DEPARTAMENTO DE TAQUIGRAFIA, REVISÃO E REDAÇÃO

NÚCLEO DE REDAÇÃO FINAL EM COMISSÕES

TEXTO COM REDAÇÃO FINAL

Versão para registro histórico

Não passível de alteração

CPI - CRIMES CIBERNÉTICOS			
EVENTO: Audiência Pública	**REUNIÃO Nº: 0177/16**		**DATA: 29/03/2016**
LOCAL: Plenário 14 das Comissões	**INÍCIO: 14h53min**	**TÉRMINO: 18h24min**	**PÁGINAS: 72**

DEPOENTE/CONVIDADO - QUALIFICAÇÃO

GABRIEL BOFF MOREIRA - Coordenador-Geral de Combate aos Ilícitos Internacionais do Ministério das Relações Exteriores.
MARCONI DOS REIS BEZERRA - Diretor do Departamento de Segurança da Informação e Comunicações da Casa Militar da Presidência da República — DSIC.
JOSÉ RICARDO SOUZA CAMELO - Chefe da Divisão de Operações do Centro de Defesa Cibernética — CDCIBER.
WILLIAM MURAD - Diretor de Inteligência da Secretaria Extraordinária de Segurança para Grandes Eventos do Ministério da Justiça.
LEONARDO BOSELLI DA MOTTA - Diretor do Departamento de Infraestrutura e Serviços de Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão
EDUARDO ARTHUR IZYCKI - Oficial de Inteligência da ABIN.
ELMIZ ANTONIO ROCHA JUNIOR - Delegado da Coordenação-Geral da Diretoria Executiva da Polícia Federal — CGE/DIREX.

SUMÁRIO

Seminário sobre Segurança Cibernética para as Olimpíadas Rio 2016.

OBSERVAÇÕES

Houve exibição de imagens.
A reunião foi suspensa e reaberta.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Boa tarde a todos.

Declaro aberto o Seminário sobre Segurança Cibernética para as Olimpíadas Rio 2016, prevista para acontecer no próximo mês de agosto.

Expediente. Comunico que a CPI recebeu a seguinte correspondência:

Ofício nº 70, de 2016, justificando *"a ausência do Deputado Marcelo Aguiar das reuniões realizadas nos dias 16 e 22 de março em razão de compromissos políticos."*

Ordem do Dia.

O seminário que ora se inicia decorre da aprovação dos Requerimentos nºs 126/2015, de autoria do Deputado Silas Freire, e 140/2016, proposto pelo Delegado Éder Mauro.

Da leitura dos requerimentos, percebe-se a preocupação dos Parlamentares com a segurança dos Jogos Olímpicos Rio 2016, que acontecerão entre os dias 5 e 21 de agosto no País, em razão dos últimos ataques terroristas ocorridos na França e na Bélgica, preocupação também externada pelo Deputado JHC no Requerimento nº 133/2015.

Encontram-se presentes representantes dos Ministérios das Relações Exteriores, dos Ministérios da Defesa, da Justiça, do Planejamento, Orçamento e Gestão, da Casa Militar e também da Presidência da República, da Agência Brasileira de Inteligência e da Polícia Federal.

Informo que este seminário está sendo transmitido pela Internet na página camara.leg.br. As pessoas que nos assistem podem formular perguntas aos convidados.

Diante da quantidade de oradores e por se tratar de um seminário, vamos dividir as apresentações em duas Mesas.

Convido para compor a primeira Mesa os seguintes convidados: Sr. Gabriel Boff Moreira, Conselheiro Coordenador-Geral de Combate aos Ilícitos Internacionais do Ministério das Relações Exteriores; Sr. Marconi dos Reis Bezerra, Diretor do Departamento de Segurança da Informação e Comunicações da Casa Militar da Presidência da República; o Coronel José Ricardo Souza Camelo, Chefe da Divisão de Operações do Centro de Defesa Cibernética — CDCIBER; e o Sr. William Murad,

Diretor de Inteligência da Secretaria Extraordinária de Segurança para Grandes Eventos do Ministério da Justiça.

Formada esta primeira Mesa, agradeço aos convidados e concedo a palavra ao primeiro expositor, o Sr. Gabriel Boff Moreira.

O SR. GABRIEL BOFF MOREIRA - Muito obrigado, Deputada Mariana Carvalho.

Srs. Deputados, senhoras e senhores, primeiro eu queria agradecer a oportunidade de estar aqui hoje para compartilhar a visão do Itamaraty sobre crimes cibernéticos, especialmente neste momento em que nós nos preparamos para as Olimpíadas.

Eu queria dizer inicialmente que aqui nós temos representantes de vários órgãos do Governo brasileiro, que têm um papel muito importante no combate aos ataques cibernéticos e na sua neutralização. Essas pessoas conduzem, do ponto de vista operacional, essas atividades.

O Itamatary tem, por outro lado, um papel um pouco diferente do papel operacional. O Itamaraty não entra em campo para neutralizar atividades, ataques cibernéticos. O nosso papel é muito mais o de estimular, criar um ambiente favorável para a cooperação internacional para neutralizar esse tipo de atividade. É algo também extremamente importante. Como eu vou mostrar mais adiante, nós não temos um arcabouço normativo internacional que permite o combate ao crime internacional, aos crimes cibernéticos.

Então, o nosso papel é mais o de criar um espaço para o desenvolvimento da cooperação internacional e também o desenvolvimento de normas internacionais.

Eu queria falar um pouquinho sobre a situação do Brasil em termos de segurança cibernética. O crime cibernético mais comum do nosso País é a fraude bancária *on-line*. O Brasil, embora não haja dados muito confiáveis, é um país que se situaria em segundo lugar em número de crimes dessa natureza, depois da Rússia. Mas, segundo dados oficiais, o número de ataques cibernéticos teria crescido 197%, em 2014. Então, é algo que vem realmente sendo motivo de grande preocupação no País.

Bom, esses números impressionam em boa parte porque mais da metade da população brasileira, quase 60% — 58%, na verdade —, está conectada à Internet.

Só para ter uma base de comparação, na China e na Índia, por exemplo, esse número é de 49%, e na África do Sul é de 18% — para exemplificar com países parecidos com o Brasil, países do BRICS. E aqui no Brasil cerca de 45% de todas as transações bancárias são realizadas por meio digital.

Além disso, também há uma abundância muito grande de terminais eletrônicos no Brasil, em muito mais densidade do que em outros países muito importantes. Por exemplo, no Brasil há 130 máquinas, esses terminais bancários eletrônicos, para 100 mil adultos. No caso do Reino Unido, por exemplo, esse número é um pouquinho inferior, é 127 por 100 mil habitantes. No caso da França, esse número é 109, e, no caso da Alemanha, é 116. Então, o Brasil tem uma atividade muito maior, tem muito mais atividade bancária *on-line*. Isso facilita muito os crimes, os ataques e as fraudes cibernéticas.

Mas o Brasil aparentemente não é um País tão vulnerável quanto se pensa, analisando esses números. Existe um índice que se chama Índice Global de Segurança Cibernética, que é produzido pela União Internacional de Telecomunicações, que mede o nível de compromisso dos países com relação à segurança cibernética. E o Brasil está muito bem posicionado nesse índice. Ele está em quinto lugar, junto com outros países, como os Estados Unidos, Canadá, etc.

Para as Olimpíadas, esses ataques cibernéticos de que eu falei, que são os ataques, a gente pode dizer, tradicionais aqui no Brasil, não são os únicos ataques que devem preocupar, enfim, mas também ataques a infraestruturas e sistemas. E eu tenho certeza de que os outros expositores aqui falarão com muito mais propriedade do que eu sobre isso.

Bom, ataques mais comuns em grandes eventos. O que a gente pode esperar como uma ameaça para as Olimpíadas do Rio de Janeiro? Eu acho que a gente tem uma base de comparação que é o que nos chegou de relato da equipe que trabalhou na segurança cibernética das Olimpíadas em Londres, em 2012. Eles registraram 165 milhões de incidentes, mas incidentes, na maior parte deles, triviais. Uma pessoa que não conseguiu acessar ou errou a senha, por exemplo, caracteriza um incidente, mas não tem nenhuma importância do ponto de vista da segurança. Enfim, mudanças de senha, esse tipo de coisa, também são incidentes, mas que não têm nenhuma importância.

Desses 165 milhões, apenas 97 incidentes foram considerados preocupantes do ponto de vista da segurança, e seis deles apresentaram uma ameaça real. Dentre esses seis, eu destacaria alguns: tentativa, por exemplo, de invadir a infraestrutura de tecnologia da informação na véspera dos jogos, que foi uma tentativa por dez minutos, sem êxito. E alega-se que essa tentativa veio de um grupo de *hackers* do Leste Europeu.

Também no dia da cerimônia da abertura, em 27 de julho de 2012, houve um ataque aos sistemas de energia do parque olímpico, que é um caso típico de ataque com o propósito de negar serviço. E esse ataque também foi impedido e teve uma duração de 40 minutos.

No dia seguinte à abertura das Olimpíadas, também teve um anúncio, em redes sociais, por *hackers*, de ataques conjuntos também a sistemas de infraestrutura. Também houve ataques de *spams* em sistemas de tecnologia de informação de uma grande agência de notícias internacional, o que acabou bloqueando endereços de IP e impedindo o acesso de outros meios de comunicação.

Enfim, são esses tipos de ataques que a gente pode esperar para as Olimpíadas e para os quais teremos que estar preparados.

Bom, há quem defenda que esses ataques que esses ataques são, na verdade, superdimensionados, que eles não apresentariam grande risco e que não haveria nenhum registro de um ataque cibernético de grandes proporções em grandes eventos recentes.

Mas, de todo modo, em todos esses últimos grandes eventos, sempre houve um grande esforço entre as agências e um grande esforço internacional para neutralizar esse tipo de ataque.

Bem, eu queria destacar que uma das ameaças que tem surgido no debate internacional como uma grande ameaça são os ataques à infraestrutura. Quer dizer, de 2012 para cá são 4 anos e, como esse mundo virtual é muito dinâmico, os riscos também são dinâmicos e cada vez aparecem riscos maiores e diferentes.

Enfim, há também uma grande ameaça com relação a ataques à infraestrutura, como ataques às centrais de energia, por exemplo, usinas hidrelétricas.

Outra preocupação recente de quem é especialista no assunto indica que também há o perigo de ataques espaciais, principalmente interrupção ou interferência em sinais de satélite, o que, enfim, resultaria em efeito muito devastador, já que tudo está mais ou menos interligado com GPS, sistemas de comunicação, sistemas de telefonia celular, voos, etc. Então, esse é um tipo de ataque que também deve preocupar o Governo brasileiro.

Bom, qual é o problema disso tudo? O problema é que existem ataques cibernéticos; eles são cada vez mais comuns e, ao mesmo tempo, eles são crimes transnacionais. Quer dizer, é impossível delimitar, dentro de um próprio Estado, os crimes cibernéticos. Crimes cibernéticos, em geral, envolvem mais de um país; envolvem servidores que estão localizados, às vezes, em vários países, não apenas em um; e envolvem também empresas que têm servidores em vários países. E mais recentemente houve uma grande utilização também de algumas nuvens, as quais, às vezes, são de difícil identificação, pois não se sabe a que país pertencem.

Então, isso torna o espaço virtual cada vez mais complexo e, por consequência, cada vez mais difícil também de enfrentar e neutralizar os ataques cibernéticos.

A má notifica é que, na verdade, não há regras universais para combater crimes cibernéticos. Existem algumas iniciativas regionais. A União Africana tem regras comuns para enfrentar esse tipo de crime, assim como a União Europeia, os países do Caribe e a Liga dos Estados Árabes. Talvez, a principal convenção, o principal instrumento jurídico que cria regras para tratar e para combater crimes cibernéticos seja a Convenção de Budapeste, que foi negociada no Conselho Europeu no começo da primeira década deste século — acho que no ano 2000 ou 2001.

A Convenção de Budapeste foi negociada no Conselho Europeu, mas, na verdade, ela está aberta à adesão de outros países de fora da região. Outros países como Estados Unidos, Canadá e México já aderiram à Convenção de Budapeste.

O debate internacional sobre esse assunto está muito polarizado. Na verdade, existem os países da Convenção de Budapeste, cujo objetivo é universalizar esse instrumento jurídico, que é um instrumento jurídico regional, e existem outros países, — e o Brasil está dentro desse grupo de países, junto com China, Índia, Rússia —

que pretendem negociar no plano internacional um acordo universal, independente da Convenção de Budapeste.

Então, existem essas duas visões muito distintas sobre a questão do combate ao crime cibernético, e hoje não há perspectiva de consenso — isso do ponto de vista até um pouco cético —, porque o processo de negociação de um instrumento universal anda a passos muitos lentos. Enfim, o processo existe, mas anda a passos muito lentos, e a única perspectiva que nós temos é a de que, talvez, em um horizonte mais largo de tempo, teremos algumas regras mais universais para tratar de crimes transacionais.

Então, na verdade, existe um vazio leal internacional para combater crimes cibernéticos.

Mas, pensando um pouco sobre as Olimpíadas, acho que o que mais importa não é o que fazer depois que acontece um crime cibernético. E todos esses instrumentos que eu falei são instrumentos que regulam a atuação dos Estados, enfim, das entidades, quando ocorre um crime cibernético — não é? Refiro-me às regras para investigação de crime, para manutenção de provas — e este é o grande problema do crime cibernético, porque as provas são sempre muito voláteis, são provas que não existem fisicamente. Então, a preservação da prova é um grande desafio.

Portanto, para as Olimpíadas eu acho que o mais importante não é saber o que será feito quando se comete um crime, mas é prevenir o acontecimento desse crime. E, como se pode depreender do que foi dito em relação às Olimpíadas de Londres, o mais importante é evitar que ocorra um ataque cibernético que comprometa o evento, seja algo que estrague a festa — por exemplo, um apagão no dia da abertura —, seja a manipulação de resultados da competição. Este último é um dos pontos principais de preocupação também. Quer dizer, esses dados dos juízes que estão analisando, que estão fazendo o julgamento de um evento esportivo, estes dados que circulam por sistemas digitais sejam afetados e manipulados. Esta é uma grande preocupação também.

É também preocupação atos que sejam mais complicados e mais complexos que gerem inseguranças, a exemplo da negação de serviços. E isso inclui a questão de interceptação, por exemplo, de sinais de satélites, etc.

O mais importante, então, é a atuação imediata para interromper e neutralizar ataques cibernéticos. Para isso, eu acho que o mais importante, do ponto de vista, pelo menos do Itamaraty, é a cooperação internacional. Ela é fundamental, pois, como eu falei, são ataques que geralmente envolvem mais de um país, às vezes vários países, o que torna muito difícil identificar a fonte desses ataques. Então, é imprescindível trabalharmos com outras agências, com outros países. Isso é absolutamente fundamental.

Mas esse exercício não deve ser confinado ou limitado aos Governos. Também é importante envolver o setor privado, principalmente o setor privado da área tecnológica.

Em Londres, por exemplo, o êxito em conter ataques ao sistema daquela agência de notícias aconteceu em grande parte porque houve uma ação junto a empresas que combatiam os chamados *Spams*. Então, esse foi um elemento importante na neutralização deste tipo de ataque.

No plano doméstico vai haver — e já está havendo, na verdade — uma forte coordenação entre as agências que cuidam da questão de segurança dos jogos. Mas, enfim, os demais apresentadores aqui vão fazer um relato muito mais rigoroso e preciso do que o meu.

Eu só gostaria de citar, então, que nas Olimpíadas do Rio haverá um forte esquema para combater ataques cibernéticos. O Itamaraty, como eu disse inicialmente, não é um órgão operacional do Governo brasileiro; não está nas atribuições do Itamaraty combater operacionalmente crimes cibernéticos. Nós temos um papel mais de negociação de normas internacionais de combate ao crime cibernético. Mas eu acho que temos um papel importante ali de auxiliar as agências que estão envolvidas, que estão no *front* dos combates aos ataques cibernéticos; auxiliar na facilitação da cooperação internacional, nos contatos com os governos estrangeiros, nos contatos com outras entidades internacionais. Enfim, o Itamaraty está disponível e tem uma função importante nessa área.

Gostaria de, mais uma vez, agradecer a oportunidade de compartilhar a visão do Itamaraty sobre isso.

Muito obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada.

Concedo a palavra ao Sr. Marconi dos Reis Bezerra, Diretor do Departamento de Segurança da Informação e Comunicações da Casa Militar da Presidência da República.

O SR. MARCONI DOS REIS BEZERRA - Deputada Mariana Carvalho, Presidente da Mesa; Srs. Deputados Silas Freire e Delegado Éder Mauro, em nome de quem a Casa Militar agradece a oportunidade de estar aqui com os senhores e as senhoras para falar a respeito das ações que a Casa Militar tem realizado para fortalecer a segurança da informação e das comunicações na administração pública federal.

Preparei alguns eslaides. Permitam-me ficar em pé, por favor.

(Segue-se exibição de imagens.)

Preparei alguns eslaides com algumas ideias das atividades que nós temos realizado. Ao final, pretendo passar aos senhores e às senhoras informações sobre ações de curto, médio e longo prazo que temos preparadas, tendo em vista a segurança — e acho que é este o foco principal desta nossa reunião — dos Jogos Olímpicos Rio 2016.

Estamos na Casa Militar da Presidência da República. Somos do Departamento de Segurança da Informação e Comunicações. Aqui nós apresentamos a estrutura atual da Casa Militar, para informação de todos, tendo em vista que foi recente a reestruturação do Governo, a reforma ministerial.

A Casa Militar herdou do então Gabinete de Segurança Institucional da Presidência da República as suas principais atividades.

O nosso Departamento de Segurança da Informação e Comunicações, que anteriormente estava subordinado ao Secretário Executivo do GSI, agora se encontra em uma assessoria especial da Secretaria Executiva do Conselho de Defesa Nacional — CDN, tendo em vista o forte vínculo do Departamento de Segurança da Informação com o CDN e que os normativos e as atividades que nós realizamos ali, em conjunto com o Comitê Gestor de Segurança da Informação — sobre o qual vou comentar mais adiante —, que é órgão de assessoramento do Secretário Executivo do Conselho de Defesa Nacional.

As outras atividades já vinham sendo realizadas pelo GSI. A Casa Militar, então, herdou essas atividades, que vêm prosseguindo normalmente.

Neste eslaide eu coloquei o que foi definido no Decreto nº 8.577, do final do ano de 2015, que estabeleceu as competências da Casa Militar, herdadas do GSI.

