Paulo, o caso de um suspeito de participar como moderador e controlador de operações em websites, através do uso exatamente do programa Mujahideen Secrets. Ele também atuava, segundo a Polícia Federal, no financiamento ligado à rede Al-Qaeda.

A Polícia Federal conseguiu prender o suspeito quando ele estava com o seu computador ligado e logado no programa para evitar que o sistema de criptografia impedisse o acesso aos arquivos pela Polícia.

Finalmente, a questão dos ataques terroristas em si. Aqui nós temos de separar o ciberataque propriamente dito e também os chamados ataques ciberassistidos. Isso é muito importante. Nós temos que ataques tradicionais têm sido facilitados pelas tecnologias de informação. Por exemplo, no atentado de Paris, durante o cerco ao Bataclan, o terrorista começou a assassinar as vítimas assim que ele percebeu, pelo Twitter, que as pessoas estavam descrevendo que as agências de operações especiais da França estavam cercando o teatro e estavam se preparando para entrar nele.

Em Mumbai, nós tivemos outro caso terrível. Uma das vítimas no Hotel Taj se escondeu e conseguiu, através das mídias sociais, entrar em contato com uma repórter e descrever o que via. Por essa descrição, os terroristas viram, descobriram onde essa vítima estava se escondendo, retornaram ao local e a executaram.

As cenas que nós vemos também no atentado em Nairóbi, no Westgate Mall, mostram claramente que os terroristas consultaram e utilizaram o telefone celular durante o sítio para poderem conseguir informações externas. Estavam sendo dirigidos por fontes externas. Então, nós não podemos esquecer que também as ameaças tradicionais podem fazer-se valer dos instrumentos e tecnologias cibernéticos.

Além do ciberataque propriamente dito, nós temos aqui ataques sofisticados, de alta tecnologia, em que nós temos diversos métodos diferentes. Por exemplo, o ataque eletrônico, que são acessos aos aparelhos eletrônicos para obter informações, interferir em processos ou construir bases para outros ataques; a subversão de cadeia de produção, em que a tecnologia é alterada para facilitar ataques futuros ou interferir com serviços; as operações em redes e operações psicológicas.

Nós temos de entender também que os efeitos podem ser bastante diversos. Nós temos desde operações com perfil mais discreto, apenas de coleta de inteligência com operações de acesso, passando por operações de ciberinterrupção, em que se interrompe o fluxo de informação do sistema ou função do sistema de informação e, em um pior cenário, podemos chegar a um ciberataque em que eu teria efetivamente o uso da força e a provocação de danos. Esses danos, por sua vez, podem ser tanto físicos - como, por exemplo, se pensamos em alteração de sistemas de transporte, de sistemas de escada que controlam grandes maquinários etc. -, mas também não podemos esquecer dos efeitos de sintaxe, que são aqueles ataques à lógica da informação, adiantamento ou comportamento imprevisível do sistema. Aqui as eleições do Trump e as suspeitas de implantação de informações falsas nos lembram, por exemplo, da importância dos efeitos de semântica e dos efeitos de semântica, que são aqueles ataques à confiança do sistema e da própria informação, causando dano ao processo decisório em si.

É importante destacarmos também que alguns grupos já possuem unidades ciberterroristas. O próprio Estado Islâmico possui diversas entidades de ciberataque. Elas se uniram recentemente, em março de 2016, no chamado Ciber Califado Unido, que conta não apenas com suas operações corriqueiras, mas também com uma grande rede de pessoas que não pertencem propriamente ao Estado Islâmico, mas simpatizam com suas causas e, portanto, também tentam promover ataques.

Aqui é importante lembrarmos que, apesar de haver uma discussão, uma suspeita de que eles ainda não possuem tecnologia para ataques de maior escala ou sofisticação, eles já têm feito diversos ataques menores, e um deles, inclusive, novamente, envolve o caso brasileiro. Num período próximo à realização das Olimpíadas, o grupo Ciber Califado divulgou a chamada Kill List, uma lista com mais de mil nomes, com nomes, endereços eletrônicos, senhas e detalhes de diversas pessoas e diversos oficiais do mundo inteiro. Nessa lista, havia o nome de 50 brasileiros, e o Estado Islâmico sugeria aos seus seguidores que utilizassem essa lista para cometer assassinatos contra aquelas pessoas.

Quanto aos canais de comunicação, a internet também prevê uma série de canais diferentes como, por exemplo, os protocolos de Voz sobre IP, que apresenta uma dificuldade grande para os serviços de inteligência, já que não se cobra normalmente por ligação, mas por mensalidade, o que traz uma dificuldade nas investigações de chamadas específicas; além da possibilidade do uso de instrumentos de alteração do IP e de criptografia; *e-mails* em que são utilizados técnicas de anonimato, como a famosa técnica de salvar o *e-mail* e não enviá-lo, por exemplo; serviço de mensagens e de *chat rooms*, em que eu não tenho registro de comunicações - às vezes, o registro é feito inicialmente para entrada, mas esse registro é provido pela própria pessoa que entra, e a conversa em si não é registrada; nuvens e serviços de acompanhamento de arquivos, em que técnicas como criptografia, anonimato, *peer-to-peer* ou protocolos FTP também têm dificuldade enormemente na parte de inteligência e investigação; instrumentos de criptografia, que são utilizados tanto *at rest*, nos instrumentos físicos, quanto *in transit*, no momento da transmissão, da informação; e até mesmo o uso de redes *wireless*, sem fio. O uso de redes compartilhadas pode trazer também problemas para precisar e identificar quem está fazendo aquele acesso específico. O que é mais preocupante é a existência de novas técnicas como o uso de rádio de alta frequência e de alta performance que transmitem informações diretamente de um computador para outro sem passar por servidores, dificultando enormemente a interceptação e a vigilância.

Assim, para concluir, nós temos que ter em mente que o uso terrorista da internet é um problema real, amplo e que acontece através das fronteiras, em diversas fases que vão muito além do que o mero e simples ciberataque. A resposta a essa ameaça exige uma cooperação integrada entre diversas agências e mesmo entre os países, já que se trata de uma ameaça que ocorre transnacionalmente. Deve-se também chamar a atenção para a importância da cooperação com o setor privado.

E, finalmente, para terminar, é preciso destacar que nós temos observado cada vez mais uma convergência entre o crime e o terrorismo. Isso também se reflete no ciberespaço. Nós temos observado cada vez mais uma convergência entre o chamado cibercrime e o ciberterrorismo.

Obrigado.

O SR. PRESIDENTE (Fernando Collor. Bloco Moderador/PTC - AL) - Muito obrigado ao Prof. Dr. Jorge Mascarenhas Lasmar, da Pontifícia Universidade Católica de Minas Gerais. E

Passo a palavra agora ao Dr. Marcus Vinícius Reis, Coordenador-Geral de Defesa da Secretaria de Assuntos Estratégicos.

O SR. MARCUS VINÍCIUS REIS - Boa noite a todos. Eu gostaria, primeiro, de agradecer ao Senado Federal, em nome do Presidente Fernando Collor. Queria agradecer também à Presidente, Deputada Bruna Furlan - muito obrigado -, e a todas as autoridades aqui, embaixadores e embaixadoras, pela oportunidade de a gente estar discutindo esse tema tão importante. A minha apresentação até coincide um pouco, tem um caráter um pouco complementar em relação ao que o Prof. Gills e o Prof. Lasmar falaram. Eu vou falar um pouco sobre o combate a essa nova forma de terrorismo, que é o ciberterror.

O ciberterror está muito relacionado ao terrorismo do século XXI. Ainda que ele não tenha se iniciado no século XXI, ele tem muito a ver com essa sociedade da informação em que a gente vive hoje. Então, as características do terrorismo do século XXI são o terror que dá impacto, o terror de mídia, o impacto sobre os alvos civis. Essas organizações terroristas, associações terroristas estão preocupadas com alvos civis. Antigamente, o terrorismo visava amedrontar o Estado, através de ataques aos seus membros, às pessoas que trabalhavam para o Estado, seus policiais, seus militares. O terrorismo do século XXI visa a alvos civis.

A questão das armas de destruição em massa também é um fator novo. Ou seja, a tecnologia vai ficando acessível não só para os Estados e para as organizações; para os grupos ilegais, essa tecnologia também começa a ficar mais acessível. E essa é uma preocupação muito delicada nessa nova era da nossa sociedade.

O caráter de descentralização, principalmente depois do 11 de setembro. As organizações antigamente mostravam sua cara. Era uma estrutura hierárquica, organizada. Você, quando queria negociar com determinada organização, sabia quem era o líder daquela organização. Hoje, não; elas são descentralizadas. Elas atuam nas sombras; a gente não enxerga essas organizações. E isso vai ter impacto no combate. A dificuldade de o Estado combater uma organização dessa é gigantesca.

Na questão do ciberterror, a gente vai ver que é o uso dessas novas tecnologias para cometer atos que vão assustar a sociedade da mesma forma como se fosse derrubar um edifício, como se fosse explodir uma bomba.

Sobre os aspectos atuais o Prof. Gills já falou, nós temos uma legislação que cita a sabotagem por intermédio do uso de meios cibernéticos. Isso está na nossa legislação. O mundo é um ambiente propício para essa forma de ameaça à sociedade. Nosso mundo é interconectado. Todo mundo depende de uma rede de dados, da internet, de um sistema computacional - bancos, escolas, sistemas de saúde, todos nós dependemos da computação, da informática hoje em dia. Isso traz uma simetria que é vantajosa para essas organizações. Se a gente pensar num combate assimétrico, de um Estado, por intermédio de suas Forças Armadas, contra outro Estado, isso é uma coisa; essas novas ameaças se apresentam através de uma relação que não é de Estado contra Estado - às vezes até é, mas a gente não consegue enxergar a cara do outro Estado. A gente está vendo um grupo subnacional, a gente está vendo uma pessoa operar e a gente não enxerga lá a farda daquele militar.

Excesso de mão de obra. Hoje em dia, para esses grupos ilegais, recrutar é muito fácil. O mundo tem um excesso de mão de obra na área da informática, e isso é essencial para essas organizações recrutarem pessoas.

Dificuldade em controlar o ciberespaço. É muito difícil para os Estados controlar esse ciberespaço. O ciberespaço é diferente deste espaço que estou vendo aqui, esta sala delimitada por paredes que eu consigo controlar - eu consigo, através da Polícia do Senado, controlar esta sala; o ciberespaço, não. A gente não enxerga isso.

As nossas infraestruturas críticas. O mundo ainda não tem uma proteção adequada para suas infraestruturas críticas. Isso é muito importante. Essas infraestruturas estão relacionadas a toda a infraestrutura que é importante para a sobrevivência da sociedade. De bancos a sistemas de abastecimento, sistemas de transmissão de dados, Receita Federal, etc., tudo depende de uma rede de dados atualmente. E nós vamos perceber também que esse é um problema que às vezes ultrapassa a

segurança pública. Ele vai para a segurança nacional, ele vai para a área de defesa. A gente vai ver que tem de haver uma relação, uma inter-relação entre a nossa segurança pública e o setor de defesa.

Então, o ciberespaço tem essas características. É uma dimensão intangível. É diferente do ambiente operacional em que as Forças Armadas estão atuando usualmente. "Ah, a gente vai atuar no espaço tal, no Estado tal. Aqui tem um rio, aqui tem montanha." Isso é difícil, é totalmente diferente, é um espaço intangível. Ele é produto da ação humana. Pela primeira vez, um ambiente foi criado pelo homem; o ambiente, o ciberespaço é um produto da ação humana.

A questão da transversalidade. Eu não consigo... Um ataque cibernético não vai só perturbar o Estado de maneira direta. Ele é transversal: eu posso atacar o sistema militar, o sistema de escola, de saúde, de abastecimento, os aeroportos. Ele é transversal. E isso vai criar uma consequência no combate. O combate não pode ser o combate do passado, em que o criminoso comete um crime, ou um Estado invade o nosso e a gente vai só com as nossas Forças Armadas, só com as nossas polícias atuar nesse espaço. Esse espaço vai demandar a atuação de outros órgãos do Estado - órgãos que mexem com informação. Então, não é mais um espaço característico somente do combate da Polícia Federal, ou das polícias civis, ou das Forças Armadas. Ele vai exigir uma comunicação interagencial entre diversos órgãos do Estado, e inclusive órgãos privados também - por que não? Os bancos são muito bons nisso. Os bancos conseguem atuar com os Estados. Os bancos têm muita informação. Sistemas de dados privados de lojas... Então, a sociedade tem de começar a se preocupar com essa questão da operabilidade nesse novo ambiente.

O ciberespaço é global, ele não é local. Isso também muda tudo. Aquela visão antiga da soberania nacional tem de ser modificada. Um terrorista que utiliza arma cibernética através de um computador no Paquistão, que vai invadir uma rede de dados na Itália, e que de repente foi contratado por uma organização que está na África... Os Estados têm de conversar, porque as informações estão transitando em diversos Estados. Os Estados têm de ser ágeis. Essas organizações são ágeis. As compras, o recrutamento, tudo é ágil. Essas organizações já conseguem atuar nesse novo ambiente com uma agilidade incrível. Os Estados têm de aprender a atuar nesse ambiente. E aí a gente vai ter de rediscutir a questão da soberania, como é isso, como a gente quer atuar. A gente tem de atuar de maneira global. Então, o ciberespaço vai envolver os bancos, redes públicas, redes privadas, sistemas de transporte, energia, saúde, redes de educação, sistemas militares e segurança pública. Tudo depende desse ciberespaço. Tudo depende desse ambiente hoje em dia.

Eu fiz esse desenhozinho. O ciberespaço está ali embaixo. A nossa vida pública está nele. A nossa vida privada está nele. E a vida das organizações está nele. Existem ameaças a ele - o cibercrime. Os crimes cometidos através desse espaço, hoje em dia, são uma realidade. Nós temos legislação sobre isso. É uma realidade. Há o ciberterrorismo, e a gente vai ver que vai existir a convergência, esse cibercrime e ciberterrorismo. O tema da convergência é muito atual hoje, e os erros também. Vão existir erros que vão causar prejuízos nesse ciberespaço, às organizações, à vida privada, a tudo.

O que é o ciberterrorismo? A gente vai ver que o ciberterrorismo é o uso dessa violência - ou seja, é uma violência à sociedade - de forma preparada por organizações - os alvos, em sua maioria, são civis -, com motivos políticos, por meio de sistemas computacionais e de dados. É uma definição simples. Na verdade, a definição de terrorismo está ali em cima. No último item, só, que eu inseri a parte desse novo espaço. Um atentado terrorista a esse espaço pode ter características devastadoras, maiores do que o 11 de setembro. Você modificar a conta de banco das pessoas, você derrubar o sistema de transporte aéreo de um país, isso pode ter consequências gigantescas - gigantescas!

A definição que o FBI usa: são atos de organizações subnacionais, planejados previamente - a questão do planejamento -, com motivação política e direcionados a sistemas de informação, computacionais, programas computacionais e de dados e que resultam em violência contra civis. Essa é uma definição. As características dessa forma de terrorismo - a gente já falou de algumas - é a questão da descentralização. Às vezes, uma rede, uma organização terrorista está atuando com células em cinco, dez, vinte países. Os Estados têm de saber atuar de maneira descentralizada também, através de suas inteligências, em cinco, dez, vinte países também, e rapidamente. Os Estados têm de ser rápidos também. O uso da tecnologia. O Estado não pode ficar atrás da tecnologia que essas pessoas usam. Nós não podemos correr atrás das tecnologias que estão sendo usadas aí. E, quando atingimos essa tecnologia, eles inventam outra coisa, e conquistamos essa tecnologia novamente. O Estado tem de estar à frente. Por isso, o nome disruptivo.