Destaco apenas algumas delas, vinculadas ao nosso tema aqui, a exemplo das *"atividades de segurança da informação no âmbito da administração pública federal"*. Essas são atividades que a Casa Militar prossegue desempenhando.

Também compete à Casa Militar da Presidência da República *"apoiar técnica e administrativamente o funcionamento do Conselho de Defesa Nacional — CDN"*, tendo em vista o que já comentei, mas vou destacar novamente um pouco mais à frente, sobre o Comitê Gestor de Segurança.

Essa é a nossa estrutura do Departamento de Segurança da Informação e Comunicações, com as Coordenações-Gerais. Vou falar um pouco de cada uma delas mais adiante.

Ali está a nossa vinculação de coordenação com o Comitê Gestor de Segurança da Informação — CGSI e o vínculo de assessoramento ao Conselho de Defesa Nacional.

O Comitê Gestor de Segurança da Informação é um órgão de assessoramento ao Secretário Executivo do Conselho de Defesa Nacional. Reúne-se mensalmente no Anexo I do Palácio do Planalto, e o Diretor do Departamento de Segurança da Informação e Comunicações — DSIC é o coordenador dessas reuniões.

No âmbito desse Comitê, são elaborados todos os normativos que temos em vigor, que, segundo o TCU estabeleceu em alguns acórdãos, são obrigatórios para todos os órgãos da administração pública federal. Esses são normativos e instruções que regulam a segurança da informação no âmbito da administração pública federal, os quais são publicados no âmbito do Comitê Gestor de Segurança.

Falo agora sobre cada uma das coordenações, conforme comentei com os senhores.

Há a Coordenação-Geral de Gestão do DSIC. É a coordenação mais próxima da elaboração de normas e capacitação de servidores. Isso tudo é realizado com a participação do Comitê Gestor, composto por 17 Ministérios que se reúnem conosco e elaboram esses normativos publicados no âmbito da Casa Militar.

Outra coordenação nossa, a Coordenação-Geral do Centro de Tratamento de Incidentes de Segurança de Redes de Computadores, tem a missão principal de operar e manter o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal — é o nosso CTIRGov. Vou falar um pouco mais sobre o Centro mais adiante.

E há a Coordenação-Geral do Núcleo de Segurança e Credenciamento, que foi fortalecida com a Lei de Acesso à Informação, de 2011, regulamentada em 2012.

Nessa Coordenação está o Núcleo de Segurança e Credenciamento, que é o órgão central de credenciamento e segurança, que credencia empresas, órgãos públicos e privados e pessoas para o tráfego da informação classificada, conforme previsto na Lei do Acesso.

Essa Coordenação também assessora o Chefe da Casa Militar na formulação de acordos internacionais de troca e proteção mútua de informação classificada com outros países.

Aqui eu coloquei apenas a legislação pertinente ao tema que estamos abordando. Para as nossas atividades no âmbito da Casa Militar, eu destaco apenas o Decreto nº 3.505, de 2000, que instituiu a Política de Segurança da Informação e o Comitê Gestor da Segurança da Informação.

Ele era coordenado, na oportunidade, pelo GSI. Destaco também o Decreto nº 5.772, de maio de 2006, que criou o DSIC, e a Medida Provisória nº 696, de 2015, que vem passando por reformulações — já passou pelo Governo —, mantendo agora a competência de coordenar as atividades de segurança da informação no âmbito da administração pública federal.

Isso consta da Medida Provisória nº 696, que já passou pela Câmara e pelo Senado. Estamos aguardando a promulgação da lei.

Há outras leis amparam nosso trabalho, mas apenas deixo o registro.

Aqui está apenas um *flash* de uma das reuniões do nosso Comitê Gestor da Segurança da Informação. Como eu comentei, ele foi instituído no ano 2000 pelo Decreto nº 3.505, assim como a Política de Segurança da Informação para todos os órgãos da administração pública federal.

Esse Comitê foi criado em 2000 e, partir de 2006, com a criação do DSIC, começou a se reunir. Em 2008 houve a primeira instrução normativa.

Vou mostrar aos senhores algumas delas, que já foram publicadas e estão disponíveis no nosso *site.*

O Comitê é composto de 17 órgãos. Ele é coordenado pela Casa Militar da Presidência da República e dele participam outros 16 Ministérios, que se têm reunido conosco mensalmente no Anexo I do Palácio do Planalto.

Aqui, meus senhores, eu coloquei alguns acórdãos que o TCU tem publicado nas suas auditorias de órgãos da administração pública federal. Ele ressalta que as normas publicadas pelo então GSI, agora Casa Militar, são obrigatórias. Elas não são facultativas, e sim obrigatórias para a Alta Administração.

No Acórdão nº 1.233, de 2012, inclusive, o TCU enfatiza isso e nomeia também o GSI como órgão governante superior em questões de segurança da informação e comunicações.

Nesse mesmo acórdão, ele elenca outros 12 órgãos governantes superiores, cada um numa determinada atividade. O GSI foi eleito, na oportunidade, para questões de segurança da informação.

Outro acórdão que destaco é o Acórdão nº 3.051, de 2014, que enfatizou, mais uma vez, a obrigatoriedade das normas. Ele enfatiza a Norma Complementar 2, que é uma norma de planejamento de ações de SIC. Ele reforça que o GSI tem desempenhado um papel preponderante na regulamentação do setor e na promoção de ações de capacitação e também recomenda que o GSI elabore uma estratégia geral de segurança da informação.

Esse acórdão é de 2014; em 2015, ano seguinte, nós já publicamos nossa estratégia de segurança da informação para toda a administração pública federal.

São apenas dois os acórdãos que eu destaco. Eles têm sido lembrados em todas as auditorias que o TCU realiza nos órgãos da administração pública federal.

Alguns conceitos, meus senhores, só para nós focarmos a nossa atividade principal, que é de segurança da informação e defesa cibernética para os Jogos Olímpicos Rio 2016. Nós estamos falando de segurança da informação e comunicações.

O que é segurança da informação e comunicações? Esta definição consta da primeira instrução normativa, que publicamos em 2008. Isso está definido lá

textualmente como *"ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações"*.

Essa é uma dica que nós vimos passando para todos os órgãos da APF, sempre que demandados a respeito da segurança que deve ser dada para as suas informações. Essa é a nossa dica para todos os órgãos da APF.

Ali eu coloquei a abrangência dessa dica. Muitas vezes se pensa que segurança da informação envolve apenas tecnologia, computadores e redes, mas não é só isso. Ela envolve os recursos humanos; envolve todos os sistemas de informação, *software* e *hardware*; envolve as áreas e instalações; e envolve os recursos materiais, os prédios onde esses equipamentos estão instalados. Todos os ativos de informação estão envolvidos na SIC.

Outra definição muito importante são os ativos de informação. O que são ativos de informação? Também não é apenas tecnologia; os recursos humanos sempre estão presentes ali. Ativos são os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais; e os recursos humanos.

Nós costumamos dizer que o elo mais fraco na cadeia de segurança da informação é o ser humano; que às vezes esquece um papel em que há uma informação sensível em cima da mesa; que se esquece de trancar a gaveta; que utiliza um meio inseguro para se comunicar. Portanto, é sempre o ser humano o elo mais fraco da cadeia. A tecnologia pode estar no estado da arte, mas, se a pessoa deixa alguma falha, por esquecimento ou por algum motivo qualquer, fica fragilizada, então, toda a segurança da informação. Todo aquele investimento em tecnologia que se buscou fica fragilizado diante dessas questões que envolvem a fragilidade do ser humano.

Como eu disse aos senhores, aqui temos as normas já publicadas. Nós temos a Instrução Normativa nº 1, de 2008, que falava sobre a gestão de SIC de uma maneira geral; e, de 2008 até 2015, nós já publicamos 21 normas complementares, com o auxílio do Comitê Gestor de Segurança da Informação.

Essas são normas que cobrem todo o espectro da segurança da informação na gestão de risco; nas equipes de tratamento de incidente de rede, como o órgão deve montar uma equipe, como ele deve treiná-la, quais os pré-requisitos que esses

servidores devem atender; como tratar a gestão de incidentes em redes; como utilizar recursos criptográficos. Sobre todos esses temas nós temos um normativo que orienta o órgão. Caso ele queira implementar algum deles, apresentamos quais as condições e os pré-requisitos que devem ser atendidos para que ele cumpra o previsto nesse normativo.

Temos aqui uma de nossas coordenações, que é a Coordenação-Geral de Gestão de SIC. Realizamos um grande trabalho de capacitação e conscientização dos servidores da administração pública. Desses mais de 1 milhão de servidores que nós temos na administração pública federal, já há mais de 50 mil servidores sensibilizados e mais de 6 mil capacitados. Varia apenas a questão da duração do treinamento: 40 horas, 1 semana ou às vezes um treinamento de 2 dias.

Nós temos mais de 300 especialistas em gestão de SIC que foram formados num acordo realizado entre o então GSI e a UnB. Foram quatro versões desse curso de Mestrado em Gestão de Segurança da Informação. Mais de 300 já foram formados e estão trabalhando hoje em toda a administração pública federal. Isso gerou um arcabouço de mais de 2.200 casos de estudo, que foram apresentados por esses alunos. Nós temos realizado inúmeras oficinas e colóquios técnicos no anexo do Palácio do Planalto e em outros locais. Já foram realizados também em outras cidades do Brasil, em eventos para os quais convocamos o pessoal, a fim de trocarem ideias a respeito da segurança da informação.

Aqui temos a Coordenação-Geral do Centro de Tratamento de Incidentes de Rede. Vou discorrer a respeito apenas de alguns números sob essa coordenação. Ela monitora hoje mais de 320 grandes redes de computadores. Quando digo “grandes redes” são redes de presença nacional, em todo o ponto do território nacional. O Exército Brasileiro, por exemplo, bem representado aqui, é uma das redes que nós monitoramos — nós acompanhamos a situação dela. A rede dos Correios também é monitorada. O Ministério da Saúde, que está presente em todos os Municípios brasileiros, também tem sua rede monitorada. Então, são grandes redes que são monitoradas a respeito de tentativas de ataques, pichações, etc. Essas redes são monitoradas pelo nosso CTIR Gov.

Nós recebemos notificações de mais de 180 Equipes de Tratamento e Respostas a Incidentes de Rede — ETIR nos órgãos da administração pública federal.

Diariamente nós recebemos em torno de 80 incidentes não resolvidos por essas ETIR em todo o Brasil. Nós recebemos e fazemos o devido tratamento. Isso gera notificações a quem foi atacado, e, caso tenhamos alguma informação a respeito do atacante, temos um canal direto, então, com a Polícia Federal, a quem passamos aqueles dados disponíveis para que sejam tomadas as providências.

Quarenta e oito por cento desses incidentes encaminhados ao CTIR Gov são resolvidos em até 24 horas. Os que não são resolvidos não dependem de nossas ações, do CTIR Gov. São contatos de gestores de segurança dos órgãos que não foram encontrados ou estão de férias, ou o desenvolvedor do sistema não foi localizado para que seja sanado aquele problema. São vários tipos de ocorrências que podem retardar a solução desse incidente.

Ali eu destaco os dois centros de tratamento acreditados internacionalmente. No Brasil, nós temos o CERT.br, lá em São Paulo, que cuida da Internet em âmbito comercial e civil, e o CTIR Gov, que monitora as redes de Governo. Tudo que é .gov., .mil, .leg., .jus, enfim, tudo que é de Governo está a cargo do CTIRGov, localizado em Brasília, e no restante da rede está o nosso CERT.br, lá em São Paulo.

Ainda sobre a Coordenação-Geral do Centro de Tratamento de Incidentes de Redes, já focado no objetivo principal da nossa reunião, segurança para os Jogos Olímpicos e Paraolímpicos Rio 2016, nós temos uma atuação conjunta do CTIR Gov com diversas entidades do Governo Federal. O CTIR Gov, nos Jogos Olímpicos, operará com outras ETIR, aquelas mais de 180 que já comentamos, bem como o CDCiber, o CERT.br, por conta do Comitê Gestor da Internet — CGI.br, o SERPRO/Ministério da Fazenda, entre outros.

Esse trabalho conjunto visa mitigar a incidência de segurança na rede e consta de uma Portaria Interministerial assinada, em 2015, pelo Ministério da Justiça, pelo Ministério da Defesa e pelo então GSI, que aprovou o Plano Estratégico de Segurança Integrada para os Jogos Olímpicos e Paraolímpicos Rio 2016, já em plena execução.

Aqui eu destaco, meus senhores, a nossa Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da APF.

Como eu já comentei lá atrás sobre aquela recomendação do TCU, em 2014 começamos a realizar um estudo interno, com a participação do Comitê Gestor, e, em maio de 2015, essa estratégia foi aprovada por uma portaria do Secretário-Executivo do Conselho de Defesa Nacional.

Essa estratégia tem a missão de fortalecer a política e o planejamento de SIC. O objetivo principal, aquele que dá o norte a essa estratégia, é fortalecer a política e o planejamento de SIC e a Segurança Cibernética na APF, visando assegurar e defender os interesses do Estado e da sociedade para a preservação da soberania nacional. Essa estratégia tem 10 objetivos estratégicos e 38 metas estratégicas que vigoram nesse período de 2015 a 2018.

A respeito da estratégia, ainda, tenho um breve relato sobre o mapa estratégico. Nós temos aqueles dez objetivos estratégicos, divididos em quatro eixos. O primeiro deles, lá em cima, com resultados para a sociedade. A estratégia também é voltada para a sociedade, porque não adianta a administração pública federal atuar, proteger as suas redes, se a sociedade estiver fragilizada. Então, há objetivos na estratégia que visam fortalecer os resultados da segurança para a sociedade. Alguns deles são voltados para o Governo; outros para aprendizado, crescimento e inovação — alguns objetivos têm a participação do MCTI e dos órgãos de pesquisa e desenvolvimento —; e há um objetivo estratégico voltado para a parte de planejamento orçamentário de segurança da informação.

Aqui, já me aproximando do final, eu gostaria de passar para os senhores algumas ações que nós temos planejado tendo em vista a proximidade dos Jogos Olímpicos e Paraolímpicos Rio 2016.

Ontem nós tivemos uma reunião na Casa Militar com o Chefe do Centro de Defesa Cibernética. Já fizemos uma primeira aproximação para traçar ações que poderemos realizar em conjunto, até porque ele está com a missão de coordenar as ações de segurança e defesa cibernética para esse evento especificamente. Nós definimos ali algumas ações de curto prazo, as duas primeiras mais a cargo da Casa Militar, em que pretendemos, em um primeiro nível político e estratégico, alertar a alta administração da APF, por meio de correspondência oficial no início de abril —

pretendemos fazer isso —, para as medidas preventivas em prol da segurança da informação e da segurança cibernética. O nosso Chefe da Casa Militar vai expedir um ofício a todos os Ministérios alertando para as questões de segurança, recomendando a devida segurança das suas redes, em um nível mais alto, para o conhecimento de todos.

Em um nível estratégico e de gestão, estamos agendando para 13 de abril o dia da próxima reunião do Comitê Gestor de Segurança da Informação, que vai ser realizada no anexo do Palácio do Planalto, uma reunião ampliada do Comitê Gestor. Não se trata apenas de reunião com os membros do Comitê Gestor, mas pretendemos também convidar os gestores de segurança da informação e de tecnologia da informação de toda a administração pública federal, visando reforçar aquele alerta, que já passamos para a alta administração, sobre as medidas preventivas de segurança da informação e segurança cibernética.

Em um nível mais técnico-operacional, nós pretendemos também convocar uma reunião de coordenação do CTIR Gov com as Equipes de Tratamento de Incidentes de Redes — ETIR da APF, para o estabelecimento de protocolo especial, por ocasião dos Jogos Olímpicos, prevendo acompanhamento de 24/7 das redes de Governo e um plano emergencial de notificações. Essa é uma atividade que nós estamos planejando em um nível mais técnico-operacional, o que pretendemos fazer ali em ordem cronológica.

Por último, queremos reunir os técnicos para debatermos melhor esse tema no Palácio.

Apresento aqui algumas ações de médio e longo prazo, que também já estão em execução. Eu comentei bastante aqui sobre a estratégia de segurança da informação, mas nós temos também a Estratégia de Governança Digital da administração pública federal, que é uma estratégia publicada pelo Ministério do Planejamento, Orçamento e Gestão no início deste ano.

Ambas as estratégias deixam bem clara essa questão de que a Casa Militar é o órgão central da governança de SIC e SegCiber na APF. Ela deverá promover a formulação de uma Política Nacional de Segurança, que nós não temos ainda no Brasil. Aquela Política de Segurança da Informação, de 2000, o Decreto nº 3.505, é para a administração pública federal. Ela não abrange os outros Poderes.

Precisamos realmente de uma Política Nacional de Segurança da Informação e Comunicações e de Segurança Cibernética que abranja todos os Poderes. Esse é um dos objetivos da nossa estratégia. Também a estratégia da EGD, do MPOG, diz que a Casa Militar é o responsável pela formulação de ações no sentido de que publiquemos, no curto prazo e no médio prazo.

O SR. PRESIDENTE (Deputado Silas Freire) - Por favor, caminhe para a conclusão.

O SR. MARCONI DOS REIS BEZERRA - Muito obrigado.

Era isso que eu tinha a apresentar.

O SR. PRESIDENTE (Deputado Silas Freire) - Muito obrigado, sem dúvida nenhuma, Sr. Marconi dos Reis Bezerra, que muito contribuiu e deve continuar contribuindo com o nosso seminário.

Com a palavra, agora, o Coronel José Ricardo Souza Camelo, Chefe da Divisão de Operações do Centro de Defesa Cibernética — CDCIBER, organização do Exército, que dispõe de até 20 minutos.

Ele também pode fazer uso dos instrumentos para sua demonstração.

O SR. JOSÉ RICARDO SOUZA CAMELO - Boa tarde a todos.

Sr. Deputado, Sra. Deputada, autoridades, senhoras e senhores, meus cumprimentos.

Em primeiro lugar, agradeço a oportunidade, em nome do General Carvalho, Comandante de Defesa Cibernética. Já há um novo termo que eu também vou mostrar aqui. Temos o nascimento do Comando de Defesa Cibernética a compor, com o Centro de Defesa Cibernética, mais uma unidade que está 100% voltada para a defesa cibernética da Nação.

Nós sempre iniciamos as nossas apresentações com esses *slides* em que mostramos algumas cenas operacionais, ou do nosso cotidiano, mas que enfatizam sempre a parte do nosso pessoal. A cibernética, apesar de toda a matemática, lógica e eletrônica envolvidas, não resiste, mesmo com toda a automatização que se pode colocar, sem um ser humano bem treinado e bem capacitado, e os talentos sendo utilizados. Isto é uma coisa que o comando de defesa cibernética trabalha já desde a criação, quando núcleo do Centro de Defesa Cibernética, em 2009, para

que nós formemos massa crítica para trabalharmos nesta área extremamente complexa.

Infelizmente, a definição não está tão boa, mas outra expressão chave para nós é “ação colaborativa”. Eu até brinco com meus companheiros, lá do Centro de Defesa Cibernética: não há vida possível na defesa cibernética sem colaboração. Nós não somos autossuficientes, por mais adiantados que sejamos em termos de produto tecnológico, processos e *experts* trabalhando na área. Não há como extrapolarmos toda a demanda existente em segurança e defesa cibernética.

Nós utilizamos muito esta frase: a defesa cibernética como extensão do papel constitucional das Forças Armadas na defesa nacional. É óbvio que nós não estamos insinuando nenhum tipo de mudança na Constituição. Apenas queremos chamar atenção para o fato de que esse dito mundo virtual é uma nova dimensão de combate, e as Forças Armadas estão, desde a edição da estratégia nacional de defesa, na sua primeira versão, em 2008, se adaptando e se modernizando justamente para fazer jus ao que o Brasil merece em termos de sua defesa também no espaço cibernético.

Sem querer gastar aqui o nosso tempo com partes não tão voltadas para o nosso objeto, os Jogos Olímpicos, é sempre bom enfatizar que esse espaço cibernético — e muitas vezes o nosso contato dá-se mais em filmes de ficção como algo meio fantasmagórico — realmente extrapola, vaza entre os nossos dedos, utilizando aqui uma metáfora. Ele não tem nenhum tipo de limitação física. Os *bytes* que trafegam pelos meios de comunicação não “vestem uniformes”, como diz um colaborador nosso, ou seja, não são tão identificáveis. Então, aquilo que serve para o bem também serve para o mal.

Um dos principais ataques, e até citado pelo conselheiro ali, que é denegação do serviço, são ataques formados por tráfego legítimo. É um dos ataques mais medievais e também mais eficazes contra as estruturas e sistema de informação. Então, é algo que temos que ter sempre em mente.

A incerteza da segurança é uma notícia não muito boa. Nunca haverá 100% de segurança no que diz respeito à segurança de defesa cibernética, e sempre trabalhamos com modelo de mitigação do risco, diminuindo o risco, convivendo com alguma coisa residual. A facilidade do acesso ou a facilidade de uso de tecnologia

funciona como um canto da sereia — pois aqui, se desligarmos nossos celulares, a maioria de nós vai até passar mal porque é quase que um órgão vital —, e está mais do que provado que até pelo celular podemos ser espionados. No Centro de Defesa Cibernética, por exemplo, não usamos celular. Há esse tipo de restrição por questão de segurança.

Esse cenário vem de várias literaturas, mas, no nosso trabalho prático, todo dia ele é confirmado. Então, em termos de ameaça cibernética das principais categorias, nós enxergamos o crime, o terrorismo, a espionagem e as ações, em uma situação mais extrema, de guerra, propriamente, cibernética.

No caso do crime — e não é a área de defesa, é área policial —, muitas vezes, tropeçamos em coisas que estão envolvidas com o crime. Aí usamos a nossa parceria com a Polícia Federal.

Em relação ao terrorismo, mais usual por cooptação e obtenção de recursos humanos através das redes sociais, mas nada impede que seja utilizado também, como bem lembrou o Conselheiro, para provocar tragédias pelo mundo virtual, e ainda bem que isso não aconteceu significativamente. Aconteceram alguns episódios — a literatura aborda alguns casos reais —, mas de grandes proporções e, em particular, em grandes eventos não ocorreram, e esperamos que não aconteçam.

Quanto à espionagem industrial e à de Estado, os escândalos recentes dispensam comentários. Os hacktivistas são atores a princípio sem coordenação ou sem causa — dizem que têm uma causa. Eles atacam de maneira caótica e têm um grande poder. Muitos deles têm *expertise* técnica fantástica. Para nossa sorte, também não são tão coordenados; quando se coordenam, viram criminosos. Há esse outro lado também, incomodam bastante, principalmente nos grandes eventos.

Por fim, outro campo de batalha hoje é a possibilidade de resolvermos guerras utilizando a cibernética. Isto não é ficção científica. Eventos reais muito claros e muito bem documentados já mostraram isso. Não é brincadeira, realmente.

Traçado esse cenário, no que as Forças Armadas estão trabalhando para materializar sua ação no que diz respeito à defesa nacional? Foi criado o Comando de Defesa Cibernética — CDCiber, coisa de poucos dias. Até uma curiosidade: eu brinco, às vezes, que o pai nasceu depois do filho. O Centro de Defesa Cibernética

foi criado como Núcleo em 2010 e depois foi ativado como Centro, definitivamente, em 2012. Trabalhou em todas as questões cibernéticas, das letras A a Z. Obviamente, nosso trabalho foi sempre muito pesado e agora começamos a dividir um pouco mais as tarefas, sendo que a parte estratégica fica com o Comando de Defesa Cibernética, cujo comandante é o General Carvalho, e o nosso lema é de coordenação e integração. O braço operacional é o Centro de Defesa Cibernética. Em termos experimentais, estamos trabalhando com a parte de ciência e tecnologia, parte de doutrina, parte de inteligência, estratégia e capacitação de pessoal. E o Centro de Defesa Cibernética, em linguajar militar, trata da parte, realmente, de combate.

Vou passar um *slide* que o nosso Comandante nunca deixa de mostrar nas suas apresentações, e que para nós é muito importante: é este átomo estilizado, que representa, que sintetiza nossas preocupações. O núcleo do átomo, propositadamente, são os recursos humanos.

Como eu enfatizei logo no início, e o primeiro *slide* tenta demonstrar, sem recurso humano capacitado e motivado — e, muitas vezes, o talento está sendo descoberto, utilizado, motivado e está trabalhando conosco —, nós não vamos muito longe, mesmo com toda a parafernália tecnológica de que dispomos hoje em dia.

Naturalmente, a ciência e tecnologia são indispensáveis. Não só há a questão de comprar caixinhas na loja de *software*, mas devemos desenvolver, como país grande que somos, a parte de ciência e tecnologia. Isto é extremamente importante.

Temos uma parceria com o Ministério da Ciência, Tecnologia e Inovação nesse sentido e que tem dado já os primeiros frutos; a doutrina para disciplinar como esse instrumento de combate entra no cenário de defesa; a inteligência, como área fundamental de apoio à decisão, de busca da informação, para apoio da decisão dos comandos envolvidos. A inteligência clássica, feita com todas as fontes, tem seus limites e seus processos baseados em seres humanos. Em cibernética, eu tenho milhões, bilhões, trilhões e, acima disso, informações digitais que precisam ser digeridas por tecnologia. Aí juntamos muito o processo de inteligência e o processo de ciência e tecnologia; e as operações que definem — desculpem-me abusar um pouco do linguajar militar — a manobra, ou seja, como o combate vai ser feito.

Tudo isto é emoldurado pela segurança da informação e comunicações. Como enfatizou anteriormente o General Marconi, esta é a base da segurança cibernética e da defesa, com amparo legal.

Ainda que existam alguns vácuos legais no que diz respeito à legislação brasileira, se comparada a outros países, é muito importante ficar explícito aqui que as Forças Armadas trabalham sempre se pautando por todo instrumento legal disponível ou o que, por analogia, pode ser utilizado no uso da cibernética. Isto é muito importante por conta de, às vezes, algumas interpretações errôneas no uso da própria cibernética que podem existir.

No que se refere à mobilização da capacidade cibernética, quando usamos a palavra mobilização, significa que estamos obtendo meios fora da Força, ou seja, não temos a pretensão, no Ministério da Defesa, de que a defesa nacional esteja limitada ao pessoal da uniforme.

Em termos de cibernética, é uma lição aprendida muito nítida e que não pode nunca ser esquecida. Às vezes, um procedimento simples dentro da nossa casa com o nosso filho, que está lá em um joguinho que baixou da Internet, pode fazer uma diferença imensa em um processo de obtenção de uma informação crítica para um governo. Isto fica muito nítido, é uma lição muito clara na cibernética.

Afunilando agora para o nosso objeto principal, os Jogos Olímpicos, em que o Centro de Defesa Cibernética — a unidade do combate, vamos dizer assim — está trabalhando? Aqui aparece uma nova sigla, o CCSDCiber. Já vou explicar o que é.

Esse primeiro parágrafo é um extrato do nosso plano operacional no que diz respeito aos Jogos Olímpicos. Então, a redação pelo rito militar fica desta forma:

> *"A fim de cooperar com o Estado-Maior Conjunto das Forças Armadas, o Comando Geral de Defesa de Área* — os Comandos de Defesa de Área são comandos instituídos para os Jogos Olímpicos no Rio de Janeiro —*, os Comandos Centralizados e os CDSs* — os CDSs também no Rio de Janeiro, e os CDAs são nas cidades-sede do futebol —, *mais o EMCFA, na garantia da segurança dos Jogos Olímpicos e Paraolímpicos 2016, coordenar e integrar* — estas são duas palavras-chave —

num ambiente interagências — também é outra expressão-chave — *as atividades de Segurança e Defesa Cibernética contra ações cibernéticas hostis."*

Ali embaixo está a legislação que nos ampara. Só enfatizando, a questão da coordenação e integração: a coordenação é o trabalho conjunto para estabelecer estratégias entre as agências envolvidas, em particular para compartilhamento das informações sobre o espaço cibernético, de tal modo a protegê-lo proativamente ou, se for o caso, reagir com prontidão a algum tipo de violação de segurança; e a integração, além de compor um time que trabalha como um sistema entre todas as agências, adiciona valor, no caso do Centro de Defesa Cibernética, em particular com instrumentos de gestão de risco, parte de pesquisa e análise sobre o espaço cibernético, gestão e tratamento de incidentes de rede e diagnósticos de riscos específicos em redes com as quais nós temos governança.

A sigla CCSDCiber é do rito terminológico do Ministério da Defesa. Então, há comandos centralizados, como nós chamamos, e a entidade que responde, dentro do Ministério da Defesa, pela defesa cibernética é o Centro de Coordenação de Segurança e Defesa Cibernética, que nada mais é que o Comando de Defesa Cibernética ou o Centro de Defesa Cibernética e a equipe que vai para o combate, que nós chamamos de Destacamentos de Defesa Cibernética, destacamentos compostos pelas três Forças. Eles vão estar presentes em todas as cidades-sede dos eventos olímpicos, nas cidades-sede do futebol e, obviamente, no Rio de Janeiro.

Apesar de todo o mundo virtual a que nos referimos em relação à cibernética, percebemos que o contato humano é essencial também, até porque muitas das vezes, como aqueles que nós vamos compor a defesa não entendem tanto do negócio de segurança cibernética, nossa presença física pode fazer uma diferença brutal em termos de reação ao incidente ou prevenção a esse tipo de evento.

Nós temos aproximadamente 120 pessoas — ali estão 117. Esse número, com o planejamento, vem sendo ajustado — que vão compor todos esses destacamentos, sendo que o destacamento de Brasília é o destacamento central, é a cabeça do sistema.

Aqui temos um *zoom* na área do Rio de Janeiro. Nós temos aí o CGDA, o Comando Geral de Defesa Diária, que é a estrutura de segurança das Forças Armadas no Rio de Janeiro, não é só de cibernética. Nós vamos compor o time deles lá, e da mesma forma, os centros de defesa setoriais em quatro regiões — Deodoro, Maracanã, Copacabana e Barra — vão ter de brigadas responsáveis por essas áreas. O Distrito Naval também, se não me engano — não me lembro agora da região —, terá uma unidade da Marinha e outras do Exército, em que estaremos também presentes fisicamente, com nossa parafernália tecnológica, apoiando em particular a proteção das redes de comando e controle que vão dar sustentação e proteção às equipes de segurança e de defesa.

Bom, se não me engano, esse é o meu penúltimo ou último *slide*. Os meus colegas do centro, autores dessa figura, juram que ela é autoevidente. Eu não vou torturá-los explicando ponto por ponto, mas ela sintetiza como são esses destacamentos. Eu acabei não explicando, mas uma fração da unidade principal, no caso do centro de defesa cibernética, vai para o "campo" — entre aspas —, para o combate direto.

Esse destacamento representa o destacamento tanto de Brasília, quanto os destacamentos remotos. Ali na posição do centro, um pouco à direita, ele representa o destacamento de Brasília. Ele é subdividido em uma sessão de inteligência que trabalha com toda a comunidade de inteligência brasileira, obtendo informações da fonte cibernética para apoio e decisão. Tem uma seção de operações que trabalha tanto com monitorações automáticas de sensores espalhados pelas nossas redes, redes em que nós temos governança, quanto de parceiros, que nós acompanhamos o *status* de alguns dos seus serviços que são voltados para Internet, monitoramos e detectamos anomalias de forma automática, o que é representado ali na parte de baixo. E, na parte de cima, no canto superior direito estão os nossos parceiros: Sete BR, CTIR Gov, CERT, SERPRO, Polícia Federal, ANATEL, as equipes de tratamentos de incidentes das demais forças.

Toda essa comunidade compartilha informações sobre o espaço cibernético de tal forma que, se uma violação for feita, tenhamos uma reação técnica adequada oportuna, ou tenhamos uma forma também de prevenir, detectando mobilizações ou

violações de segurança que podem levar a um mal maior, neutralizando essa ameaça.

Essa neutralização, esse tipo de ação, varia muito, porque os processos técnicos dependem do tipo de violação de segurança do qual estamos falando. Já este é um assunto um pouquinho mais técnico, e não teríamos tempo para explorar todos aqui.

Mas, de um modo geral, até o Conselheiro também colocou aqui algumas categorias: os famosos *spams*, os famosos *Phishing* são terríveis. Houve até um evento grave, durante a Copa do Mundo, envolvendo um órgão da administração pública, alguns tipos de invasões também aconteceram, como no Twitter de outra instituição, que por pouco não provoca tragédia num estádio. Ainda bem que talvez esse lado assim um pouco mais brincalhão brasileiro tenha ajudado nessa hora, porque era uma ameaça de bomba que foi tuitada meia hora antes do jogo Brasil e Chile. Então, depende muito tipo de evento, o tratamento técnico que é dado.

Bom, esse é meu último *slide*, enfatizando mais uma vez a nossa ação colaborativa. Essa constelação aí é cada vez maior. Às vezes, até por questões de não tumultuar muito o quadro, a simplificamos, mas temos parcerias com universidades, com unidades militares, com empresas privadas, com instituições de pesquisa, além das universidades propriamente ditas, com organizações da administração pública federal, com times de segurança públicos e privados, com times de segurança internacionais.

Então, como eu disse, nós consideramos impossível trabalhar com cibernética sem uma parceria forte. Isso se baseia num processo de construção de confiança que pode ser destruído em alguns minutos e demora anos para ser reconstituído. É um trabalho no qual o Centro de Defesa Cibernética agora, o Comando e o Centro vêm trabalhando muito firme, muito delicado, muito lento.

Às vezes dá fruto só anos depois, como nós estamos colhendo frutos hoje do começamos lá em 2008, 2009, mas que é extremamente precioso para nós. Mas fazemos questão de divulgar isso para ressaltar a relevância dessas unidades para nós. A parceria com a ANATEL, com o Ministério das Relações Exteriores, o SERPRO, a Polícia Federal, a Marinha, a FAB, estruturas críticas, como, por

exemplo, Itaipu, Ministérios, como MCTI, a Casa Militar, o CERT, as universidades. Isso para nós é ouro puro.

Sra. Deputada, termino por aqui.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Muito obrigada, Coronel.

Eu concedo a palavra ao Sr. William Murad, Diretor de Inteligência da Secretaria Extraordinária de Segurança para Grandes Eventos.

O SR. WILLIAM MURAD - Deputada Mariana, boa tarde, colegas da Mesa, demais Parlamentares, senhoras e senhores, inicialmente, tentarei aqui sintetizar as linhas gerais do planejamento de segurança dos Jogos Olímpicos Rio 2016. Em seguida, vou tentar aproximar a questão central deste seminário em relação a esse planejamento.

É importante destacar de início que os Jogos Olímpicos são o maior evento do mundo. Talvez os senhores e as senhoras já tenham ouvido falar dos números, mas eu vou destacar aqui alguns deles para que nós tenhamos uma pequena ideia da sua dimensão.

Nos Jogos Olímpicos, haverá aproximadamente 15 mil atletas, entre atletas olímpicos e paraolímpicos. Na Copa do Mundo, houve cerca de 800 atletas. Na Copa do Mundo, houve um campeonato mundial. Nos Jogos Olímpicos, houve 42 campeonatos simultâneos em quatro regiões olímpicas do Rio de Janeiro e em mais cinco cidades do futebol.

Em alguns dias de evento, haverá mais de 1.500 deslocamentos em um único dia da Vila dos Atletas para as demais regiões olímpicas. Ao final dos jogos, haverá aproximadamente 30 mil deslocamentos. Esses números dão um pouco a dimensão que tem esse evento.

Obviamente, quando falamos de segurança pública ou de segurança *lato sensu*, a complexidade vem junto. Quando nos deparamos com todos os elementos para se desenhar e se fazer um planejamento dessa magnitude, o pilar central que guia todo o processo é sem dúvida o pilar da integração.

Não se concebe falar em planejamento de segurança sem se falar em integração. E aqui, quando me refiro a esse termo, a integração não é aquela

integração da boca para fora. Não pode ser a integração da boca para fora. A integração tem que ser efetiva, sob pena de termos resultados desastrosos à frente.

Ainda em relação à integração, nós podemos dividi-la, na verdade, em três campos. O primeiro deles é a integração entre os eixos. Os principais eixos que atuam na segurança de modo geral. O primeiro eixo é o de segurança pública. Nós temos o eixo de defesa nacional e temos o eixo da inteligência. Esses três eixos têm que se integrar de maneira precisa para que o resto do planejamento seja coeso.