Criativo ao extremo. É uma forma criativa de ameaçar a sociedade. O Estado tem de ser criativo também para combater isso. E isso vai atingir tanto a área de segurança como a área de defesa. Há a cibersegurança e a ciberdefesa.

Antes de um ataque, nós temos de estar preocupados com as medidas. Quais são as medidas? As antimedidas. No que temos que pensar? Principalmente na parte de inteligência. Havendo o ataque, temos que atuar durante o ataque e após o ataque com as nossas contramedidas.

Depois, há uma característica que é muito importante. Nós temos de estar preocupados com a resiliência. É impossível se defender 100% de todos os ataques que uma sociedade vai sofrer. Vai haver algum ataque. É impossível se defender

100%. Só que, a partir do momento que acontece isso, nós sociedade temos de estar preparados para passar por cima disso. É a resiliência. A sociedade precisa voltar. Às vezes, ficamos muito focados na prevenção e na repressão. Temos de estar preocupados com a resiliência social. O Estado tem de voltar. O sistema de abastecimento, o sistema de controle aéreo têm de ser reerguidos imediatamente, para a sociedade voltar a funcionar, para a economia girar, para as pessoas voltarem a trabalhar. Então, nós temos de estar muito preocupados também com a questão da resiliência. É tão ou, às vezes, até mais importante que a preocupação com a as medidas de precaução e de combate ao terrorismo.

Nesse quebra-cabeça pequeninho, eu coloquei inteligência como fator fundamental. A inteligência é essencial no combate e, principalmente, na prevenção. A inteligência é essencial para fornecer o subsídio necessário à pessoa que vai tomar a decisão. As decisões tendem a ser as mais certas possíveis de acordo com a informação que ela tem. Aí nós vamos ter as nossas antimedidas, de que eu falei, as medidas de precaução, as contramedidas, como é que vamos combater, e a resiliência, mas eu fiz questão de colocar inteligência ali, porque é muito importante desenvolvermos, mantermos e ampliarmos o nosso sistema de inteligência.

Ali, em azul, está a questão da cooperação entre agências. Esse ambiente não é um ambiente de combate de uma agência só, não. Às vezes, em um ataque cibernético ao sistema de transmissão de energia do Brasil, vão ter de atuar a Polícia Federal, o Operador Nacional do Sistema, o sistema brasileiro que cuida dessa área, a Abin. Todo mundo vai ter de participar disso. Então, a cooperação entre agências é essencial.

Quando eu falo em disruptivo, é principalmente porque hoje nós sempre estamos usando as tecnologias que nós temos e visando sempre à prevenção e à repressão. Nós queremos prevenir um ataque e nós queremos investigar os ataques que aconteceram, para ver se colocamos essas pessoas na prisão. Mas temos de pensar mais um pouquinho. Nós temos de ir além. Nós temos de pensar no que vai existir. Isso é disruptivo. Mas o Estado, a sociedade tem de estar preparada para saber o que vai ser usado lá na frente. Esta é a característica do disruptivo: o que vão usar, o que podem, futuramente, usar contra a gente. O Estado tem de estar preparado para isso.

E, aí, muda tudo, porque, aí, nós vamos combater já sabendo que aquilo existe. E nós não vamos combater uma coisa que aconteceu. Nós vamos aprender sobre o que aconteceu, para tentar combater os próximos ataques. Nós já vamos tentar prever, planejar, olhar lá para frente, olhar as novas tecnologias que são possíveis de serem usadas nesse setor. E trabalhar para evitar, para se preparar para esses ataques.

Há também a questão da resiliência. Eu gosto de bater nesta tecla: é impossível prevenir todos os ataques. Nem os Estados Unidos da América conseguem. É impossível. Vai haver. Só que nós temos de estar preparados, para que, quando passarmos por isso, nós passemos de forma mais rápida e menos traumática possível. Que a sociedade consiga voltar e se reerguer o mais rápido possível. É a resiliência. Isso é muito importante. Equipes para reerguerem um sistema, para voltar a transmissão daqueles dados; construção, a partir de engenharia; ajuda às vítimas. Este é um outro ponto desse processo: a questão da resiliência. Nós temos de estar preocupados também, a partir da legislação, em facilitar resiliência social. A sociedade precisa voltar a funcionar.

E, por fim, a questão da convergência. O que é a convergência? O terrorismo, nos últimos anos, passa por um fenômeno muito interessante. Depois que o mundo perdeu dinheiro, principalmente dinheiro que vinha da Guerra Fria, para financiar algumas organizações terroristas, essas organizações perderam dinheiro. E elas começaram a atuar na ilegalidade, no crime, cometendo crimes - tráfico de drogas, sequestro, tráfico de material proibido -, para arrecadar dinheiro, para financiar seus atentados. E, aí, nós vamos ver uma convergência entre o terrorismo e o crime organizado.

Nessa área cibernética, nós estamos vendo isso também. Diversas organizações terroristas têm células especializadas em cometer crimes, fraudes, se apropriar de dinheiro, para financiar os seus atentados, que podem ser ciber ou não. Esse é o fenômeno da convergência.

Um dado que me deixou assustado que eu vi, na semana passada ou retrasada, é que, por exemplo, na questão das moedas virtuais, essas moedas bitcoin... Trinta por cento do valor dos bitcoins... O bitcoin pode ser utilizado de forma maravilhosa, ou seja, uma moeda virtual que facilita as transações, mas também pode ser utilizado para o crime, e com dificuldade para o Estado rastrear isso, da forma como está sendo usado isso.

Então, esses grupos vão utilizar essas novas tecnologias para financiar os seus atentados ou para cometer atentados também na área cibernética. Já se percebeu que um atentado nessa área tem efeitos catastróficos para uma sociedade. Então, ele pode gerar uma complicação social muito grande. E este é o fim do terrorismo: a pressão política a um Estado.

Não sei se eu falei um pouco rápido.

(Soa a campainha.)

O SR. MARCUS VINÍCIUS REIS - Era isso o que eu queria falar.

Muito obrigado a todos e a todas.

A SRª BRUNA FURLAN (PSDB - SP. *Fora do microfone*.) - A gente que agradece.

O SR. PRESIDENTE (Fernando Collor. Bloco Moderador/PTC - AL) - Muito obrigado ao Dr. Marcus Vinícius Reis, Coordenador-Geral de Defesa da Secretaria de Assuntos Estratégicos.

Passo agora a palavra ao General de Divisão, Paulo Sérgio Melo de Carvalho, Diretor de Relações Institucionais da Rede ANSP (an Academic Network at São Paulo).

V. Sª tem o tempo de 20 minutos para sua exposição.

O SR. PAULO SÉRGIO MELO DE CARVALHO - Agradeço o convite do Senador Fernando Collor para abordarmos esse tema extremamente relevante que é o terrorismo cibernético.

Cumprimento a Deputada Bruna Furlan, os Srs. Embaixadores, meus senhores e minhas senhoras.

É muito difícil falar depois que *experts* falam sobre um tema que dominam. Eu vou abordar dentro de uma linguagem simples, como é a linguagem do soldado.

Nós trabalhamos, há algum tempo, na parte cibernética, principalmente como General de Brigada e General de Divisão, no Centro de Defesa Cibernética e no Comando de Defesa Cibernética, durante os grandes eventos.

Para iniciar a nossa exposição, nós resolvemos definir o que é o espaço cibernético. Ele é composto pelas informações em equipamentos que são processadas, armazenadas e transmitidas. Trata-se de um espaço virtual, não físico, criado por meios computacionais, onde está a chave de tudo: as pessoas físicas ou jurídicas, isoladamente ou em grupos integrantes de organizações públicas ou privadas podem se comunicar e trocar informações.