Nós temos uma demonstração muito clara de entrosamento em relação a esses três eixos, que é o plano estratégico de segurança integrada, publicado no ano passado. O plano foi construído por representantes da segurança pública, pelo Ministério da Justiça e por representantes do Ministério da Defesa. Também a Casa Civil da Presidência da República e a Agência Brasileira de Inteligência participaram diretamente disso. Esse plano traz aspectos importantes e relevantes que guiam todo o restante do planejamento a que me referirei em seguida.

O segundo ponto da integração que é importante, e aí já falo especificamente da segurança pública, é a integração entre os órgãos de segurança pública nos três níveis de Governo, ou seja, entre os órgãos federais, do Estado e do Município que tenham relação com a segurança pública — na verdade, não só os que tenham relação com a segurança pública, mas todos aqueles cuja atividade, de alguma forma, impacte a segurança pública, como os órgãos de trânsito, entre outros.

Por fim, o terceiro pilar da integração é o relativo à cooperação internacional, citada inclusive aqui pelo colega do MRE.

Enfim, não se pode conceber um planejamento de segurança sem falar em integração. Também é importante que se diga que ninguém inventa a roda. O planejamento de segurança segue necessariamente experiências que nós tivemos no Brasil, em grandes eventos nacionais, ou seja, as lições aprendidas com as boas práticas identificadas e com aquelas que não deram certo, desde o Pan-Americano, passando pelos Jogos Mundiais Militares, pela Rio+20, pela Copa das Confederações, já em 2013, pela Jornada Mundial da Juventude e, por fim, pela Copa do Mundo, em 2014. Todas as experiências colhidas nesses grandes eventos estão sendo utilizadas para a construção do planejamento dos Jogos Olímpicos no que diz respeito à segurança.

Além da experiência em grandes eventos nacionais, o planejamento de segurança incluiu diversas visitas técnicas a inúmeros eventos internacionais, desde os Jogos Olímpicos de Londres, em 2012, passando por inúmeros eventos em diversos lugares: no Canadá, o Pan-Americano; nos Estados Unidos, eventos de grande porte, como o Super Bowl, entre outros; na Europa, a primeira edição dos Jogos Europeus; na China, o Campeonato Mundial de Atletismo; além de maratonas no mundo inteiro — tivemos a oportunidade de visitar a Maratona de Boston, a Maratona de Berlim e a Tour de France. Digo isso aqui justamente para ilustrar que todo o planejamento de segurança traz essa experiência internacional na sua gênese.

Pois bem, a partir disso e da construção, inicialmente, de um Plano Estratégico de Segurança Integrada, foi possível desenhar princípios, metas e, fundamentalmente, estabelecer as atividades por que cada eixo seria responsável em relação à segurança para os Jogos Olímpicos.

No caso da questão cibernética, foi atribuída ao Ministério da Defesa a defesa cibernética, como bem explicado pelo Coronel José Ricardo, em relação ao CDCiber e a investimentos que foram recebidos para essa defesa.

No que diz respeito à segurança pública, gostaria de chamar a atenção para dois aspectos. O primeiro deles diz respeito à questão de crimes em geral praticados pela Internet, o que foi citado aqui também na apresentação anterior.

A investigação de todo e qualquer crime é atribuição das Polícias Judiciárias, seja a do Estado, seja a Polícia Federal, em âmbito federal, e esses órgãos participam ativamente do planejamento de segurança dos Jogos Olímpicos. Nós temos, em cada um dos Estados que estão envolvidos com os Jogos, uma comissão estadual da qual todos os órgãos de segurança pública, nos âmbitos federal, estadual e municipal, participam e dentro da qual debatem aspectos relevantes de segurança pública de âmbito federal, estadual e municipal participam e debatem aspectos relevantes de segurança.

No caso dos crimes cibernéticos, esse é um assunto tratado por parte da Polícia Civil e por parte da Polícia Federal. Há questões específicas e assuntos específicos que decorrem dos Jogos que vêm sendo debatidos nesses ambientes

relativos a esses temas. Mas aqui acredito que o principal tema, que consta pelo menos no convite que me chegou, seria relativo ao terrorismo.

Em relação a esse tema, creio que o mais importante destacar é que, da mesma maneira que destaquei os aspectos de integração tanto no âmbito nacional quanto no âmbito internacional, entre os eixos que participam disso, no campo do terrorismo, não é diferente. Há uma integração bastante sólida entre os eixos de segurança, repito, segurança pública, defesa e inteligência.

No campo internacional, há também uma integração bastante sólida, tanto no que diz respeito aos órgãos centrais de inteligência por parte da ABIN — Agência Brasileira de Inteligência, que terá um centro internacional de inteligência, com diversos órgãos internacionais presentes; como no campo da segurança pública, por meio do Centro Integrado de Enfrentamento ao Terrorismo — CIET, coordenado pela Polícia Federal, do qual participarão inúmeros países, inúmeros representantes de órgãos policiais de diversos países.

Nesse aspecto, obviamente por essa reunião ser aberta, não me cabe entrar em aspectos e detalhes do planejamento relativos a esse assunto, mas vale ressaltar que, dentro da estrutura toda montada para os Jogos Olímpicos, há uma preocupação muito grande em relação a esse tema.

O Brasil tem buscado as experiências dos principais países que vivenciam esse tema em seu cotidiano. São países da Europa, da América do Sul e da América do Norte. Esses países estão em permanente troca de informações e experiências, tanto no aspecto da inteligência como no aspecto operacional. Receberemos no Brasil alguns países com uma estrutura bastante robusta para que essa troca seja efetivada de uma maneira mais célere.

Então, há uma preocupação bastante grande em relação ao monitoramento de atividades terroristas. Esses países colaboram de maneira direta conosco.

No País, a Polícia Federal, junto com a Agência Brasileira de Inteligência, tem feito trabalhos específicos ligados a esse tema.

Às vezes até me surpreendem comentários de alguns especialistas ou de supostos especialistas que dizem que o País não está dando a devida atenção a esse tema. Quem participa do planejamento e do tema especificamente no seu dia a

dia sabe o quão caro é esse tema e o tamanho da importância que a ele é destinada.

Neste momento, diversas reuniões com os parceiros internacionais e com os parceiros da rede de inteligência interna de nosso País estão sendo realizadas. Na Comissão Estadual de Segurança Pública e Defesa Civil para os Jogos Rio 2016 no Estado do Rio de Janeiro, amanhã daremos o início aos trabalhos da Oficina Temática de Enfrentamento ao Terrorismo. Essa Oficina discutirá o tema já no aspecto operacional.

Participam dessa Oficina todos os órgãos de segurança pública envolvidos com o planejamento de segurança dos Jogos Olímpicos, como o Ministério da Defesa e a Agência Brasileira de Inteligência.

Então, é importante esse registro. Apesar de toda a preocupação, apesar do momento delicado que vivemos — na última semana, infelizmente, temos tomado conhecimento diariamente de ações terroristas ocorridas pelo mundo —, é importante que se destaque que há, sim, uma preocupação muito grande em relação a isso e que esse tema vem tendo a devida atenção.

Às vezes somos perguntados: *"Mas o Brasil está preparado para esse enfrentamento?"* Há uma questão que nós sempre colocamos. Existe todo um planejamento que vem sendo feito de maneira integrada de fato, e não apenas de boca. Há todo um processo de construção conjunta em cada uma das cidades de futebol desde a base, que passa por todas as operações especiais dos Jogos, incluindo a operação de revezamento da tocha, as cerimônias de abertura e encerramento, entre outras específicas. Há toda uma energia e todos os recursos colocados para esse fim. Tudo isso, somado à cooperação internacional que receberemos e à ajuda que nos darão os países que vivenciam esse problema no seu dia a dia, nos traz a tranquilidade de que estamos, sim, cuidando com muito zelo desse tema.

Isso tem um reflexo todo na parte cibernética. Além de equipes de segurança pública envolvidas na temática no que diz respeito aos aspectos de crime e aos aspectos relacionados ao terrorismo, teremos equipes de diversos países com troca de informações especificamente no que diz respeito à questão cibernética.

Então, na verdade, é importante que todos tenham um pouco de conhecimento do trabalho que é dispensado em relação a esse tema por parte dos órgãos envolvidos com o planejamento de segurança.

Deputada, a minha intenção era a de falar de forma bastante genérica. Então, termino aqui a minha fala.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Agradeço ao senhor pela apresentação e até mesmo por ter aceitado o convite também para participar deste Seminário.

Consulto aos autores, tanto ao Deputado Silas Freire quanto ao Delegado Éder Mauro, se podemos fazer as perguntas no final ou preferem aproveitar o fato de que esta Mesa já está formada e fazê-las aos nossos convidados e depois aos outros.

O SR. DEPUTADO SILAS FREIRE - Vamos intercalar porque senão nós vamos terminar, Presidente, nos estendendo com a outra Mesa. Vamos aproveitar esta Mesa que está posta.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Então, concedo a palavra ao Deputado Silas Freire e, logo em seguida, ao Deputado Delegado Éder Mauro.

O SR. DEPUTADO SILAS FREIRE - Sra. Presidente, primeiro, quero parabenizar V.Exa. pela condução desta CPI e por ter aceitado a minha ideia e a do Deputado Delegado Éder Mauro.

Quero dizer que temos que deixar aqui o legado deste Seminário e uma proposta de criarmos, na Comissão Permanente de Ciência e Tecnologia, Comunicação e Informática, uma Subcomissão de Combate ao Crime Cibernético — é uma sugestão que nós queremos apresentar a V.Exa. — ou mesmo uma Comissão Permanente Mista de Combate ao Crime Cibernético. Por que mista? Nós tivemos no Senado Federal, através do Senador do meu partido, o PR, o Senador Magno Malta, um brilhante trabalho de elucidação de um crime de pedofilia que estava emaranhado sobre o crime cibernético.

Quero agradecer a participação de todos os expositores e falar da nossa preocupação. Nós vimos, nessa primeira Mesa, uma organização, uma explanação didática, mas que não nos tranquiliza por conta do momento que o mundo vive.

Senhores, desde a parte política do Itamaraty até a parte das Forças Armadas, esse assunto nos deixa ainda muito preocupados, diante do que temos acompanhando no mundo. Há iminência de ações terroristas.

Por exemplo, foi publicada uma matéria na revista *Exame* do dia 17 de novembro do ano passado sob o título: *Estado Islâmico está planejando Ataques Cibernéticos com Mortes, diz o Reino Unido*.

A matéria da revista relata que militantes do Estado Islâmico estão tentando desenvolver a capacidade de lançar esses ataques. O Estado Islâmico, que já usa a Internet para fins de propagandas hediondas, para a radicalização, para o planejamento operacional e também para recrutar os seus integrantes, vai mais longe. Ele está em busca — pelo nosso conhecimento, ainda não conseguiu — de instrumentos que possam causar um terrorismo mundial. Isso nos preocupa, uma vez que o próprio Ministro das Finanças da Grã-Bretanha disse que a Internet representa um eixo crítico de potencial de vulnerabilidade.

Mas, desde a primeira exposição do Conselheiro Gabriel, que disse que nas últimas Olimpíadas tivemos aquele crime de invasão de senhas, temos visto, nos grandes eventos, que os caras entram ou tentam, por exemplo, entrar nas contas várias vezes apenas para deixar as contas inutilizadas. E querem fazer isso com os turistas que estão frequentando o País.

Imaginem o que os turistas que vêm ao Brasil vão passar com suas contas travadas. Os *hackers* vão tentar interditá-las justamente com a intenção não de consegui-las, mas de interditá-las para deixar os turistas sem recursos, sem acesso à rede bancária.

São esses tipos de crimes que podemos até chamar de simples, que não são significativos, mas para o turista, que sai lá do seu país para vir ao Brasil e ficar aqui com essa limitação, sem dúvida nenhuma, é muito difícil.

O Estado Islâmico também tem divulgado vídeos com decapitação de reféns e pretende criar um califado mundial, pretende impor até um código cibernético. E nós não podemos deixar isso acontecer.

Quero deixar claro que o que observei é que já há realmente uma integração, pelo menos nesta primeira Mesa, e uma organização, mas quero também deixar claro que não tira o nosso susto. E “não tirar o susto” é até melhor, porque, às vezes

— e os senhores são mais experientes do que nós aqui —, a tranquilidade pode nos trair. Então, aquela coisa de estarmos todo o tempo assustados pode nos trazer um cuidado maior.

A Olimpíada representa diversos riscos à segurança. Cito os protestos, o hackerismo, o protesto contra o Governo brasileiro, contra entidades de organização, principalmente a cooptação.

Já há informação de que terroristas mundiais poderiam estar tentando cooptar jovens brasileiros não só em relação a ataques cibernéticos, como, através da Internet, na formação do exército, na realização de ataques físicos. Sabemos que essas pessoas não têm limites. Imaginamos que o que vimos na Alemanha e o que aconteceu na França não vai acontecer no nosso País. Diante da possibilidade desse susto, temos que continuar pensando que pode acontecer conosco aqui também.

Cito ainda ataque de navegação a serviços tradicionais, como parte de grandes campanhas de *hackers* contra os grandes eventos e contra alvos específicos; os ataques que aproveitam a lógica de negócio, tal como o uso de *scripts* automatizados, para executar um número excessivo de acesso a *sites,* com o objetivo simplesmente de impedir o acesso ao *site.* Ele quer prejudicar o acesso ao *site.* E tudo isso, numa competição dessas em que a comunicação é tudo, vai acabar atrapalhando.

Cito o bloqueio de contas de usuários, como já disse aqui. Estou só relembrando. Lembro ainda que os grandes eventos apresentam-se como uma oportunidade para o cometimento de delitos favorecidos a partir da tecnologia. Necessita-se assim conhecer os problemas decorrentes da interferência do modo de utilizar as novas tecnologias, a partir da análise dos conceitos peculiares e tradicionais do cibercrime e de outros, por exemplo, da guerra cibernética, que nós tememos. Os senhores mesmos disseram que há possibilidade disso, e não podemos descartá-la.

Não podemos descartá-la de jeito nenhum, principalmente durante o maior evento mundial. Não é uma copa do mundo, não é uma paraolimpíada, não é um pan-americano. É uma Olimpíada!

Cito *sites* falsos para a venda de ingresso para os Jogos Olímpicos — e isso entra mais na parte policial —, que enganam usuários, fazem vendas fraudulentas, vendem, obtêm dinheiro da vítima e não entregam. Tudo isso pode estar acontecendo.

Podem estar sendo programadas para acontecer diversas fraudes de cartão de crédito, de débito, aproveitando o grande fluxo, segundo os números dados pelo Itamaraty, que temos de interceptações eletrônicas bancárias. O País realmente usa muito isso. Poderá haver a clonagem de cartões de crédito. Muitos países ainda não adotaram cartões com tecnologia de *chip*! Vamos ter turistas aqui com cartões sem *chip.* Assim ficam bem mais fáceis de serem clonados.

Cito o aumento de casos de compras fraudulentas com cartões clonados no comércio *on-line*, no comércio físico; de problemas de turistas de outros países que utilizam cartões de bancos ou de empresas de cartões que os lojistas não conhecem. Logo estes lojistas terão maior dificuldade para identificar visualmente um cartão clonado.

Então, essa festa não é para nos trazer prejuízo. Nós temos que tomar cuidado e o quanto pudermos fechar todas as portas.

Essa é a nossa preocupação, mas eu acho que este seminário traz uma colaboração muito grande, mostra que este Parlamento, Sra. Presidente, está preocupado. Nós estamos vivendo uma turbulência política. Só se fala em *impeachment* neste País. O Brasil parou, e estamos na porta da Olimpíada.

Outra coisa: o maior instrumento hoje para o mal — ele também é para o bem — é a Internet. Os senhores sabem disso e já vão ter que lidar, como o mundo inteiro está lidando, com aplicativos que insistem em dizer que não podem abrir a comunicação. Nós já vamos ter que lidar, diante de todos esses riscos, com aplicativos tipo WhatsApp, a que, dizem, nós não podemos ter acesso. A tecnologia ainda não nos dá acesso a ele, e hoje é o mais usado por esses criminosos no mundo inteiro.

Então, eu quero parabenizá-los e dizer que a explanação dos senhores nos contempla. Mas há pontualmente algumas questões — eu citei, por exemplo, *scripts* —, e quem quiser pode ficar à vontade para indicar o seu posicionamento em relação à nossa preocupação com esse momento olímpico.

Espero que essa preocupação, senhores, não seja só no momento olímpico. Como o próprio General Marconi nos disse aqui, nós temos que preparar uma política nacional de segurança cibernética, que não é só para as Olimpíadas, não. Que usemos as Olimpíadas para isso, mas que nós também possamos garantir o nosso futuro! O País é grande e está vivendo um momento de turbulência.

Muito obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Deputado Silas Freire.

Concedo a palavra ao Deputado Delegado Éder Mauro.

O SR. DEPUTADO DELEGADO ÉDER MAURO - Sra. Presidente, Srs. Deputados, quero de antemão agradecer a presença do Conselheiro Gabriel Moreira, do Sr. Marconi Bezerra, do Sr. Rômulo Menezes e do Coronel José Camelo, que faz parte do nosso Exército Brasileiro. Eu, em particular por ter sido policial durante 30 anos e filho de militar da Aeronáutica, tenho uma admiração muito grande pelas nossas Forças Armadas, porque é onde se aprende o respeito, a disciplina e a defesa deste País, sobre o que muito aprendi desde criança. Infelizmente, lamentamos o momento político que se vive, em que as Forças Armadas não são vistas da forma que deveria. Sempre digo que um país seguro, que quer a paz, tem que deixar evidente que pode se defender.

Hoje, embora o Brasil não seja exatamente um país que queira guerra, que não seja um alvo em potencial do próprio Estado Islâmico, pelo menos teoricamente não, nós nunca podemos pensar que nada vai acontecer conosco ou dentro do nosso território. Desde os ataques de 11 de setembro, tem havido eventos tristes em todo o mundo, envolvendo pessoas inocentes, que perdem sua vida por atos cometidos por essas pessoas de mente doentia, que vêm causando terror no mundo. Eu sempre digo que o inimigo que age covarde e silenciosamente não declara guerra, apenas anuncia o resultado.

A nossa preocupação nesta CPI se deu principalmente porque, no meu gabinete, recebi pessoas ligadas à Agência Brasileira de Inteligência — ABIN dizendo que nada estava sendo feito para prevenir ou remediar um evento terrorista dentro do nosso País, levando em consideração que, embora nós não sejamos um alvo em potencial, nós vamos receber delegações europeias e principalmente norte-

americanas. No Brasil, com toda a sua dimensão, com toda a extensão de sua fronteira — somos conscientes disso, principalmente como policial —, é difícil a fiscalização. Temos que estar preocupados com isso.

Em relação ao envolvimento da questão cibernética, nesta semana nós recebemos exatamente uma notícia de que os próprios Estados Unidos, assim como outros países que procuram estar o tempo todo acompanhando esse tipo de ação, conseguiram quebrar o bloqueio do telefone de um terrorista morto no último evento, mesmo contra a vontade da operadora.

Nós estamos muito aquém dos outros países. Embora sejam desenvolvidos, de potencial militar e tecnológico muito maior que o nosso, nós temos que estar preocupados. Diante dessas ocorrências, e como vai haver um evento esportivo neste País, eu gostaria de fazer algumas perguntas, embora algumas sejam direcionadas também para a Mesa que virá posteriormente.

Pergunto o seguinte: se existe alguma medida a ser adotada em específico em relação a esses eventos para as Olimpíadas; se existiram casos fracassados durante outros grandes eventos em 2015; se existe alguma restrição legal para ampliar exatamente a segurança cibernética; se existe acompanhamento, pelos órgãos deste País, principalmente com o evento que está para acontecer, de células possíveis do Estado Islâmico no Brasil; se existe troca de informações com países ligados a esses eventos; se existe acompanhamento principalmente de adultos e jovens brasileiros que são assediados pela Internet por grupos do Estado Islâmico; se esses brasileiros são acompanhados preventivamente para evitar qualquer evento dessa natureza, como muito se tem visto em outros países; se existe um plano, diante de tudo o que já foi vivido, para prevenir um ataque; por fim, caso ocorra o evento, se existe um trabalho preestabelecido para o pós-evento: socorro, forma de agir, forma de bloquear o outro evento sequencial.

Pois, senhores, sinceramente, nós não temos visto nenhuma movimentação nesse sentido e gostaríamos — e o povo brasileiro gostaria também — de saber dos senhores, que fazem também segurança neste País, o que está acontecendo.

Obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Sem dúvida, quero até agradecer aqui tanto ao Deputado Silas Freire quanto ao Deputado Delegado Éder

Mauro pelo requerimento, por trazer em debate este assunto, que é de preocupação de todos.

A imagem do nosso País para fora, quando se fala das Olimpíadas, é realmente de as pessoas terem esta visão da insegurança. É uma insegurança de um modo real, e a imaginem no modo virtual. Nós ficamos com essa grande preocupação, ainda mais tendo em vista o grande aumento no número de crimes cibernéticos existentes no nosso País.

Primeiramente vou passar a palavra ao Conselheiro Gabriel para que faça algumas considerações aos autores do requerimento. Depois falarão os demais convidados.

O SR. GABRIEL BOFF MOREIRA - Muito obrigado, Deputada Mariana Carvalho. Eu quero fazer algumas considerações gerais no âmbito de competência do Itamaraty. Então, não vou poder falar sobre outros pontos que são de competência mais específica dos outros órgãos aqui presentes.

Mas eu queria tocar num assunto que é a questão do terrorismo, que eu não incluí na minha apresentação inicial, mas que é um tema, sim, fundamental. Eu queria parabenizar a Casa por ter aprovado recentemente a lei que tipificou o crime de financiamento de terrorismo. Eu acho que esse foi um momento histórico, digamos assim, do ponto de vista do Itamaraty.

Nós estávamos há mais de 10 anos esperando pela aprovação de uma lei que tipificasse o crime de financiamento de terrorismo. No plano internacional, nós estávamos sendo muito cobrados, quer dizer, o Brasil estava sendo muito cobrado, principalmente pelo GAFI — Grupo de Ação Financeira Internacional, que tem sede em Paris e que tem uma atuação muito importante no combate ao terrorismo, principalmente cortando canais de financiamento de grupos terroristas.

Então, eu queria parabenizar a Casa pela aprovação da lei. Foi realmente um marco importante, que confirma o compromisso que o Brasil vem demonstrando no plano internacional com relação ao combate ao terrorismo.

Eu queria também dizer que isso facilita muito a nossa cooperação internacional, que já é muito fluida. Já temos uma cooperação muito fluida, muito eficiente, eu diria, com vários países, principalmente países que vivem o problema do terrorismo. O terrorismo é algo presente não só em países europeus, mas

também em países asiáticos, africanos. Eu queria também dizer que, na verdade, o maior volume de, digamos assim, vítimas de terrorismo não estão na França nem na Bélgica, estão em países em desenvolvimento, na Ásia, na África. O maior número de mortes acontece nesses países, e não em países desenvolvidos, embora haja uma tensão muito maior dos meios de comunicação em relação a atentados que ocorram em países europeus.

Do ponto de vista do Itamaraty, e eu queria pegar como gancho o que falou também o colega da Secretaria Extraordinária de Segurança para Grandes Eventos, na verdade, já trabalhamos em coordenação aqui, internamente, a questão da cooperação internacional, que é importante. O Itamaraty muitas vezes é procurado por outros países, via nossa rede de embaixadas, e nós recebemos muitas informações relativas a atos de terrorismo, a possíveis ameaças terroristas, a nomes de possíveis terroristas, e nós, imediatamente, sempre quando recebemos esse tipo de informações, nós as incluímos e as enviamos à Polícia Federal, ao Ministério da Defesa, aos órgãos competentes do Ministério da Justiça, para que se tomem as devidas providências.

Então, do lado do Itamaraty, além de facilitar o ambiente para cooperação internacional no combate ao terrorismo e no combate aos crimes cibernéticos, nós sempre repassamos informações importantes para a Polícia Federal e para os órgãos competentes para evitar, por exemplo, a concessão de vistos, enfim, para que sejam tomadas as devidas providências quando pessoas suspeitas tentem entrar no Brasil.

Eu acho que seriam essas as considerações que eu gostaria de fazer.

Muito obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Eu só queria fazer uma pergunta, aproveitando que o senhor representa o Itamaraty.

Na sua fala, o senhor citou a Convenção de Budapeste. O senhor poderia justificar alguns motivos de que tem conhecimento de por que até agora o Brasil é um país que não faz parte dessa convenção?

O SR. GABRIEL BOFF MOREIRA - Bom, alguns anos atrás houve uma ampla discussão no Governo brasileiro sobre se o Brasil deveria ou não aderir à Convenção de Budapeste. O resultado dessa consulta — na verdade, foi uma

decisão tomada em conjunto por vários órgãos da administração pública — foi a de que havia alguns elementos da Convenção de Budapeste que eram particularmente problemáticos para o Brasil, que violavam, eram contrários a leis brasileiras, etc. O principal elemento que naquele momento — e eu acho que continua vigente essa preocupação — era um artigo que previa o acesso transfronteiriço de dados.

Na verdade, numa investigação criminal envolvendo um crime cibernético, a Convenção de Budapeste permite que um país consiga dados de outro país sem necessariamente esse outro país autorizar a saída desses dados. Então, alguns bancos de dados, por exemplo, podem ser acessados por outro país no âmbito de uma investigação criminal sem autorização do país que detém esses dados. Naquele momento — e hoje ainda é — isso foi considerado problemático para o Brasil.

O Brasil tem presente que é importante a cooperação judicial, a cooperação legal, a cooperação jurídica, mas essa cooperação jurídica tem que ter certos parâmetros, e esses parâmetros da Convenção de Budapeste não atendiam aos parâmetros que o Brasil estava acostumado a utilizar em ações de cooperação jurídica. Havia também outras preocupações.

A Convenção de Budapeste previa que os países-membros, os que faziam parte da convenção, teriam que observar pelo menos dois acordos internacionais de propriedade intelectual, principalmente de *copywrite*. Eram acordos a que o Brasil não havia aderido, porque víamos problemas fundamentais neles. Esses dois elementos não admitiam reserva, então o Brasil não poderia aderir à Convenção de Budapeste e eventualmente indicar reservas a esses dois ativos, porque esses ativos, pela convenção, não eram passíveis de reserva.

Então, eu acho que foram esses os principais elementos que dificultaram e tornaram impossível, pelo menos do ponto de vista jurídico, a adesão do Brasil à Convenção de Budapeste.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada.

Concedo a palavra ao Diretor do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, Sr. Marconi dos Reis Bezerra.

O SR. MARCONI DOS REIS BEZERRA - Obrigado, Deputada Mariana.

Sobre o que aqui foi relatado pelo Deputado Silas e pelo Deputado Éder, vou fazer apenas alguns comentários. Nós vimos aqui, na fala do Deputado Silas, a preocupação constante dele. A preocupação não é só dele. Eu tenho certeza de que esta sala está cheia de pessoas preocupadas com a segurança cibernética para os grandes eventos. É uma constante nossa também.

Nós estamos preocupados também, mas eu gostaria de dizer que só a preocupação não resolve. Nós temos até um jargão na vida militar que diz que *"preocupação não é ação tática"*. Só a preocupação não resolve nada, ela depende de uma ação para tentar mitigar ou evitar aquela preocupação. E essa é uma atividade constante também.

Cito só como exemplo a preocupação que temos ali, o que nós temos feito em termos de ação. Temos tentado capacitar as pessoas, conscientizá-las; trabalhamos juntos aos órgãos, orientando-os e participando de campanhas de conscientização e motivação para as questões de segurança da informação, de como tratar a questão de controle de acesso do computador, de *login*; de como não divulgar a senha para ninguém, aquelas recomendações que todos os senhores já têm acompanhado. O pessoal da rede bancária tem uma preocupação muito grande também com isso.

Mas, no nosso caso, eu cito especificamente aqui o nosso Centro de Tratamento de Incidentes de Segurança de Redes de Computadores. A equipe do CTIR Gov monitora aquelas mais de 320 grandes redes que comentei aqui. É uma estrutura muito grande, que depende de um trabalho muito pesado. Nós costumamos até brincar internamente ali, dizendo, para quem nos visita lá, que essa equipe fica trancada numa sala e tem direito a tomar dois banhos de sol por dia. Então, eles ficam atentos ali, com os olhos grudados nas telas, olhando o que está se passando nas redes, tentando ver o mais rápido possível de onde veio uma tentativa de ataque para avisar aquele órgão que foi alvo de ataque. Muitas vezes, na maioria delas, o órgão que foi atacado não sabe. Ele foi atacado, e o vírus está lá na rede dele, disseminando-se para outros computadores. Então, ele precisa ser avisado o mais rápido possível para evitar a propagação daquele problema.

Uma palavra-chave que eu cito aqui, que também já foi citada pelo Coronel Camelo, é a cooperação. Nós, sozinhos, não fazemos nada. A cooperação é fundamental nessa área de segurança da informação. O desafio nosso é grande,

mas é um desafio que não é apenas nosso, de quem está no Governo, de quem está tentando trabalhar para proteger as redes; esse desafio é de todos nós, é de todo cidadão brasileiro. É um desafio grande, mas, com cooperação, com colaboração de todos, nós pretendemos alcançar sucesso nessa segurança.

Destaco também que a questão da segurança é descentralizada. A segurança cibernética nos nossos normativos, como tratamos a segurança da informação, é totalmente descentralizada, ou seja, nós dizemos o que os órgãos têm que fazer. Eu cito como exemplo a nossa norma de gestão de risco. Cada órgão da administração pública federal tem que cumprir essa norma, elencando na sua área de atuação quais são os riscos prováveis e existentes e o que ele fará mediante um risco iminente.

Portanto, essa gestão de risco é de cada órgão. Não cabe a nós do Governo entrar em cada repartição, em cada setor e dizer o que deve fazer. Eu acho que a descentralização é nesse sentido. Cada órgão é dono do seu setor e deve obedecer às normas e cumpri-las. Com isso, acreditamos que os riscos serão mitigados e a segurança será aumentada.

O Deputado Delegado Éder comentou sobre medidas que os membros da Mesa estão fazendo ou pretendem fazer. Nós na Casa Militar elencamos algumas ações de curto prazo que já estão em planejamento e vão entrar em execução no decorrer do próximo mês. Há preparativos.

Já participamos de algumas reuniões com o Comitê Olímpico lá no Rio de Janeiro, inclusive, com membros da nossa equipe do Centro de Tratamento de Incidentes de Segurança de Redes de Computadores. Essas são atividades que já vêm sendo realizadas, e nós temos a intenção de intensificá-las daqui até o evento em si.

Comentou-se aqui também sobre o histórico de eventos anteriores, Copa do Mundo e outros dos quais nós participamos em conjunto com outros órgãos da administração pública, inclusive com o CDCiber, e não tivemos notificação de sucesso da parte do atacante. Sofremos vários ataques, mas foram todos detectados e resolvidos a contento. Não temos grandes prejuízos nem memória negativa de eventos anteriores.

Era só isso o que eu tinha a dizer.

O SR. DEPUTADO DELEGADO ÉDER MAURO - Sra. Presidente, eu peço desculpas. Vamos votar e depois retornaremos.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Como estamos em votação nominal, vou suspender a reunião por 5 minutos, tempo que os Srs. Deputados terão para votar no plenário e voltar à reunião para ouvir as considerações finais dos convidados.

Está suspensa a audiência por 5 minutos.

(A reunião é suspensa.)

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Declaro reaberto o seminário.

Concedo a palavra ao Coronel José Ricardo Souza Camelo, Chefe da Divisão de Operações do Centro de Defesa Cibernética.

O SR. JOSÉ RICARDO SOUZA CAMELO - Eu fiz algumas anotações aqui. O Deputado Delegado Éder Mauro fez várias colocações, além do Deputado Silas Freire. Eu vou tentar compor uma resposta que tenha um mínimo de abrangência no que diz respeito ao que foi abordado. Para isso, vou usar um pouco do histórico do trabalho do Centro de Defesa Cibernética, a unidade que foi para o combate logo de início, em 2012, na Rio+20.

Nós tivemos a preocupação, desde o primeiro evento, de trabalhar com lições aprendidas. Então, existem algumas centenas de lições aprendidas já cadastradas daquelas coisas que colocamos sob forma de hipótese, e elas se confirmaram; outras coisas que achávamos que sabíamos, e que não se confirmaram; e outras variantes a respeito dos nossos procedimentos e do nosso planejamento, justamente para garantir uma continuidade, uma evolução dos trabalhos.

Cada grande evento foi uma escola diferente, em particular os dois primeiros. Na Rio+20, o planeta inteiro atacou Brasil. Isso é literal, não é força de expressão. Os ativos principais relativos à Rio+20 eram protegidos na infraestrutura do SERPRO, que foi o grande herói em termos de proteção naquele evento. É um dos nossos parceiros principais e um dos pioneiros da área de segurança da informação em termos da administração pública federal. É um parceiro muito importante, que tem uma estrutura muito madura. Nós, compondo com o SERPRO e outras

instituições — a Polícia Federal, por exemplo, trabalhou fisicamente junto conosco, lá no Rio de Janeiro, e também a ABIN —, aprendemos muito nessa composição.

Uma das coisas que nós percebemos logo de cara foi que muitos processos davam certo, porque o Cel. Camelo havia participado, desde Capitão, em vários grupos de trabalho interministeriais com especialistas de segurança da organização A, B, C e D, e isso fez uma diferença muito grande na hora de resolver determinados problemas. O Cel. Wallier, companheiro meu que foi o comandante do destacamento na Rio+20, foi o coordenador do CTIR GOV, uma função anterior a do CDCIB. Foi chave para trabalhar com isso.

Então, essas amizades nos demonstraram o quão importante, em termos não simplesmente de pessoas, mas de instituições, extrapolando, fazendo a comparação do que é essencialmente humano, é a questão de relacionamento e desenvolvimento de confiança para instituições também. Em compensação, outras coisas não funcionaram.

Na Copa das Confederações, nós já com essa ação colaborativa um pouco mais amadurecida, estávamos esperando ataques muito mais intensos no que diz respeito a ataques cibernéticos e hacktivismo. Houve a edição da Lei 12.737 — acho que são esses os três últimos dígitos —, a que o pessoal apelida de Lei Carolina Dieckmann, o que aparentemente dissuadiu muito. Inclusive, a Polícia Federal, em uma das reuniões de coordenação, disse que já havia identificado algumas pessoas físicas responsáveis por lideranças *hackers* em trabalho conjunto conosco, durante a Rio+20, e que estaria então fazendo um trabalho de dissuasão.

Poucas semanas depois, entre a Copa das Confederações e a Jornada Mundial, apareceu um vídeo dos hacktivistas no Youtube dizendo que haviam sido visitados, mas que não desistiriam, etc. Embora as curvas de ataque, de um modo geral, tenham aumentado, no que diz respeito ao grande evento, especificamente, elas foram bem mais modestas.

Só que a Copa das Confederações foi outra escola, porque a mobilização de rua apoiada pelos movimentos de redes sociais foi algo que nós nunca havíamos visto nem nada parecido. Foi um poder de mobilização imenso — imenso — tanto de coisas legítimas com protestos que o País merecia para o seu próprio amadurecimento quanto de coisas extremamente perigosas no que diz respeito a

ações de rua e provocações para causar tumulto, para, enfim, criar situações adversas para as forças de segurança de forma totalmente artificial. Foi uma escola também fantástica. Nós acumulamos muitas lições aprendidas e amadurecemos a questão do relacionamento.

A Jornada Mundial e a Copa do Mundo, no que diz respeito 100% à cibernética, a ataques, foram eventos um pouco mais suaves, vamos dizer assim. Ainda, na Copa do Mundo, como eu citei na minha apresentação, houve dois eventos um pouco mais significativos, que poderiam ter se tornado muito mais graves, mas que foram neutralizados com ações de coordenação do gabinete de crise que nós instituímos *ad hoc* com as instituições parceiras na época.

Então, o que acontece? Uma das formas de atenuar o problema, ainda que não resolva, é justamente nos preocuparmos sempre em não reinventar a roda, que é uma coisa que muitas vezes com as tecnologias novas temos uma tendência a achar que o novo criou situações com as quais não sabemos mais lidar. Mas, por incrível que pareça, para o pessoal técnico muitas vezes produtos tecnológicos absolutamente novos ainda mantêm processos antigos da década de 90, início dos anos 2000, porque com eles sabemos lidar, mas só que estão com outros nomes e acontecem muito mais rápido. Então, valorizamos muito essa questão das lições aprendidas e tentamos disseminar isso entre os parceiros.

No que diz respeito à ação do Centro especificamente, temos parcerias estratégicas para tentar trabalhar esse amadurecimento do País o mais rápido possível, e temos assento no Comitê Gestor da Internet, que faz toda a governança, que trabalha na governança da Internet brasileira, temos trabalhos com o Ministério da Ciência e Tecnologia, com soluções nacionais que estão sendo trabalhadas de equipamentos cujo domínio pode fazer uma grande diferença principalmente para coibir ações de espionagem.