O espaço cibernético não tem limite de fronteiras. Ele é global. Para isso, nós militares tivemos que nos adaptar para combatermos uma nova dimensão. Como já foi falado aqui, nós dependemos muito das pessoas, dos especialistas, dos técnicos, e aí nós temos uma criatividade imensa para fazer face aos *softwares*, aos aplicativos. Não adianta ter os melhores *softwares* e aplicativos se não tivermos os nossos talentos capacitados para isso. Também lembro que tudo o que nós vamos fazer tem o famoso efeito colateral: qual é o dano que pode causar ao sistema.

Os meios de tecnologia que estão disponíveis para nós nos defendermos também estão disponíveis para os atacantes. E aí nós sempre estaremos na defensiva. Sempre os operadores cibernéticos vão estar na ofensiva e nós temos que buscar fazer a defesa dos meios computacionais.

Aquele cadeado que está ali à direita é para ressaltar que não existe sistema computacional seguro; não há em nenhuma parte do mundo. Sempre haverá um flanco vulnerável. E, para isso, os nossos amigos *hackers* são expertos nisso, principalmente durante a madrugada, quando eles trabalham.

Vivemos uma guerra da informação onde a criatividade não tem limite. Ali, à esquerda, há um barbeiro que, para manter o seu cliente, coloca uma parte transparente para a pessoa ficar consultando o celular. A informação hoje é assíncrona. E nós, por mais queiramos visitar os nossos entes queridos, vamos estar sempre ali com celulares, *smartphones*. E aquela pessoa que nós fomos visitar fica olhando.

Então, nós temos que nos policiar agora porque vivemos uma guerra de cubo mágico em que estão as redes sociais proliferando. E isso é, como foi falado, o que os terroristas utilizam.

Quais são as ameaças? São essas: os atores governamentais ou não governamentais, motivados, com elevada capacidade técnica, sempre vão explorar as vulnerabilidades. Aí está uma grande deficiência das pessoas. Nenhum desenvolvedor se preocupa, quando está fazendo sistema, com a parte de segurança. E ele não gosta que seu sistema tenha vulnerabilidade. Então, muitas vezes, durante os nossos trabalhos quando estávamos na ativa, tínhamos que falar com os comandantes, com os diretores, para sensibilizarem os seus técnicos de que devem manter os sistemas atualizados e que há algumas vulnerabilidades.

Realização sem autorização legal de ações para acessar, extrair, danificar ou destruir dados ou informações sensíveis que estejam em trânsito ou estejam armazenadas, sistema de informações utilizado por órgãos governamentais, empresas ou indivíduos.

Como já foi falado também por alguns painelistas, esse sistema é todo imbricado. Tem que haver uma cooperação muito grande entre os órgãos públicos e as empresas.

E aí estão as ameaças que nós vivemos hoje no século XXI.

Crime cibernético grassa no mundo, já corresponde a 2%, 3% do Produto Interno Bruto mundial, e só não é mais divulgado porque, como já foi comentado, o sistema bancário tem um sistema de proteção cibernética muito eficiente e busca barrar alguns ataques.

Ali embaixo há a parte de espionagem, que não é somente entre os Estados, mas principalmente a espionagem industrial; o ciberterrorismo, que nós vamos comentar; e o "hackerativismo", que era a grande preocupação de qualquer sistema, de qualquer gerente de sistema de informação. E hoje nós vivemos uma guerra cibernética.

Então, as Forças Armadas de qualquer país entendem que não adianta mais combater com fuzil e com carro de combate. Existe um novo meio de combater, que é a cibernética, que precisa atuar independentemente da sua capacidade somente; precisa da mobilização da capacidade cibernética, principalmente dos meios civis; deve usar a cibernética para fazer economia de meios.

E hoje nós já entendemos que existe uma nova fonte de inteligência: a cibernética. Os *bits* não vestem uniformes e nós não sabemos onde eles estão. Os *botnets* que estão ali hoje podem ser usados como uma tropa de infantaria no princípio da massa, fazendo ataques maciços em qualquer parte do mundo. Para isso, além das dimensões que nós já temos (a terrestre, a marítima, a aérea e a espacial), na atualidade existe a dimensão cibernética, que é multifacetada e, como já foi comentado aqui, está em todas as outras dimensões, é multissetorial.

Nós entendemos, como está na Lei 13.270, de 16 de março do ano passado, antes da Olimpíadas, o que seja terrorismo: "Prática, por um ou mais indivíduos, de atos de terrorismo por razões de xenofobia, discriminação, preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, paz social e incolumidade pública". Quais são os atos de terrorismo? Estão listados lá. O terrorismo clássico, convencional, está aí: "Atentar contra a vida ou a integridade física de pessoa, usar ou ameaçar usar, transportar, guardar, portar ou trazer consigo explosivos, gases tóxicos, venenos, conteúdos biológicos, químicos, nucleares ou outros meios capazes de causar danos ou promover destruição em massa.

E onde entra a cibernética? Atos de terrorismo: "Sabotar o funcionamento ou apoderar-se, com violência, grave ameaça a pessoa ou servindo-se de mecanismos cibernéticos [usando a internet, usando a *web*], do controle total ou parcial, ainda que de modo temporário (...)" Aí estão listadas, praticamente, as nossas infraestruturas críticas e alguns serviços essenciais de qualquer nação, como meios de comunicação, meios de transportes, portos, aeroportos, estações ferroviárias e rodoviárias, hospitais e casas de saúde, escolas. Então é necessária uma grande preocupação do Estado em fazer a proteção cibernética. E não pode ser apenas uma proteção, tem de ser uma defesa, uma segurança ativa.

Visto o espaço cibernético, onde entra o terrorismo? Terrorismo e espaço cibernético. Hoje nós trabalhamos principalmente com as atividades de apoio que já foram levantadas aqui e vou abordar algumas. Quais são as ações efetivas? São aquelas objetivas e aquelas ameaças latentes.

Atividades de apoio. Comando, controle e comunicações. Já foi enfatizado aqui. Os amigos do terror usam e abusam da internet para fazer o comando e o controle das comunicações. Escrevi ali inteligência. Por quê? Utilizando as redes sociais, os terroristas fizeram várias ações num simples endereço de uma filha de um delegado, verificando a agenda de uma autoridade. Então, com tudo isso eles fazem um trabalho utilizando a internet.

Propaganda extremamente utilizada. Aí, como já foi falado, recrutamento, radicalização e incitamento; ampla utilização das redes sociais para fazer isso,

Acesso a recursos. Hoje, inclusive, eles estão contratando *hackers* não só para trabalhar na parte de crimes cibernéticos, mas também para ajudar os terroristas.

Na parte de logística e no hacktivismo, quais são as ações efetivas? Busca e seleção de alvos e principalmente as infraestruturas críticas.

Então, durante os grandes eventos de que o Brasil foi sede, nós fizemos um grande trabalho preventivo em relação às infraestruturas críticas, principalmente buscando fazer uma proteção dos seus ativos de informação.

Quais são as vantagens de o terrorista utilizar a internet e a *web*? Primeiro, porque é em âmbito global, com espaço geográfico definido. A relação custo-benefício pode ser gigantesca. Usando um simples notebook, ele pode causar um dano - um lobo solitário - à infraestrutura crítica de um país, e tem a segurança do anonimato.

Quais seriam as desvantagens, do nosso ponto de vista? Capacidade técnica. Apesar de existirem muitos técnicos, os talentos são difíceis. Então, não adianta você querer formar um *hacker*. Isso já é nato da pessoa e ela pode ser aprimorada. O *hacker* não fica sentado num banco escolar. O *hacker* quer desafio. Então, muitas vezes, ele tem essa dificuldade, essa desvantagem, para sorte nossa.

E a ausência de dramatismo. Através da *web*, ele não vai ter uma mãe recebendo o seu filho sangrando. As imagens não são fortes como no terror, que precisa causar pânico.

Esses são exemplos do que eles utilizam.

Já foi falado ali do centro, o lobo solitário, do califado cibernético, da *picker* que eles usam, das revistas. E ali a própria Organização das Nações Unidas preocupada em fazer o contraterrorismo.

Então, essa iniciativa é muito boa para sensibilizar a sociedade de que nós precisamos fazer um trabalho preventivo muito forte.

Os exemplos estão aí, estão na *web*. Deixei ali embaixo. Isso já tem algum tempo, porque não quis colocar notícias muito recentes:

"Estado Islâmico vai 'disparar para matar' através de *ciber* ataques."

"Anonymous estão a recrutar para atacar Estado Islâmico."

"Instruções do Estado Islâmico em *websites*."

"Anonymous não são os únicos a atacar o Estado Islâmico."

"Conheça a aplicação cada vez mais usada por terroristas. [Era o telegram. E hoje eles já utilizam criptografia, utilizando VPM]

"Estado Islâmico tem '*help desk*' para terroristas 24 horas por dia."

Como nós visualizamos a atividade do Estado? Já foi comentado, foi muito usada a palavra resiliência. O trabalho tem que ser preventivo, o trabalho deve ser executado pela inteligência, buscando as ações de proteção cibernética, mas, principalmente, usando as atividades de exploração cibernética, um acompanhamento do que ocorre nas mídias sociais, buscando ter uma segurança ativa. Nós temos que fazer a defesa como eles vão nos atacar.

A atuação deve ser conjunta, envolvendo as três Forças Armadas, e o trabalho deve ser colaborativo interagência, independentemente de cargo e função. Funciona muito, nessa parte, o que nós chamamos de canal técnico. Então, tem que deixar os talentos dos Estados trabalharem, envolvendo também as empresas, independentemente de uma autoridade; deve ser multifacetado e um projeto lateral. Isso que nós procuramos fazer, o Exército procurou fazer durante os grandes eventos, contando principalmente com a colaboração da sociedade e também das empresas, independentemente de cargo e função. Então, para o trabalho preventivo, nessas ações colaborativas, nós tínhamos que buscar os talentos, onde eles estivessem.

Esse é o desafio! Capacitar e aperfeiçoar recursos humanos para realizar ações cibernéticas eficientes, eficazes e efetivas, com ampla atuação interagências e com foco na sensibilização e conscientização da sociedade brasileira para a importância da segurança e defesa cibernéticas. A segurança cibernética precisa ser eficaz para que a defesa cibernética seja mínima.

Então, esse é o trabalho preventivo que nos ajuda contra as atividades do terrorismo e para isso devem trabalhar esses órgãos. Às vezes não sai com um órgão, mas sai com outro, mas, a princípio, o que nós precisamos é que o Governo, a academia, a sociedade e a indústria estejam todos entrelaçados na luta pelo combate ao terrorismo cibernético.

Então, não adianta só as Forças Armadas quererem aquele produto, precisa da pesquisa e do desenvolvimento da empresa, da academia, e a empresa precisa desenvolver, fabricar a Ferrari que nós precisamos para ganhar a corrida contra o terrorismo cibernético.

Muito obrigado.

O SR. PRESIDENTE (Fernando Collor. Bloco Moderador/PTC - AL) - Muito obrigado ao General de Divisão Paulo Sérgio Melo de Carvalho, Diretor de Relações Institucionais da Rede ANSP (an Academic Network at São Paulo).

Antes de passar às perguntas dos internautas, eu me permitiria fazer alguns comentários sobre o tema hoje tratado nesse nosso painel.

A questão do terrorismo ou ciberterrorismo. Na minha visão, salvo melhor entendimento de outros que tenham opinião divergente, há um subproduto extremamente perigoso nesse combate ao chamado ciberterrorismo, que é exatamente a perda paulatina dos direitos e das garantias individuais do cidadão dos Estados nacionais.

A cada momento que se avança nessa inovação tecnológica para evitar ciberataques, avança-se também na privacidade, na intimidade do cidadão comum. E, muitas vezes, em alguns países, nós encontramos órgãos do Estado, que têm acesso a esses equipamentos de última geração para também ajudar na detecção de ciberataques, que se utilizam de tais equipamentos para entrar no campo dos direitos e das garantias individuais, que no nosso caso, aqui no Brasil, é uma cláusula pétrea. E isso interfere diretamente nas nossas relações sociais. Isso é algo inadmissível.

É preciso, paralelamente, haver também uma legislação que puna aqueles agentes do Estado que utilizem de forma irregular, irresponsável, de forma maldosa os equipamentos de que dispõem para expor, sem nenhum escrúpulo, pessoas, gente do povo, que são apontados já, pela divulgação que é feita dessas imagens, como pessoas que são culpadas dessa ou daquela ação que eles julgam ser punível nas investigações que estão levadas a cabo.

Então, é muito importante, no meu entender, que nós possamos compartimentar toda essa louvável estrutura de que cada um dos Estados nacionais buscam se equipar para proteger o Estado contra esses ciberataques, para evitar o que aqui foi dito pelos nossos palestrantes, de pontos próprios da segurança nacional desses Estados, como os ciberataques em relação ao sistema bancário, ao sistema aeroportuário, ao sistema rodoviário, ao sistema portuário, enfim, e outros.

Mas é importante também que nós vejamos o outro lado da moeda. Que essa busca incessante, que deve ser sempre atualizada, de técnicas para evitar o ciberataque ou o ciberterrorismo, não dê em nenhum momento autoridade, a esses órgãos que estão trabalhando em função disso, para intervir, de forma tão violenta, na privacidade e na vida das pessoas, porque isso - como disse - fere, no caso brasileiro e acredito que de muitos Estados nacionais, um direito fundamental que é a garantia dos direitos individuais da pessoa humana.

De modo que acredito sejamos todos nós participantes e responsáveis, de alguma forma, pelo sucesso de evitarmos que os nossos Estados sofram com esses ataques. O Brasil, aqui foi dito, teve uma atuação extraordinariamente exitosa durante as Olimpíadas, que não houve sequer um ato, até mesmo briga de rua. Aqui no Brasil isso não ocorreu. Uma demonstração de que os órgãos competentes para tratar desse assunto se saíram muito bem e foram elogiados por todos os organismos de segurança dos países cujas representações estiveram disputando aqui as Olimpíadas.

Mas vamos fazer uma reflexão e dar uma atenção muito especial para que isso acabe não afetando - volto a dizer - as garantias e os direitos individuais da pessoa humana.

Passando às perguntas dos internautas, gostaria que os senhores palestrantes, caso tenham interesse em anotar... Alguns são comentários, outros são perguntas:

De Wallace Araújo, de Minas Gerais; ele fala: barreiras somente para radicais.

De Andréa Amorim Campos, do Rio Grande do Sul, que diz: a Lei do Terrorismo no Brasil deve ser revista; nas Olimpíadas - ela cita as Olimpíadas - a operação obteve resultados confortantes para o mundo, mas ocasionou injustiças para os indiciados. Aí não entendi direito o que ela quis dizer aqui. Sabemos que um rapaz - ah, sim - foi morto na cadeia por suposto crime de terrorismo, mas nada se comprovou. Não tomei conhecimento disso também, mas os nossos palestrantes irão ter oportunidade de falar sobre essa questão.

De Pedro Paulo Lopes da Silva, do Rio Grande do Sul: nem um, nem outro, penso que devemos investir muito mais recursos em pesquisa e desenvolvimento, ampliar os programas já existentes junto a universidades, fomentar a criatividade desde cedo pelo sistema educacional.

De Andréa Amorim Campos, do Rio Grande do Sul: temos um sério problema a ser resolvido: qual é o estigma da imagem criada do terrorista? Muitos sofrem com a discriminação de sua cultura, principalmente a religiosa; generaliza-se.