Enfatizei na apresentação a questão da capacitação e da descoberta de talentos. Muitas vezes na área cibernética não conseguimos acabamos parando num determinado ponto da capacitação. Mas o talento, utilizando uma forma mais jocosa de lidar com o problema, aquele maluco, para quem colocamos só a pizza embaixo da porta para alimentá-lo, e ele está lá enlouquecido, programando e descobrindo coisas novas, normalmente nós não o formamos, ele é descoberto.

Trabalhamos nossas escolas militares, nossos cadetes, para achar quem tem vocação e poder trazê-los para a área.

E, mais uma vez, a questão da ação colaborativa não é um problema fácil de lidar, porque é uma lição mundial que vem da segurança da informação e se aplica totalmente na segurança cibernética. Trabalhamos por ciclo de amadurecimento. É lento, infelizmente, porque, ao mesmo tempo em que é lento que as pessoas se convençam de segurança, é muito rápido que as pessoas se seduzam pelo canto da sereia. Então, qualquer tecnologia nova que nos conecte melhor e mais rápido é imediatamente, inquestionavelmente e sem nenhum tipo de critério aceito por nós. Esse é o pesadelo do profissional de segurança, porque é justamente por aí que o elo mais fraco se quebra.

Sr. Deputado, eu gostaria até de ter uma resposta a mais, uma bala de prata para dar solução, mas isso não é uma questão brasileira.

Recentemente, estive com um companheiro num curso específico da área de segurança cibernética, na Alemanha — um curso americano feito na Alemanha —, que reuniu mais de 60 países, e os discursos eram absolutamente similares aos brasileiros. Nós temos *gaps* tecnológicos, é verdade, mas os nossos processos, as soluções que enxergamos estão *up to date* com relação ao mundo. O que mais precisamos é de apoio, em termos de priorização, política nacional, é fiscalização dos órgãos públicos, instrumentos normativos para apressar ou acelerar o desenvolvimento do setor privado também, no que diz respeito às suas implementações. Seja no público ou no privado, quando se fala em segurança é um incômodo, ninguém gosta de digitar duas senhas, ninguém gosta de ativar um *software* com criptografia para falar seguro ao telefone, e por aí vai. Ninguém gosta disso. Então, é um trabalho de educação muito forte também.

Infelizmente, não conheço, e estamos muito sintonizados com o mundo nisso, não existe a bala de prata, mas existem, sim, formas de lidar com o problema, atenuando os riscos, principalmente com pessoas, com processos em como lidar com a questão e, por último, por incrível que pareça, com produtos tecnológicos.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Coronel.

Concedo a palavra para as suas considerações ao Sr. William Murad.

O SR. WILLIAM MURAD - Vou ser breve, Deputada.

Em relação a três questionamentos que o Deputado Éder fez, ao final, em razão da sua abrangência — são questões que vão além da questão cibernética, mas que também se relacionam com ela —, eu queria não só tecer alguns comentários, mas trazer alguns exemplos do que vem sendo feito.

A primeira questão é em relação à troca de informações internacionais. Eu posso afirmar aqui, Deputado Éder, com uma convicção bastante alta, que nós estamos, sim, com um alto nível de troca de informações com os principais países, no que diz respeito às questões relacionadas ao terrorismo.

Em maio, agora, nós teremos um *briefing* internacional, com a participação de mais de cem países, países que estarão presentes nos Jogos Olímpicos. Na sequência, teremos um seminário internacional, no qual especialistas das polícias que atuaram nos dois atentados que aconteceram em Paris trarão informações para os profissionais de segurança pública e outros relacionados. Traremos profissionais que trabalharam na Maratona de Boston, para trazer, também, lições aprendidas, ou seja, para colocar essa questão em debate.

Em relação aos jogos em si, nós teremos o Centro de Cooperação Internacional, coordenado pela Polícia Federal, já com a confirmação de mais de cinquenta países, se não me engano. Talvez o representante da Polícia Federal possa trazer esse número com maior exatidão. Teremos também o Centro Integrado Antiterrorismo, com a participação dos principais países que também lidam com o tema.

Então, posso afirmar, com toda a convicção, que a cooperação internacional é um ponto importante e vem balizando todo o nosso planejamento de segurança.

Em relação ao plano de prevenção de um ataque — acho que o senhor mencionou essa questão —, na verdade, Deputado, hoje nós já estamos no detalhamento de todos os planejamentos e planos operacionais relacionados a cada atividade, no que diz respeito à segurança pública. Então, vem sendo finalizado um plano operacional e seus protocolos de atuação integrada em relação ao policiamento ostensivo, policiamento de portos e aeroportos, policiamento das instalações olímpicas, policiamento de áreas impactadas, como regiões turísticas, principalmente da cidade do Rio de Janeiro. O plano prevê o detalhamento de cada uma dessas atividades, segurança de dignitários, de chefes de Estado. Tudo isso

vem sendo detalhado à minúcia. Esses planos trazem informações de quem faz o quê, como é feita a cooperação, onde começa e termina o trabalho de um órgão e onde termina e começa o do outro, ou seja, são protocolos de atuação integrada num nível mais detalhado.

Então, há, sim, planos específicos de segurança, que, considerados no seu todo, são, sim, planos de prevenção, para qualquer ação criminosa, inclusive para questões ligadas ao terrorismo.

Dou um exemplo em relação ao acesso às instalações. Há um controle extremamente rigoroso. Todas as edições dos jogos já exigem esse rigor, e não será diferente no caso do Rio de Janeiro, e isso será cercado de outras medidas, em razão do cenário atual e em razão das análises de risco que vêm sendo feitas para o momento dos jogos.

Em relação ao pós-evento, é a mesma coisa. Como eu mencionei anteriormente, não só em relação à questão do terrorismo, mas em relação a qualquer evento que possa impactar na segurança dos jogos, existe toda uma cadeia de comando, que vem desde o Centro Integrado de Comando e Controle Nacional, passa por Centros Integrados de Comando e Controle Regionais. Nós temos, no Rio de Janeiro, os centros setoriais, e, por fim, os centros de segurança da instalação. Há toda uma ligação de informações e de condutas. Todos esses centros têm a participação de todas as agências envolvidas com a segurança.

Então, nós contamos com as polícias dos Estados e o Corpo de Bombeiros para tratar dos incidentes da forma mais ampla possível, não só quanto aos aspectos criminais e para impedir que aquela ameaça prossiga, mas também tratar essa ameaça em relação ao socorro de vítimas e ao procedimento de controle do tráfego. Ou seja, há todo um planejamento integrado relacionado também ao pós-evento.

Respondendo objetivamente as questões de forma mais ampla, não relativamente apenas a questões cibernéticas, há um planejamento bastante complexo. Nós podemos estender um convite a esta Comissão para conhecer a Comissão Estadual de Segurança Pública e Defesa Civil do Rio de Janeiro e participar de uma reunião daquela comissão, onde pode ser feita uma apresentação mais detalhada que possa interessar a esta CPI. A Secretaria Extraordinária de

Segurança para Grandes Eventos do Ministério da Justiça fica à disposição para intermediar isso e muni-los com as informações que possam ser necessárias.

Muito obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Nós agradecemos, William, mais uma vez, a presença e a participação de todos neste seminário para debater esse assunto. Parabenizo mais uma vez os Deputados responsáveis pelo requerimento.

Vamos desfazer essa primeira Mesa para podermos fazer a composição da próxima. Mais uma vez, muito obrigada pela disposição de todos em contribuir com esta CPI.

(Pausa.)

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Para compor a segunda Mesa, eu convido o Sr. Leonardo Boselli da Motta, Diretor do Departamento de Infraestrutura e Serviços de Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão; convido também o Sr. Eduardo Arthur Izycki, Oficial de Inteligência da Agência Brasileira de Inteligência — ABIN; convido o Sr. Elmiz Antonio Rocha Junior, representando a Polícia Federal.

Antes de darmos início às exposições, eu vou pedir aos oradores que tentem ser um pouco mais breves, devido ao horário, ao início da Ordem do Dia e ao momento que o nosso País vive.

Já composta a segunda Mesa, eu concedo a palavra ao Diretor do Departamento de Infraestrutura e Serviços de Tecnologia da Informação, o Sr. Leonardo Boselli da Motta. Tem a palavra o Sr. Leonardo.

O SR. LEONARDO BOSELLI DA MOTTA - Boa tarde a todos. Queria agradecer mais uma vez o convite da Câmara para eu estar presente hoje, representando o Ministério do Planejamento e podendo relatar um pouco das ações que o Ministério do Planejamento está realizando para tentar melhorar a segurança da informação nos órgãos da administração.

Antes de mais nada, eu gostaria de esclarecer que o Ministério do Planejamento atua justamente apoiando outros órgãos da administração, mais especificamente o SISP — Sistema de Administração dos Recursos de Tecnologia da Informação

Nós também atuamos em cooperação com o antigo GSI — Gabinete de Segurança Institucional, que agora é o DSIC — Departamento de Segurança da Informação e Comunicações, da Casa Militar, na implantação das normas e de todas as orientações que são emanadas pela Casa Militar, que é o órgão central de segurança do Governo.

Damos algumas definições do que é crime cibernético e, assim, conseguimos resgatar duas leis. Rapidamente — não vou me delongar muito nesse eslaide —, o que é um crime cibernético? É uma ação delituosa em rede computadores, dispositivos de comunicação ou sistema informatizado. Podemos também considerar como definição a invasão de dispositivo informático; a interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informações de utilidade pública; e a falsificação de documento.

Como nós combatemos o crime cibernético? Através da segurança da informação. Aqui está o conceito do DSIC, que já foi apresentado hoje.

Na APF — Administração Pública Federal, qual é o contexto que nós observamos? Existem vários órgãos espalhados pelo Brasil todo, com dezenas de sistemas de informação, que são desde sistemas estruturantes a sistemas estratégicos das mais diversas áreas que nós possamos imaginar. Há sistema de planejamento, sistema de convênios, de segurança, de saúde, e por aí vai.

O que é um sistema estruturante? Sistema estruturante é um sistema informatizado num sistema organizacional. Por exemplo, menciono o sistema de administração dos recursos de logística, que é o SISG, e o sistema informatizado, que é o SIASG.

Sistemas estruturantes são sistemas de informação que são fundamentais e imprescindíveis para a consecução e o desempenho da missão do Estado, e para a segurança da sociedade. Eles têm que atuar, então, com eficiência e eficácia.

Outra característica dos sistemas estruturantes é que há um grande volume de transações ocorrendo nesses sistemas. Nós aqui usamos dois exemplos de volumes que foram transacionados no ano passado. Por exemplo, no SIGEPE — Sistema Integrado de Gestão de Pessoas, no ano passado houve o pagamento de cerca de 151 bilhões de reais aos servidores civis, tanto os da ativa quanto os

aposentados. E no sistema de compras do Governo houve 45 bilhões em compras e 23 bilhões em contratos.

Como eu já disse antes, esses sistemas são utilizados por todos os órgãos espalhados pelo Brasil todo. Então, existe alta capilaridade territorial. Só do Ministério do Planejamento, listamos aqui dez sistemas estruturantes, das mais diversas áreas de atuação do Ministério.

Sabemos que esses sistemas, por causa desse grande volume de recursos transacionados, também são alvos de ataques. Para que se tenha uma ideia da média de ataques diários a sistemas do Governo — dos sistemas que estão lá no SERPRO, que o SERPRO cuida —, há cerca de 500 tentativas de ataques diários. Já houve ano em que essa quantidade chegou ao pico de 2 mil ataques. Sabemos que, sempre que há um grande evento, o Brasil vira foco das atenções. Consequentemente, esses sistemas também vão sofrer uma quantidade maior de ataques.

Uma das formas de tentar reduzir as chances dos ataques é justamente utilizar certificação digital nesses sistemas. Todos aqueles sistemas que foram apresentados utilizam certificação, que é uma forma de tentar diminuir a chance de ocorrer uma invasão — ou a utilização por uma pessoa não autorizada — daqueles sistemas.

No Brasil, quem cuida da certificação digital é a ICP-Brasil — Infraestrutura de Chaves Públicas Brasileira. Ela é composta por um conjunto de entidades, padrões técnicos e regulamentos, e tem um comitê gestor que define as normas e as resoluções. A Autoridade Certificadora Raiz é o Instituto Nacional de Tecnologia da Informação — ITI, que é vinculado à Presidência da República.

Aqui há um esquema de como está composta a Autoridade Certificadora no Brasil, com o ITI em cima. Atualmente, há 14 Autoridades Certificadoras abaixo do ITI. Essas Autoridades Certificadoras são desde órgãos de Governo até empresas públicas e privadas também.

No ano passado foram emitidos por volta de 14.000 certificados para os sistemas do Ministério Planejamento. Esses certificados são emitidos junto ao SERPRO, que é a Autoridade Certificadora que o Ministério do Planejamento utiliza. Este ano foram emitidos aproximadamente 1.900 certificados. A média anual fica em

torno de 14 mil. Desde o início das emissões, nesse trabalho que o Ministério do Planejamento vem fazendo junto ao SERPRO para tentar melhorar a segurança dos sistemas estruturantes, já foram emitidos por volta de 200 mil certificados.

Eu não vou falar do CTIRGov, que já foi mencionado na apresentação anterior. Porém, vale a pena relembrar que as Equipes de Tratamento de Incidentes de Redes dos órgãos fazem esse trabalho em parceria com o CTIRGov, trocando informações. O CTIRGov também encaminha uma série de alertas e ajuda no tratamento de incidentes nos órgãos.

Como eu já disse, o Ministério do Planejamento atua apoiando a ação dos outros órgãos. Então, o Decreto nº 7.579/2011 cria, institui o SISP — Sistema de Administração dos Recursos de Tecnologia da Informação. Diversas finalidades são descritas nesse decreto. Há uma que eu posso citar aqui, que eu considero uma das mais importantes, que é justamente promover a integração, a articulação entre programas de Governos, projetos e atividades, visando à definição de políticas públicas, diretrizes e normas relativas à gestão dos recursos de TI. Ou seja, o Ministério do Planejamento, na figura da Secretaria de Tecnologia da Informação, é o órgão central do Sistema de Tecnologia da Informação, enquanto o DSIC, da Casa Militar, é o órgão central do Sistema de Segurança.

Para ajudar nesse trabalho de apoio aos órgãos, o Ministério do Planejamento, no ano passado, realizou um concurso público para o cargo de analista de tecnologia da informação, que é um cargo bem demandado pelos órgãos. A ideia é que esses servidores atuem nos órgãos do SISP, de forma a melhorar tanto a gestão quanto a governança em tecnologia da informação. Esses servidores são do Ministério do Planejamento, mas atuam de forma descentralizada nos órgãos. Foram nomeados 228 servidores no ano passado. Atualmente, no total, 510 servidores atuam nos órgãos da administração.

Outra iniciativa do Ministério do Planejamento foi o Decreto nº 8.338/2016, que instituiu a Política de Governança Digital e a Estratégia de Governança Digital. Tanto essa política quanto essa estratégia são pautadas em três eixos, que são: acesso à informação, ou seja, transparência e abertura de dados do Governo; prestação de serviços ao cidadão de forma eletrônica, para facilitar ao cidadão o acesso a serviços de Governo; e a participação social, seja por audiências públicas,

consultas públicas, sempre tentando ouvir o cidadão e permitindo que ele participe das decisões e da constituição das políticas públicas. Essa estratégia passou também por consulta pública. Houve várias contribuições.

Com relação à estratégia, é importante falar que, na distribuição desses servidores, o Ministério do Planejamento, na figura do nosso Secretário, realizou algumas reuniões com os secretários executivos de diversos órgãos, de forma a contratualizar algumas metas que esses órgãos deveriam cumprir nos próximos 2 anos. Essas metas são metas estratégicas, definidas pelos próprios órgãos, metas que já estão previstas na estratégia de governança digital e também metas estruturantes para aqueles órgãos.

Na parte de segurança, algumas metas que a gente pode citar é justamente a Implantação do Plano de disseminação do uso IPv6, que é o protocolo de comunicação da Internet, versão seis. Atualmente os órgãos usam, na sua maioria, a versão quatro. Com a implantação dessa versão do protocolo, a gente consegue não só melhorar a questão da auditoria, quando ocorreu uma invasão, por exemplo, e também a gente tem alguns protocolos mais avançados de segurança.

Para os senhores terem uma ideia, a versão quatro do protocolo permite 4 bilhões de endereços. Ou seja, quatro com nove zeros depois. Já o IPv6 é por volta de três e mais 38 zeros depois do endereço. Fica até difícil de falar esse número. Ou seja, com o futuro que nós temos, com a Internet das Coisas, é fundamental, então, a implantação de IPv6, aqui, no Brasil, que já é uma tendência mundial que já vem ocorrendo.

Outra meta que estava lá descrita é justamente a Implantação da Metodologia de Gestão de Riscos, Gestão de Segurança, que está nos órgãos, que é até mesmo uma norma do próprio DSIC. E a gente quer que os órgãos, para que eles consigam melhorar a segurança deles, tenham esses itens. E, hoje em dia, ainda tem alguns órgãos que não têm todos esses itens. Ou seja, ele não tem comitê de segurança, não tem uma equipe de tratamento de segurança instituída, não tem política de segurança no órgão e também não tem um plano de metas de segurança. Então, com essa contratualização que está sendo feita com os órgãos, a ideia é que, até o final deste ano, a gente tenha, nesses 28 órgãos que assinaram contrato com o

Ministério do Planejamento, com apoio do Ministério, todos esses itens relativos à segurança instituídos no órgão.

Bom, o Ministério do Planejamento também tem uma rede, que é uma rede de Governo, que os órgãos aqui de Brasília a utilizam, que é a INFOVIA. É uma rede que foi toda construída pelo Ministério do Planejamento. Atualmente, ela é operada pela SERPRO. É uma rede segura, totalmente montada no formato de anel. Ou seja, se romper um lado, a fibra, o órgão continua tendo acesso à comunicação com os outros órgãos e com a Internet. Toda a segurança é feita pelo SERPRO, pela equipe de segurança do SERPRO. É uma rede toda redundante, de alta disponibilidade.