É verdade.

De Fernando Claudino de Souza: Devemos implantar a teoria de recrutamento de pessoas que se adequam à área da tecnologia sobre a cibernética. Não fazer concurso público onde entram pessoas pouco competentes nessa área de informática.

Acho que aqui ela cita muito o que o general falou há pouco, que o *hacker* já nasce, ele não é formado.

Então aqui ele fala que o concurso público não dará um resultado tão bom quanto já pegar um *hacker* que tenha na sua própria genética esse talento.

De Anna Flavia Schmitt Wyse Baranski, de Santa Catarina: "O Brasil precisa investir na inteligência e nas Forças Armadas. O Brasil não precisa erguer pontes e nem erguer barreiras. O País precisa é vigiar as suas fronteiras e seus espaços aéreo e marítimo. Estar pronta para combater os inimigos sem rosto faz parte de toda a Nação zelosa."

De Sidnei Dornelles da Silva, do Rio de Janeiro: "Impedir a entrada de estrangeiros aqui, pois já está muito ruim para milhões de brasileiros no momento, e esses estrangeiros vão tirar oportunidades para brasileiros natos. Estamos em crise, esqueceram?"

Sobre essa pergunta do Sidnei, eu gostaria de fazer um rápido comentário. O Brasil é um País resultante de imigrantes. Nós somos todos descendentes de imigrantes, todos. Nós tivemos levas de imigração de japoneses, de italianos, de europeus do norte, além dos portugueses que aqui estiveram, enfim, várias levas de imigração. Do mundo árabe, importantíssima a imigração do mundo árabe, que se localizou basicamente em São Paulo. E o interessante é que a cada leva de imigração

que o Brasil recebeu, coincidiu logo em seguida um processo de desenvolvimento extremamente importante para o nosso País. Ou seja, foi extremamente saudável o processo de imigração. E o Brasil sempre foi e continuará sendo um País que, no meu entender, pelo que nós conhecemos do povo brasileiro, estará sempre de braços abertos aos imigrantes.

E para que o Sidnei Dornelles da Silva, que fez essa pergunta, tenha apenas uma ideia, no final do ano de 2016, o mundo inteiro tinha 64 milhões de refugiados em diversos pontos do Planeta. Em diversos pontos, campos de refugiados, refugiados entendidos como pessoas que se deslocaram de suas terras, de seu solo por questões de guerras, questões políticas, questão da fome, enfim, de outros males. Pois bem, no mundo, 64 milhões, no final de 2016, eram chamados *desplazados*, refugiados. O Brasil, no final de 2016, tinha somente dez mil e poucos, dez mil e trezentos refugiados para uma população de 200 milhões de habitantes. Ou seja, não é nada.

O Brasil pode fazer muito mais; e eles não estão aqui para tomar o emprego dos nativos brasileiros, não estão para de alguma forma impedir que os nossos sistemas de saúde caminhem ao contrário. Eles vêm aqui trabalhando, trabalhando e ajudando a construir uma economia mais forte para nós brasileiros.

A última pergunta é de Paulo James Martins, que fala:

> *Erguer barreiras é um pensamento economicamente inviável e fascista, porém deve-se filtrar os indivíduos que irão entrar no nosso território, mas não em razão de sua nacionalidade ou até de sua religião, mas em razão da capacidade de agregar valor ao mercado com conhecimento.*

Em relação também à questão de religião o Brasil, é um País onde convivem todas as religiões, e convivem da maneira mais harmoniosa e pacífica possível. Eu, quando Presidente da República Federativa do Brasil, cargo para o qual fui eleito e muito me honrou, por acaso, não foi nada de caso pensado, eu tinha um Ministro das Relações Exteriores que era judeu e havia um assessor que trabalhava comigo, em meu gabinete, que era libanês e tinha diversos... Nós até brincávamos muito, porque o Itamaraty, que é essa instituição de excelência não só no Brasil, mas perante todo o mundo, tem uma miríade de nacionalidades, de descendentes de nacionalidades diferentes, e todos convivemos muito bem com essa questão religiosa. Para nós isso não existe.

De modo que é possível, sim, nós vivermos em paz, em fraternidade. Eu acho que a inteligência humana deve estar à disposição para que nós possamos construir consensos; a inteligência humana não foi feita para haver xingamentos pelas redes de televisão, pelos *twitters* em relação a um chefe de Estado a, b ou c, mas sim buscar pela diplomacia, com diálogo, um meio de se construir um mundo melhor. Não será com posições isolacionistas, não será com posições unilaterais, não será com posições de força que nós haveremos de construir o Planeta de paz e estabilidade que desejamos.

É necessário que haja um pouco mais de clarividência na cabeça dos nossos estadistas, para que o nosso Planeta saia desse momento tão conturbado em que estamos vivendo e que nos causa sobressaltos. Então, mais do que nunca eu acredito que a diplomacia tem que entrar em campo. É preciso a compreensão sobretudo dos líderes, daqueles que têm mais bom senso, mais capacidade, visão de raciocínio e visão do mundo, para não entrar nessa seara, nessa rinha de briga de galos - uma briga que tem aqui no Brasil e inclusive foi proibida -, porque isso não leva a lugar nenhum, isso só faz com que se diminua, diante da população mundial, a incapacidade de lideranças mundiais promoverem algo que é absolutamente da natureza humana: viver em paz, com respeito mútuo, buscando pontos de coincidência, tentando superar as dificuldades que existem nas relações entre Estados, mas procurando sempre o consenso e a paz.

Portanto, ficam aqui as perguntas que foram formuladas pelos nossos internautas e eu passo a palavra, inicialmente, logo, ao General Paulo Sérgio Melo de Carvalho, para oferecer as suas respostas a essas indagações.

O SR. PAULO SÉRGIO MELO DE CARVALHO - Nós ouvimos o que o Senador falou, as perguntas dos internautas.

Nós entendemos que para atuar na área cibernética, o foco que aparece é a parte operacional. Nós fazemos os trabalhos de defesa cibernética principalmente para atender a inteligência, mas para exercitar esse papel, nós precisamos de uma doutrina.

Então, isso foi o trabalhado durante algum tempo pelo Exército brasileiro, quando começou o setor estratégico da cibernética: estabelecer uma doutrina de defesa e guerra cibernética. E amparado pela ciência e tecnologia, buscando, principalmente, os talentos.

O Senador já comentou aqui também que o talento é inato, mas ele precisa ser descoberto. Para isso, nós temos que fazer um trabalho, um programa de sensibilização na sociedade brasileira, como outros países já fazem. Não vou citar nomes, eu os visitei, eles começam desde o jardim de infância, ali, no primário, não sei hoje como se chama, no ensino fundamental, já identificando aqueles talentos vocacionados para a área cibernética.

Então esse programa necessita ser desenvolvido pela sociedade brasileira. Os talentos... Nós temos muita gente trabalhando na área de segurança de informação, na área de TI, mas as empresas identificam os talentos na academia. Então, hoje eu

estou trabalhando mais no meio civil, com academia e com empresas, e vejo *startups* trabalhando junto das universidades; e dá uma alegria enorme você entrar numa empresa e ver aqueles meninos e meninas trabalhando, que já são doutores.

Então, aí é que está o segredo de se buscar desenvolver uma tecnologia autóctone. Muitas das empresas que hoje nós acompanhamos buscam desenvolver sistemas aplicativos próprios.

Enfatizamos também as iniciativas que já foram tomadas pelo Governo brasileiro. Existem programas interministeriais de pesquisa e desenvolvimento. Nós trabalhamos buscando desenvolver programa entre o MCTI e o Ministério da Defesa para empresas desenvolverem o antivírus nacional, o *firewall* nacional.

Então, houve financiamento do MCTI; e sob a coordenação do Exército, do Ministério da Defesa e do MCTI, existem empresas que estão desenvolvendo essas ferramentas.

Nós entendemos que é isso, estender pontes buscando um trabalho colaborativo que não envolve só os órgãos que devem fazer a defesa cibernética, mas principalmente a academia, as empresas. Existem soluções excepcionais nas empresas e nas academias.

Muito obrigado.

O SR. PRESIDENTE (Fernando Collor. Bloco Moderador/PTC - AL) - Muito obrigado, mais uma vez, ao General de Divisão Paulo Sérgio Melo de Carvalho.

Passo agora a palavra ao Dr. Gills Vilar Lopes.

O SR. GILLS VILAR LOPES - Olá. Primeiramente, queria dizer àqueles internautas que mandaram suas perguntas que realmente o fato de eles terem feito isso, por meio daquele símbolo ali do e-Cidadania, do Senado Federal, já demonstra como a internet nos traz esse anseio de participação que muitas vezes a gente vê em livros, remete à *polis* grega, e a gente pensa: nossa, como fazer isso? Como fazer a democracia de maneira direta também? E não só por aqueles meios elencados no art. 14 da Constituição?

Então, a internet traz, no meu ponto de vista, no século XXI, alguns questionamentos e desafios, mas ela também reafirma algumas formas novas de se fazer democracia. E o e-Cidadania é um desses exemplos.

Eu mesmo, há alguns meses, também para esta Comissão, participei mandando perguntas. Então, nada mais me alegra aqui do que responder aos colegas que mandam perguntas por meio deste canal.

O Senador Collor colocou uma questão muito importante que é essa dicotomia, esse paradoxo de sopesar de um lado vigilância e controle, a vigilância estatal, o controle social, ou seja, o controle do Estado perante o cidadão, e ao mesmo tempo a ressalva, a resguarda desse direito fundamental que é a intimidade, o seu foro, seja ele no âmbito real ou seja ele no âmbito virtual. E, certamente, Senador, essa é uma pergunta problema com a qual, na academia pelo menos, a gente se defronta a todo momento.

Certa feita, eu entrevistei um dos - pode-se chamar assim - pais fundadores da internet, que foi um cientista da computação lá dos Estados Unidos, e eu perguntei a ele: Quando vocês criaram a internet - no caso específico dele, ele criou o protocolo de comutação de pacotes - 50 anos atrás, sei lá, 40 anos atrás, vocês imaginavam o alcance de insegurança que ela engendraria no século XXI? E ele disse que não, porque assim como ele, os outros acadêmicos, os outros envolvidos naquele projeto, que tinha um cunho militar de segurança nacional, da guerra fria, da Arpanet, estavam preocupados simplesmente com o papel colaborativo da rede, para que a informação tramitasse de forma descentralizada. Então, as questões securitárias ficaram em segundo plano. Décadas depois, a gente vê o reflexo disso hoje.

Trazendo mais para perto também a questão de uma falta de cultura de segurança da informação, ou cultura de segurança cibernética no Brasil, eu também já trabalhei desenvolvendo *software*, já coordenei uma equipe de *software*, e sempre eu ficava me indagando, ou indagando o meu chefe à época: Depois que a gente fizer o produto, a gente não vai testar a segurança dele? Não, porque o cliente só quer que funcione.

Então, é uma coisa muito ramificada na cultura - se eu posso dizer assim -; um aspecto mais antropológico da questão cibernética é a falta de cultura cibernética. A gente vê, em poucos casos - já respondendo a algumas perguntas aqui -, eu não diria recrutamento, mas a gente percebe como o Senado Federal, a Câmara dos Deputados, alguns órgãos, a CGU, enfatizam as maratonas *hackers*, fazendo no sentido de que o *hacker* também tenha seus problemas não são informáticos ou computacionais, mas os problemas sociais. "Vamos 'hackear' o Brasil, vamos olhar as falhas do nosso País e propor soluções." Isso é o que um *hacker*, faz um *hacker* do bem, um *hacker* social faria.

Então, em muitos eventos, em muitas instâncias municipais, estaduais e federais de que eu tenho notícia, o governo de cada uma dessas esferas está ensejando justamente a criação e a participação ativa dos *hackers* para trazer soluções a

problemas sociais que podem ser minimizados ou resolvidos em certa medida por meio dos *softwares* informacionais, dos computadores.

Terminando minha fala, se a gente falou daquela dicotomia de controle social do Estado com o indivíduo, hoje em dia, a gente fala em controle social também do indivíduo com o Estado, a questão de transparência, *accountability*, que tem trazido, tem vindo à tona justamente pelo uso dessas tecnologias de informação e comunicação, que tornam os dados mais paliáveis, mais transparentes e mais diretos para o cidadão. Então, é uma mão dupla, você dá e recebe. Cabe aos indivíduos também terem em mente - os militares chamariam de doutrina, nas nossas casas chamariam de ensinamentos - justamente promover uma cultura de paz, seja ela no âmbito das relações sociais reais, seja ela no âmbito das relações cibernéticas.

O SR. PRESIDENTE (Fernando Collor. Bloco Moderador/PTC - AL) - Grato ao Prof. Dr. Gills Vilar Lopes, professor da Universidade Federal de Rondônia.

Passo a palavra ao Prof. Dr. Jorge Mascarenhas Lasmar, da Pontifícia Universidade Católica de Minas Gerais.

O SR. JORGE MASCARENHAS LASMAR - Bem, ante os questionamentos e apontamentos que nos foram lidos pela internet, eu me sinto na obrigação de fazer coro ao Senador Collor, especialmente em dois pontos muito importantes. Primeiro, o comentário sobre a questão do xenofobismo e a ligação com a questão religiosa.

Nós falamos da importância de se pensar em ciberataque também a partir do ponto de informações falsas, ataques de semântica e de sintaxe. É exatamente isto, nós temos que ter em mente também que a cobertura desses fenômenos deve ser mais responsável, devemos evitar generalizações. Nós não podemos esquecer que terrorismo não, não está de forma alguma ligado a qualquer questão religiosa. De fato, o que nós vemos são grupos, pessoas ou indivíduos que se apropriam dos ritos, palavras, símbolos religiosos e se utilizam disso para justificar as suas ações com uma finalidade política. O que nós observamos é o uso político de símbolos e significados religiosos.

Nós temos que lembrar também que nós não podemos associar a questão da religião muçulmana com o terrorismo. Nós somos bombardeados pela mídia com essa imagem, que é uma imagem falsa.

Praticamente todas as religiões do mundo já produziram grupos que foram considerados, em um momento ou em outro, terroristas.

Ou seja, grupos judaicos, cristãos, budistas, que se utilizaram da violência e se utilizaram dos ritos e símbolos daquela religião para justificar as suas ações.

E mais que isso, quando nós olhamos o número de atentados que ocorre no mundo ocidental, mais de 75% desses atentados ocorrem por causas não religiosas. São atentados ligados à supremacia branca, a questões do meio ambiente, extrema esquerda etc. Nós não podemos então fazer essa associação irresponsável entre terrorismo e religião, nós temos que separar as coisas.

O segundo ponto é a questão da diversidade. Eu sou um grande defensor da diversidade, minha própria esposa é estrangeira, eu sou neto de imigrantes que vieram fugindo da Primeira Guerra Mundial para o Brasil. É preciso que nós nos lembremos da importância de o Brasil receber esses refugiados, no caso específico os refugiados sírios. São pessoas que muitas vezes perderam tudo com a guerra, tudo com o fenômeno do terrorismo, da guerra civil, da violência que assolou os seus países e encontraram no Brasil um ponto de acolhida.

Sim, nós estamos vivendo um momento de crise, de crise econômica, mas é exatamente nesses momentos de crise que a diversidade pode nos ajudar. Do que precisamos é de inovação e criatividade. Nós falamos bastante na questão da procura por novos talentos. E a diversidade pode trazer visões diferentes.