No início, essa rede foi inaugurada em 2004. Ela vem crescendo bastante. Para os senhores terem uma ideia, de 2011 até 2016, a gente tem alguns números de crescimento dessa rede. Atualmente, ela tem 150 quilômetros aqui, em Brasília. Noventa e quatro órgãos utilizam a Rede INFOVIA, a maioria órgãos do Poder Executivo, do Governo Federal, mas temos também órgãos do GDF que utilizam a Rede, órgãos do Legislativo, e o Senado também está conectado com a Rede INFOVIA, que tem 207 pontos de conexão.

Aqui é o mapa esquemático de como está distribuída essa Rede, aqui em Brasília. A fase 1 foi a parte inicial da Esplanada, depois ela foi se estendendo para a Asa Sul e Asa Norte. Atualmente, ela chega até os órgãos que estão no Aeroporto de Brasília, na Granja do Torto e na Academia de Polícia Militar.

Para finalizar, conforme já foi dito aqui hoje, o elo fraco da cadeia são justamente as pessoas. Então, é importante promover essa cultura de segurança de informação dos órgãos, seja por atividade de sensibilização, de conscientização, de capacitação e especialização.

O Ministério do Planejamento, por ser órgão central do SISP, realiza mensalmente reuniões com todos os órgãos da administração direta que possuem assento na Comissão de Coordenação do SISP, em que são debatidos temas estratégicos para os órgãos, como na questão de novos serviços normativos. Também sempre contamos com a presença da equipe do gabinete do antigo GSI, agora DSIC, da Casa Militar, representando e enriquecendo essa discussão na parte de segurança de informação com os outros órgãos.

Queremos também reforçar essa implantação da gestão de risco nos órgãos da administração. O Ministério do Planejamento, seguindo os normativos do GSI, no ano passado, desenvolveu uma política e uma estratégia para os órgãos conseguirem implantar essa gestão de risco. Isso também em parceria com o Centro de Tecnologia da Informação Renato Archer, de Campinas, num acordo que fizemos com eles. Nós fizemos também — e estamos em fase agora final de desenvolvimento — um *software* para facilitar a implantação da gestão de risco nos órgãos da administração.

A ideia também é massificar esse uso da certificação digital cada vez mais. Para aqueles sistemas de governo que não o utilizam, o Ministério dá apoio para podermos implantar a certificação digital em todos os sistemas e também fazer a conscientização, como foi dito aqui, dos usuários dos sistemas que utilizam certificação digital. Não basta um sistema ser seguro, se o usuário deixa anotado em cima da mesa a senha dele e deixa o *token* jogado em qualquer lugar ou o empresta para a secretária fazer alguma atividade que deveria ser da pessoa.

Bom, gente, eu tentei cumprir o prazo. Acho que consegui. É isso.

Muito obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigado, Dr. Leonardo.

Concedo a palavra ao Dr. Eduardo Arthur Izycki, Oficial da Inteligência da ABIN.

O SR. EDUARDO ARTHUR IZYCKI - Deputada Mariana Carvalho, obrigado pelo convite, em nome de quem eu aproveito para estender os cumprimentos aos demais Parlamentares.

Meu nome é Eduardo Izycki. Trabalho na Agência Brasileira de Inteligência, especificamente na Unidade de Contrainteligência Cibernética. Nossa unidade foi constituída na toada das revelações do caso Edward Snowden, a partir de 2013. A atribuição específica dessa unidade tem sido trabalhar com ameaças cibernéticas, desde então.

Pretendo ser bastante objetivo, bastante pontual em relação ao tipo de ameaça cibernética que podemos esperar e que já temos prospectada à medida que o nosso trabalho tem sido para os Jogos Olímpicos Rio 2016. Por meio de uma

taxinomia rápida e bastante flexível, nós vamos trabalhar em um conceito que denominamos, carinhosamente, de "hacker ostentação", que seria um tipo de ataque — e aqui eu trago um exemplo dele — em que o elemento malicioso invade uma página, com o objetivo exclusivo de substituir o conteúdo dela por alguma mensagem.

No caso específico, denominamos de "hacker ostentação", porque o sujeito, na verdade, não promove mensagem concreta alguma; não veicula a ideologia; não pede nem faz uma manifestação política ou religiosa. O objetivo dele parece ser hostilizar o órgão específico, atacar. Um exemplo que trazemos aqui é aquele em que o sujeito diz que o *deface*, a desfiguração, é uma arte. Vê-se que é algo relativamente elementar. Mas é uma das taxinomias das quais vamos tratar.

Em um segundo ponto, esse, sim, mais específico e mais provável de incidência durante os jogos da Rio 2016, está o ativismo digital. Aqui se encontra, sim, mensagens ideológicas, com cunho político, fomentando manifestações ou algum tipo de ação concreta por parte do indivíduo que acessa, por exemplo, essa página desfigurada. Esse é um exemplo trazido de 2013, durante a Copa das Confederações, quando houve a grande realização de manifestações públicas naquele momento.

Outro exemplo de que nós podemos tratar aqui é especificamente o da Copa de 2014, em que até a mascote à época foi utilizada para veicular uma mensagem de protesto contra as despesas realizadas para a construção de estádios, etc.

Não se limita o "hacker ativismo" e o ativismo digital a uma mensagem política, ideológica, nacional, brasileira, por exemplo. Diversos atores estrangeiros têm promovido ataques nesse mesmo sentido em páginas do Governo brasileiro. Eu trago um exemplo que seria também de desfiguração, realizado por um grupo que dá suporte a grupos que lutam na Guerra Civil da Síria.

Esse é o ataque mais provável a ser vivenciado do ponto de vista de rede de governo e aplicações na *web*, em que a desfiguração vai acontecer com intuito político, provavelmente. Considerando o contexto que é vivenciado nos corredores mesmos desta Casa, esse tipo de ação tem ocorrido. Pelo histórico demonstrado em 2013, com a Copa das Confederações, e em 2014, vai haver uma curva de

crescimento à medida que o evento se aproxime ou que a ebulição das ruas faça com que isso repercuta digitalmente também.

Eu não vou entrar no aspecto dos demais em relação a Rio 2016, mas é claro que a espionagem cibernética é a grande razão de existência da minha unidade. O Leviatã Digital, que se constitui em outros países, como, por exemplo, nos Estados Unidos ou nos países europeus — e foi citado pelo Deputado o exemplo da quebra da criptografia em relação a dispositivos móveis, por parte de serviços de polícia daquele país —, é um exemplo dessa capacidade cada vez mais crescente de espionagem cibernética.

Faço uma rápida menção ao terrorismo cibernético. A minha área não é o terrorismo em si, mas posso tratar do assunto do terrorismo cibernético na seguinte medida. O cenário em que um sujeito integrante de um grupo terrorista se senta em frente a um computador e, por meio cibernético, vamos chamar assim, realiza uma ação concreta, com efeito cinético, com efeito material, com prejuízo de vida humana, com prejuízo de propriedade e de instalações, hoje é tecnicamente muito difícil. Os relatos que são encontrados desse feito são associados a ameaças estatais, com grande suporte financeiro, com grande treinamento e preparação. A atribuição é um problema. No ambiente cibernético não se pode, categoricamente, afirmar que determinado país atacou outro. Há um exemplo mais recente, como o das hidrelétricas na Ucrânia, que foram atacadas, e os resultados cinéticos foram produzidos lá. As evidências coletadas, naquela ocasião, sugerem que o autor era, de fato, patrocinado por um governo, e não um grupo entusiasta, da área de tecnologia da informação, que decidiu realizar essa ação.

Aqui vale um segundo ponto, não excessivamente técnico: a capacidade de se interagir com um sistema de automação de uma infraestrutura de grande porte, como uma hidrelétrica, requer um conhecimento muito específico daquelas máquinas, daquele protocolo. Isso nem sempre é possível. É muito raro, inclusive, encontrarmos o que podemos chamar de “comunidade hacker”.

Vamos falar de guerra cibernética. Não pretendo me imiscuir em um tema que é tão bem abordado pelo Coronel Camelo, juntamente com o pessoal do Centro de Defesa Cibernética, mas é o cenário em que *bits*, e não balas, vão ser disparados no

futuro. Tomara que nenhum dos dois seja disparado, mas, enfim, seria esse o contexto.

Uma das rações pelas quais eu não coloquei crime cibernético como um tipo de ameaça é porque a realização dele, em muitos casos, é tipificado como crime, e tanto a Polícia Federal quanto a Polícia Civil poderiam, de fato, iniciar a persecução criminal para praticamente as três hipóteses. Essa é a razão pela qual ele não está categorizado ali.

Eu vou desdobrar, com mais detalhes — de maneira objetiva, é claro, porque eu não quero me estender em relação ao tempo —, a ameaça cibernética que tende a atuar nos grandes eventos. O objetivo, em num evento tão grande quanto as Olimpíadas, seria justamente macular a imagem da organização, do próprio evento ou promover a própria mensagem justamente pelo alto perfil do evento. É muita gente assistindo ao evento. Naturalmente, a mensagem que ele tenta conduzir vai ser acompanhada por muitas pessoas, o que torna isso atrativo, mesmo para grupos estrangeiros, por exemplo.

Em 2013 e 2014, observamos que, mesmo os grupos que poderiam ser classificados como "*hack* ostentação", por exemplo, ou o sujeito que veicula mensagem de autoelogio, aquelas mensagens até jocosas, no sentido de *"Eu sou muito capaz. Você, administrador da rede, não sabe o que está fazendo"*, muitos deles alteraram o conteúdo das desfigurações, de modo a reverberar protestos de rua, independentemente da ideologia que veicularam, mas alterando o perfil do ataque por eles intentado. Então, a gente acredita que isso deve acontecer novamente agora, nos Jogos Olímpicos.

O que a gente fez em termos práticos até agora, dos últimos dois eventos para cá? A gente promoveu o cruzamento de bases de dados públicos com registros de ataques. Na prática, o que a gente fez foi uma grande mescla entre um registro de um pouco mais de 2 milhões de ataques em relação a 170 mil serviços de Internet brasileiros. E aqui eu estou me referindo a ataques especificamente de desfiguração, é a ideia do *hacktivism*. Não vou entrar em mais detalhes, porque seriam outros números e a gente não conseguiria vencer isso no prazo que me foi concedido. Significa o quê? Desses 2 milhões de ataques, quais deles foram dirigidos a esses serviços de Internet do Brasil? Aqui, eu me refiro a serviços

governamentais identificados por ".gov", ".leg", ".jus", que são do Poder Executivo, Judiciário, Legislativo e Ministério Público das três esferas, federal, estadual e municipal.

O que se observou é que, desses 2 milhões de ataques, em mais de 100 mil... A gente observou a dispersão por 200 países, e, desses, 100 mil ataques dirigidos contra governo. Dos ataques desferidos contra governo, nós temos — precisamente atualizado hoje, pela manhã — 12.405 ataques que foram realizados contra serviços brasileiros, do Governo brasileiro, de alguma esfera, não necessariamente em relação ao Ministério, não necessariamente em relação a esta Casa, ao Poder Legislativo Federal, mas, em alguma medida, atacaram uma página, uma aplicação *web* de Governo brasileiro.

Se forem observar — o prazo, o lapso temporal coberto por esses ataques vai mais ou menos em 16 anos —, é uma conta em que se tem dois ataques e meio por dia acontecendo. Então, isso é uma ameaça presente, cuja ocorrência naqueles momentos de grandes eventos se acentuou, razão pela qual se conclui que tende a ocorrer novamente. Mas o número é muito vasto e, naturalmente, a gente precisa de algum critério para priorizar e selecionar quais ameaças são mais perigosas, mais agudas ou mais capazes.

Num primeiro momento, a gente observou a questão da nacionalidade ou idioma utilizado pelo grupo, porque isso indicaria a propensão de ataque a alvos brasileiros, especificamente o Governo. Numa amostragem rápida daqueles 12 mil ataques, observa-se que os ataques praticados por grupos, utilizando português ou outros indicativos que sugiram a nacionalidade brasileira, correspondem a quase 40% do total, mas percebe-se a grande quantidade e a variação de países, por exemplo, que indicam que o atacante oportunista, de ocasião, pode não ser de nacionalidade brasileira, o que remonta à fala do pessoal do Ministério de Relações Exteriores aqui, que a elucidação de problemas de ataques cibernéticos envolve realmente cooperação internacional profundamente.

Em geral, as mensagens desferidas por esses grupos não têm conteúdo nenhum contra o Brasil, são veiculações de mensagens políticas de interesse nacional, de interesse doméstico daquele país, daquele grupo que desferiu o ataque.

Num segundo ponto, a gente passou a fazer justamente a análise qualitativa desse conteúdo, com a ideia de classificar os grupos com aquelas categorias. Três categorias emergiram em maioria. Aqui há o destaque para os 7% em relação a grupos que nós classificamos de cibercriminosos, porque, em outras ocorrências, observou-se que aquele mesmo grupo que pratica uma desfiguração realiza também um ato que seria considerado "visando lucro", vamos dizer assim, com a ideia de que ele obtém uma informação e procura vendê-la para benefício pecuniário, razão pela qual ele não se encaixaria nas categorias de ostentação, no sentido de autopromoção, nem no sentido de *hacktivism*, em que ele procura veicular uma mensagem político-ideológica de sua preferência. Então, a tônica do ataque acaba sendo ainda a ostentação, no sentido de que as pessoas estão tentando praticar, demonstrar a sua própria destreza na área de tecnologia da informação.

Num terceiro ponto, nós observamos a avaliação do histórico de atuação em relação a uma agenda política doméstica em grandes eventos. Então, seria a coincidência do interesse do sujeito, a motivação política, relacionada ao histórico recente. É evidente que a atuação passada não necessariamente prediz o comportamento futuro, mas é um indicador que pode ser utilizado, se for combinado com outras evidências disponíveis.

A gente pôde chegar à conclusão de que 28% daqueles grupos estão ativos no presente momento, seja desferindo ataques neste momento, enquanto a gente conversa aqui, enquanto eu faço esta exposição, ou através de outros tipos de manifestação em ambiente digital virtual, uma cifra que sugere a presença, a veracidade da ameaça ou a credibilidade da ameaça diante dos Jogos Olímpicos.

O fato é que, desses 1.600 grupos que nós identificamos originalmente dentre aqueles que praticaram os 12 mil ataques contra serviços de governo, um detalhe adicional que procuramos observar, no nosso caso, foi a questão da automatização do ataque. Isso é muito importante na medida em que maximiza o efeito, o impacto midiático da mensagem veiculada. O sujeito não desfere um único ataque, mas desfere uma sequência deles, para que essa sequência maximize sua chance de ter sucesso. E, por extensão, uma vez que tem sucesso, passa a impressão, para o público que assiste, de que ele é realmente muito capaz ou que o Estado foi, de fato, atingido de maneira severa.

Com esses critérios, a gente pôde observar uma lista — e aqui, os Deputados, V.Exas. me perdoem, porque, por se tratar de audiência pública, eu tive que omitir os nomes especificamente dos grupos. A gente não poderia divulgar essa informação. Ela é tratada de modo classificado. Mas essa listagem indica quais são os 22 grupos, salvo engano, mais relevantes, considerados mais atuantes e que têm o perfil ativo com uma vocação "*hacktivista*" em termos de atuação.

O destaque é dado em cinza para os grupos que, em outros eventos — e ali a penúltima e a antepenúltima colunas indicam a Copa das Confederações e a Copa do Mundo —, em que pesados ataques com características ideológicas foram deferidos por esses grupos, por esses grupos específicos. Hoje, alguma informação existe sobre esses grupos e iniciativas podem ser tomadas em diversos sentidos.

Evidentemente, o objetivo da Agência Brasileira de Inteligência não é efetivar a neutralização dessas entidades. Isso é uma competência que pertence a outras entidades, à entidade policial, tanto que o pessoal de defesa cibernética, todos eles partiram, em alguma medida, dessa atribuição, mas de todo modo essa informação hoje é conhecida pela Agência, pela ABIN.

Eu encerro aqui minha participação.

Ah, sim, perdão. Só um detalhe: a frequência da campanha disso aqui foi adicionada também. Foi considerado como um dado relevante ali, quando foi intensificado o ataque e foram considerados os períodos de inatividade de grupo. Você tem vários períodos de hiato; período em que o grupo se manifesta, atua — 30 a 40 dias de hiato — e volta à tona.

Isso foi contabilizado de modo a perceber quais grupos hoje, por exemplo, estariam no provável período de hiato que eles já demonstraram no passado recente. Então, em alguma medida, aqueles grupos ativos não necessariamente serão o sujeito que hoje, neste instante, encontram-se nesse *status*.

Mas eu encerro, deixo o meu contato. Coloco-me à disposição para perguntas, para eventuais dúvidas e esclarecimentos.

Claro que a gente abordou um ponto específico em relação ao *hacktivism*.

Minha colega, a Carolina, está à disposição para responder a perguntas específicas sobre o tema terrorismo, caso seja do interesse dos Deputados.

Obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Muito obrigada, Dr. Eduardo.

Concedo a palavra ao Sr. Elmiz Antonio Rocha Junior, Delegado, para fazer a sua apresentação.

O SR. ELMIZ ANTONIO ROCHA JUNIOR - Boa tarde, Deputada Mariana, em nome de quem eu saúdo todos os Parlamentares e demais autoridades. Eu vou ser bem breve e tentar, porque muito já foi falado aqui, Deputado Éder, o que já nos esclareceu bastante. Eu vou tentar fazer uma rápida apresentação, uma rápida conversa e ficar à disposição para eventuais dúvidas, principalmente partindo do planejamento da Polícia Federal.

Em primeiro lugar, a Polícia Federal, em unidades permanentes, possui uma divisão de antiterrorismo, a nossa Diretoria de Inteligência, que é quem concentra todas as nossas informações a respeito de terrorismo, de antiterror, e faz contato com todas as demais unidades de inteligência de outros órgãos. Nós temos também um serviço de repressão a crimes cibernéticos, que é também uma unidade permanente da Diretoria de Combate ao Crime Organizado, e que também faz parte desse rol que faz contato também com o CDCIBER — Centro de Defesa Cibernética, com o Exército, com as demais Forças. Então, nós temos parceiros nas duas áreas que nos ajudam, todos os dias, com as atividades normais da Polícia Federal e dos demais órgãos.

Para as Olimpíadas, a Polícia Federal criou uma coordenação específica, da qual eu faço parte, que é a Coordenação de Segurança para Grandes Eventos. A nossa maior missão é tentar concentrar tanto as informações quanto os planejamentos, e ajudar as unidades-fim, as áreas-fim, técnicas, a tentar fazer um planejamento global, no Brasil inteiro, de forma uniforme, e que nós possamos também, nas Olimpíadas, atuar de maneira uniforme com todos os nossos policiais.