Então, eu me lembro do caso dos refugiados sírios que estão no sul do Brasil e que estão ajudando enormemente as empresas locais a exportar para o mundo árabe. Eles trouxeram aquele conhecimento da língua, da cultura, conhecimentos locais, e estão fazendo com que essas empresas tenham um aumento muito grande da sua renda, dos empregos que estão gerando, exatamente se inserindo em novos mercados.

Nós não podemos nos fechar a essa questão. Não podemos ligar também, de maneira alguma, a questão do refugiado com a questão do terrorismo. Nós temos que lembrar que muitas vezes eles estão exatamente fugindo desse mesmo terrorismo que nós estamos aqui discutindo.

O terrorismo é uma arma de destruição social. Nós temos que ter sempre isso em mente também.

O SR. PRESIDENTE (Fernando Collor. Bloco Moderador/PTC - AL) - Muito grato ao Prof. Dr. Jorge Mascarenhas Lasmar, da Pontifícia Universidade Católica (PUC) de Minas Gerais.

Para encerrarmos o nosso painel de hoje, passo a palavra ao Dr. Marcus Vinícius Reis, Coordenador-Geral de Defesa da Secretaria de Assuntos Estratégicos da Presidência.

O SR. MARCUS VINÍCIUS REIS - Boa noite.

São excelentes as perguntas. Acho essa participação dos internautas fantástica.

Eu queria primeiro fazer um comentário sobre a questão desse conflito que existe entre segurança e liberdade, de que o Presidente Collor falou com muita propriedade. É um desafio da sociedade atual e vai ser sempre. Eu acho que não haverá respostas. Acho que em cada sociedade, em cada momento da sociedade, em cada tempo daquela sociedade ela vai aceitar mais ou menos intromissão a sua vida privada.

E aí está o papel fundamental do Congresso Nacional na sua produção legislativa de regulamentar isso, de perceber o que sociedade quer e protegê-la. E também do Poder Judiciário de poder aparar as arestas depois que acontecer alguma violação.

Isso é muito importante. Agora o conflito é um conflito da atualidade, é um conflito para o qual não vejo solução. É um conflito que vamos ter que analisar de maneira diferente em cada momento de uma sociedade.

O meu segundo ponto. O general falou da questão do recrutamento. Ele está corretíssimo. Eu acho que nós temos - e falo com louvor - um sistema de recrutamento do público maravilhoso, baseado na capacidade intelectual da pessoa, que são os concursos públicos, mas ele não deve ser o único. Ele não pode ser o único. Nós temos de ter outros mecanismos para recrutar essas pessoas, esses gênios ou para recrutar organizações, para contratar organizações para produzirem conhecimento para o Estado. Eu falei naquela questão de a gente ter uma segurança disruptiva, de a gente estar sempre à frente do criminoso, do terrorista. O Estado tem de ser ágil. As nossas formas de compra, de recrutamento são excelentes, mas nós temos de ter outras formas também.

Com a questão dos imigrantes, eu concordo totalmente. Acho que existe um preconceito muito grande quando a gente fala na questão da imigração por problemas atuais, de uma conjuntura atual que não refletem a realidade. Isso é um erro. A definição de erro é a falsa percepção da realidade.

O SR. PRESIDENTE (Fernando Collor. Bloco Moderador/PTC - AL. *Fora do microfone*.) - Muito bem.

O SR. MARCUS VINÍCIUS REIS - Eu me lembro... Se você conversa com uma pessoa de determinado país, se você conversa com uma pessoa, por exemplo, da Argentina, ela vai falar que um dos maiores problemas da sociedade argentina é a segurança pública. Quando você vai ver os dados, não é segurança pública. Uma pessoa que mora em Buenos Aires tem uma probabilidade de morrer assaltada da mesma maneira que uma pessoa na Europa. Isso é uma falsa percepção. E a gente tem de trabalhar e esclarecer. Isso é conhecimento. O Brasil vive um momento demográfico importante. A gente tem de começar a pensar na questão da imigração novamente. A gente precisa complementar a nossa população. Os imigrantes vão ter sempre um papel fundamental nisso.

Com isso, eu encerro. São os comentários que eu queria fazer.

Muito obrigado.

O SR. PRESIDENTE (Fernando Collor. Bloco Moderador/PTC - AL) - Muito obrigado, Dr. Marcus Vinícius Reis, Coordenador-Geral de Defesa da Secretaria de Assuntos Estratégicos da Presidência.

Eu gostaria, mais uma vez, de agradecer aqui a presença de S. Exªs o Senhor Embaixador da Itália, Sr. Antônio Bernardini; o Senhor Embaixador do Qatar, Sr. Mohammed Alhaykí; o Senhor Embaixador de Angola, Sr. Nelson Manuel Cosme; o Senhor Embaixador do Azerbaijão, Sr. Elkhan Polukhov; o Senhor Embaixador da Polônia, Sr. Andrzej Braiter; o Senhor Embaixador da Bolívia, Sr. José Kinn Franco. Muito obrigado pela presença de V. Exª aqui em nosso painel na noite de hoje. A Senhora Embaixadora Gisela Padovan, do Ministério das Relações Exteriores e Coordenadora da Assessoria de Assuntos Federativos e Parlamentares do Ministério das Relações Exteriores; o Cônsul da Embaixada do Cazaquistão, Sr. Rauan Akim; o Senhor Ministro Conselheiro da Embaixada da Espanha, Sr. José Manuel Pascual Garcia; o Senhor Ministro Conselheiro da Embaixada da Itália, Sr. Filippo La Rosa; o Ministro Conselheiro da Embaixada do Irã, Sr. Morad Ali Gholami Nohouji; o Senhor Conselheiro da Embaixada do Cazaquistão, Sr. Sanzhar Ualikhanov; o Senhor Conselheiro da Embaixada da Federação da Rússia, Sr. Alexander Baulin; o Adido Militar, Aeronáutico e Naval da Embaixada da Federação da Rússia, Sr. Aleksandr Alekseev, e a Engenheira de Sistemas de Informática da Embaixada do México, Srª Cynthia Margarita Herrera.

Também agradeço mais uma vez e muito especialmente aos nossos palestrantes na noite de hoje, o General de Divisão Paulo Sérgio Melo de Carvalho, ao Dr. Jorge Mascarenhas Lasmar, ao Dr. Marcus Vinícius Reis, ao Dr. Gills Vilar Lopes e muito especialmente, como disse no início da nossa reunião de hoje, a S. Exª a Deputada Bruna Furlan, Presidente da Comissão de Relações Exteriores e Defesa Nacional da Câmara dos Deputados.

Informo que o 15º Painel ocorrerá no dia 6 de novembro, segunda-feira, às 18h, neste plenário da Comissão de Relações Exteriores e Defesa Nacional, quando será abordado o tema: "Reestruturação da Defesa Nacional: reflexões sobre o preparo e o emprego das Forças Armadas no século XXI". Para expor e debater o tema, teremos como convidados o jornalista Roberto Godoy, do jornal *O Estado de S. Paulo*, o Prof. Dr. Augusto Teixeira Júnior, da Universidade Federal da Paraíba, o Sr. Carlos Erane de Aguiar, Presidente do Sindicato Nacional das Indústrias de Materiais de Defesa, e o Contra-Almirante Antonio Ruy de Almeida Silva.

Antes de encerrarmos os trabalhos de hoje, convoco as Srªs e os Srs. Senadores membros desta Comissão para nossa próxima reunião deliberativa, agendada para o próximo dia 19 de outubro, quinta-feira, às 9h, neste plenário, na qual vamos deliberar as emendas ao Projeto de Lei Orçamentária Anual para 2018, PLN nº 20, de 2017.

Agradecendo mais uma vez a presença de todas as senhoras e senhores e autoridades, a nível de excelência, declaro encerrada a presente reunião.

Muito boa noite.

(Iniciada às 18 horas e 02 minutos, a reunião é encerrada às 20 horas e 18 minutos.)