No tema das perguntas que o senhor fez, eu vou tentar esclarecer algumas coisas e me coloco à disposição em seguida. Vou tentar ser breve também por causa do andar da hora. Em cada unidade da Polícia Federal para os grandes eventos, em especial para as Olimpíadas, desde a Rio+20, nós criamos determinadas unidades de inteligência que foram voltadas para o grande evento. Essas unidades fizeram, por conta da SESGE — Secretaria Extraordinária de

Segurança para Grandes Eventos , diversas oficinas; trocaram informações o tempo inteiro; estão trocando ainda com o Exército, com as Forças Armadas, com todo o mundo; porque o nosso intuito é que, para a prevenção do ciberterrorismo e do terrorismo em si, a gente sabe que, hoje em dia, quanto mais informação compartilhada, melhor.

Nós temos a intenção, junto com os demais órgãos envolvidos com o planejamento das Olimpíadas, tanto da defesa quanto da segurança, de trocar informação. Em cada cidade-sede do futebol, como Brasília, por exemplo, nós criamos uma unidade temporária para o grande evento e essa unidade fez contato, participa das oficinas, participa de capacitação com as demais forças, de modo que a gente consiga atuar junto. Cada um na sua atribuição, mas, mesmo assim, uma atuação conjunta, de forma que todos possam trabalhar e todos possam tentar cumprir a missão da maneira melhor possível.

Dentro dessas unidades, nós temos um pessoal que se capacitou para o terrorismo e também se capacitou para esses crimes cibernéticos. Eu vou tentar me ater um pouco mais ao terrorismo, para tentar responder as perguntas. Essas unidades, que nós chamamos de Coordenação de Inteligência de cada Superintendência da Polícia Federal, vão ser coordenadas pela Diretoria de Inteligência, tecnicamente, e, como o Delegado William já antecipou, nós teremos um Centro Integrado Antiterrorismo, conforme planejamento feito pela SESGE, e nós vamos ter diversos atores dentro desse Centro Integrado.

Na estrutura de Comando e Controle que vai ser feita para a Olimpíada, que já vem vindo desde a Rio+20, aperfeiçoando com os fatos, com os erros e com os acertos, nós vamos ter um Centro Nacional de Comando e Controle, que vai ser aqui em Brasília. E esse Centro de Antiterrorismo vai ser um órgão de assessoramento para esse Centro Nacional de Comando e Controle, junto com outro Centro, também criado, que é o Centro de Cooperação Policial Internacional.

Qual é a nossa grande arma, a nossa grande força nesses dois Centros? Na verdade, é a troca de informações, porque vai ter pessoal capacitado tanto das forças de segurança, das forças de defesa, dos países envolvidos. A gente também tem feito muitos contatos com relação a esses países que já sofrem há algum tempo com esse tema do terrorismo.

A gente acompanha também essa questão tecnicamente com cursos de capacitação, com troca de informação. Isso tudo é bastante integrado, porque a gente descobriu que, sozinhos, não dá conta de fazer nada, então a gente conta com apoio do Exército, com informações do Exército, com informação das Forças Armadas em geral, dos organismos de segurança. E a gente também entende que não adianta manter a conversa, a coordenação e o planejamento numa esfera muito alta, porque quando um fato que pode ser caracterizado como terrorismo acontece, às vezes quem traz a melhor informação é a Guarda Municipal, alguém que está na rua e que não é daquela área de segurança pública. Então nós também tentamos fazer essa capacitação nessa temática do terrorismo para que nós possamos ter uma informação um pouco mais privilegiada com relação a isso.

A partir desse Centro Integrado de Comando e Controle Nacional, que vai concentrar todas as atividades, o Centro Integrado Antiterrorismo vai fazer esse intercâmbio de informações.

Hoje, com a chegada da nova Lei Antiterrorismo, sabemos que um fato, para ser declarado realmente como terrorismo, necessita de uma investigação policial antes, porque, às vezes, uma mochila deixada num aeroporto é apenas uma mochila, mas pode ser uma bomba, pode ser outra coisa. Pressupomos que, a partir daí, todos os organismos de segurança vão iniciar a busca de uma verdade concreta. E, com a lei, nós podemos fazer todas as medidas de interceptação, a partir das informações coletadas, como fazemos com atividade de crime organizado.

A pena de reclusão melhorou; nós temos as medidas de interceptação; a prisão... Hoje, o cenário para a Polícia Judiciária melhorou muito, porque nós podemos fazer um acompanhamento mais real. O que também descobrimos com relação a esse tema é que, às vezes, a informação melhor coletada dentro do ambiente que aconteceu o fato, ou alguma coisa assim, por não ser da segurança pública, precisa ser tratada. Até que realmente seja tratada essa informação e seja caracterizada como terrorismo, ela é uma ocorrência de rua, uma ocorrência normal. E, a partir desse tratamento, que envolve ações de inteligência, compartilhamento e todas as demais ações, nós poderemos chegar à conclusão de que é um possível atentado, ou um atentado em andamento, para tentar anulá-lo. As medidas judiciais

serão tomadas pela Polícia Judiciária, e nós vamos tentar anular, vamos conseguir anular esse possível atentado.

O que nós também podemos perceber é que, como nós dividimos o planejamento na Polícia Federal por eventos — por exemplo, aqui em Brasília; no Rio, que concentra o maior contingente —, nós precisávamos deslocar policiais capacitados que pudessem atuar nessas áreas. Mas não só os policiais da Inteligência da Divisão Antiterror. Nós também capacitamos os nossos policiais do aeroporto, nossos servidores administrativos, nossos servidores terceirizados, com ajuda de todas as forças de segurança, porque não fazemos sozinhos. Apesar de a atribuição, com a nova lei, ser da Justiça Federal e acabar trazendo para a Polícia Federal essa atribuição de agir nas medidas de interceptação, etc., nós sabemos que nós não conseguimos fazer sem ajuda de todos os órgãos. O Exército nos ajuda bastante. As Polícias Civis, as Polícias Militares, as Guardas Municipais são atores extremamente necessários para o combate e, principalmente, para a prevenção.

Dentro da Polícia Federal, nós tentamos capacitar tanto o nosso pessoal do aeroporto, que é da imigração; o nosso pessoal de segurança de dignitários, que acompanha Chefes de Estado; o pessoal da inteligência; e também o pessoal dos crimes cibernéticos, porque a atuação do serviço de repressão aos crimes cibernéticos hoje, não só pelo crime, mas pelo contato que tem com CDCiber, com o monitoramento, com o acompanhamento, com a troca de informações, também nos traz muitas informações importantes para uma possível prevenção de atentado terrorista.

É óbvio que não temos um efetivo suficientemente capaz para fazer exatamente tudo o que nós gostaríamos de fazer, mas, com apoio, integração e coordenação das outras áreas, dos outros organismos de segurança e de outras entidades — a Prefeitura Municipal do Rio de Janeiro tem nos apoiado bastante, aqui, o Governo do DF —, nós temos capacidade para tentar fazer uma rede de proteção em relação a esse tipo de atentado. Cada cidade tem o seu planejamento, como eu falei, e hoje sabemos que a informação é a principal arma para a prevenção dos atentados.

Na nossa estrutura de Comando e Controle, a partir de um fato qualquer que tenha sido detectado — por exemplo, em Salvador, que é uma cidade sede do

futebol —, automaticamente essa informação vai ser escalada e vai ser tratada dentro do Sistema de Comando e Controle que a SESGE planejou para a atuação das forças de segurança, não só a Polícia Federal, mas todas as forças de segurança.

Dentro de cada Comando e Controle Regional, e também no Comando e Controle Nacional, vai existir uma célula integrada de segurança pública. É nessa célula que as informações mais quentes vão chegar. Nós somos integrantes, mas vamos contar com a participação de todas as forças, porque, a partir desse tipo de integração e de compartilhamento de informações, nós conseguimos detectar, analisar, tratar a informação. E nós sabemos que uma informação num grande evento, qualquer que seja, ganha uma dimensão internacional muito grande. Então, a nossa intenção é realmente fazer um tratamento de informação para passarmos para o grupo gestor estratégico, de comando, da Presidência, da Polícia Federal, do Estado-Maior Conjunto das Forças Armadas. Queremos passar a informação mais real possível. Então, a nossa intenção, na maioria dos casos, é não escalar uma crise sem necessidade e sem o tratamento da informação devido.

Também houve uma dúvida em relação ao acompanhamento. Hoje, nós fazemos um acompanhamento das informações que recebemos tanto de outros países quanto das Forças Armadas e do nosso pessoal de imigração, de fronteira. E fazemos um acompanhamento de possíveis células, de possíveis financiamentos. E houve o questionamento também sobre jovens brasileiros. Nós temos esse acompanhamento. É claro que nós não temos o efetivo suficiente para acompanhar todos os casos, mas, a partir das informações que recebemos, nós conseguimos filtrar, selecionar e tentar chegar para acompanhar pessoas ou fatos que possam vir a caracterizar uma ação preparatória para um atentado terrorista.

A ABIN também nos ajuda bastante — eu estava me esquecendo de mencioná-la —, porque ela coordena o sistema de inteligência há muitos anos. Então, com a integração, o planejamento e a capilaridade da ABIN, ela consegue nos ajudar também no tratamento da informação. Da mesma maneira que nós temos a nossa unidade de inteligência em cada Superintendência que vai ser criada temporariamente para as Olimpíadas, a ABIN também nos apoia, junto com as Forças Armadas, neste momento, porque o tratamento de informação, antes de

qualquer deflagração, de qualquer caracterização do atentado terrorista, é muito importante.

Nós passamos por algumas situações na Rio+20; na Copa das Confederações, por conta das manifestações; na Copa do Mundo; na Jornada Mundial da Juventude, com a vinda do Papa. Se determinada informação não fosse tratada e checada por todos os envolvidos, poderia ter acontecido uma crise desnecessária. E nisso há um papel muito importante da ABIN, das Forças Armadas, da Polícia Federal, dos organismos de segurança pública — a Prefeitura do Rio agiu bastante na Jornada da Juventude.

Então, o modelo de Comando e Controle criado pela SESGE, da qual a Polícia Federal participa, tenta privilegiar — e privilegia — essa troca de informações. Hoje, nós descobrimos que não adianta termos um grupo tático preparado, treinado, capaz de acertar ou de fazer a anulação de um ato terrorista a tantos metros, entrar em determinado ambiente hostil, se nós não conseguirmos fazer um compartilhamento de informações e tratar essas informações antes que se instale uma crise.

Hoje, para a Polícia Federal, o que mais nos importa é tratar a informação, o fato que está na rua, junto com os outros organismos que participam dessa organização — e é a maior operação de segurança pública que nós vamos ter ou tivemos nos últimos tempos —, e tratar essa informação de modo a checar se realmente esse tipo de informação do fato ocorrido pode ser caracterizado como terrorismo. E, para isso, nós dependemos de informações de todos nós — Polícia Federal, Polícia Civil, ABIN, Estado-Maior Conjunto das Forças Armadas. A informação não é privilégio de poucos, é de muitos. Quanto mais informação nós tivermos, melhor nós conseguiremos tratá-la e fazer com que a Inteligência trabalhe antes da ação propriamente dita.

Eu não vou me alongar muito, até porque, se houver alguma dúvida, eu vou tentar esclarecê-la, mas esse é um panorama geral. A Polícia Federal participa desse planejamento junto com a SESGE e os outros organismos de segurança para as Olimpíadas.

Encerro minha fala, Deputada.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Muito obrigada.

Concedo a palavra aos autores do requerimento. Vou passar primeiramente a palavra ao Sr. Deputado Delegado Éder Mauro e, em seguida, ao Sr. Deputado Silas Freire.

O SR. DEPUTADO DELEGADO ÉDER MAURO - Sra. Presidente, Srs. Deputados, gostaria de agradecer, mais uma vez, aos palestrantes, na pessoa do Leonardo Motta, Diretor do Departamento de Infraestrutura e Serviços de Tecnologia da Informação; o Eduardo Izycki, da ABIN; e o Delegado Elmiz Júnior, da Polícia Federal.

Acredito que o tema já foi amplamente debatido não só por vocês, mas por nós que fizemos as perguntas. A preocupação geral era exatamente em cima das perguntas que foram feitas.

Eu tinha uma preocupação, não só como cidadão, mas como policial que fui. Sei como, pelo menos nos crimes comuns, as coisas acontecem — foram 30 anos na Polícia. Na condição de Parlamentar, fui procurado inclusive por pessoas ligadas ao sistema de segurança do Governo Federal, que denunciavam que as coisas não estavam acontecendo. Por isso, sei que a presença de vocês aqui é de suma importância.

Percebemos pela fala do delegado que existe um sincronismo muito grande entre a Polícia Federal, a ABIN e o Exército brasileiro na troca de informações, e sabemos do trabalho que vocês têm desempenhado e da força-tarefa que vocês têm em todos os setores, principalmente no tráfico internacional, em que nós temos hoje como vizinhos dois países que praticamente têm como líderes verdadeiros "cocaineiros" — o que lamentamos!

Então, eu fico satisfeito ao entender que as coisas realmente estão acontecendo de acordo com o que foi dito por todos vocês, porque a nossa preocupação é, em primeiro lugar, com as pessoas inocentes, independentemente da nacionalidade; é com os atletas que virão para cá; é com os brasileiros que apreciarão e participarão das Olimpíadas; é com a figura do nosso País, que já está tão maltratada. Esperamos que não tenhamos nenhuma surpresa. Eu sei que não é fácil — todos nós sabemos —, porque esse é um tipo crime diferenciado, silencioso e covarde, que é difícil detectar. É preciso realmente que as pessoas estejam todas

juntas, para que possamos chegar a identificar esse perigo e fazer com que a coisa não aconteça.

Então, eu só tenho a agradecer a presença de todos vocês. Volto, mais uma vez, a parabenizar todos, nas pessoas, inclusive, do Delegado da Polícia Federal e do Coronel do Exército.

Obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Deputado Delegado Éder Mauro.

Concedo a palavra ao Deputado Silas Freire.

O SR. DEPUTADO SILAS FREIRE - Para não nos alongarmos, Presidenta, eu só queria deixar aqui ainda a nossa preocupação, embora tenha notado nas falas a integração desses órgãos de comunicação, nós ainda estamos preocupados em reafirmar o compromisso e a importância de esta Comissão visitar o centro de cuidados com as Olímpiadas, convite que nos foi feito por um dos expositores.

E gostaria de deixar uma pergunta: se Deus quiser — eu sou muito crente em Deus —, nós não teremos guerra cibernética durante as Olimpíadas. Se Deus quiser, a Internet não será usada para nenhum ataque terrorista e para por nenhuma mancha na honra das nossas Olimpíadas. Passado esse momento, a segurança nacional cibernética do País tem um plano — essa é a pergunta — ou é só para as Olimpíadas?

Obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Aproveitando a pergunta de V.Exa., Deputado Silas Freire, vou fazer uma pergunta também relacionada a esse tema.

Temos percebido que a imprensa tem considerado os nossos Jogos Olímpicos, que serão realizados na cidade do Rio de Janeiro, como um evento de risco, tanto em decorrência da cobertura massiva da imprensa mundial quanto pela presença de delegações de diversas nacionalidades que são alvos do Estado Islâmico.

Tendo em vista as graves consequências dos ataques empreendidos por integrantes de grupos terroristas, como foi o caso que vitimou a cidade de Paris, na França, no dia 13 de novembro do ano passado, peço a opinião de todos que

imaginem o possível caso de uma ameaça de atentado terrorista vinculado pela Internet durante a realização dos Jogos Olímpicos aqui em 2016.

Nesse caso, vocês acreditam que há risco de que o atentado venha a se concretizar antes que seja proferida a decisão judicial, autorizando o acesso aos registros de conexão e de acesso à aplicação da Internet, necessários à identificação da autoria da ameaça? Como lidar com esse problema, na visão de vocês, e qual a melhor forma de se equacionar essa questão?

Essa é uma das questões que temos debatido muito durante este período da CPI, sobre essas consequências e as questões relacionadas à legislam. Nós sempre temos aberto aqui essa forma de diálogo para mandarem para a própria Comissão ideias e sugestões que possam dar uma melhor segurança para o uso das redes no nosso País. Se tiverem sugestões, podem mandá-las agora ou depois para o *e-mail* da CPI.

O SR. ELMIZ ANTÔNIO ROCHA JÚNIOR - Bom, deixe-me adiantar.

Com relação à pergunta do Deputado, nós temos plena convicção de que é necessário um plano. Para isso, nós temos essa integração muito boa para aperfeiçoar o plano.

A CPI conta com um membro valiosíssimo de consultoria, o Delegado Versiani, que é realmente bastante capacitado nessa área. Ele trabalhou muitos anos no serviço de repressão a crimes cibernéticos e é uma pessoa que esclarece bastante a área técnica.

Pelo menos por parte da Polícia Federal, para acompanhar a questão do terrorismo via Internet e dos crimes cibernéticos nós possuímos unidades permanentes. Quando terminares as Olimpíadas, essa unidade voltará a operar, como já operava antes dos grandes eventos, desde os Jogos Mundiais Militares.

É uma preocupação nossa fortalecer essas unidades, consolidar a capacitação de policiais, para que possam integrar essas unidades, e promover a permanência delas onde estão, tanto na Diretoria de Inteligência, quanto na Diretoria de Combate ao Crime Organizado.

E é realmente uma preocupação muito perspicaz, porque não nos adiantaria fazer um planejamento estratégico e operacional para os grandes eventos que já aconteceram e agora para as Olimpíadas, se depois não aproveitarmos nada.

Este é o principal papel da Coordenação de Segurança em Grandes Eventos dentro da unidade da Polícia Federal: fazer com que o legado operacional e o planejamento estratégico fiquem na Polícia Federal como uma arma capaz de pulverizar os métodos que nós utilizamos nas Olimpíadas, na Copa do Mundo e na Jornada da Juventude como atribuições permanentes da Polícia Federal, porque nós descobrimos que medidas administrativas simples que nós começamos a tomar nos ajudaram bastante na área de logística, área operacional e área-fim.

Então, a intenção da Direção da Polícia Federal é fazer com que esse legado, para nós, não seja apenas de compra de material ou de capacitação do pessoal, mas sim de capacitação do nosso planejamento para as operações futuras em especial na Divisão Antiterrorismo e no Serviço de Repressão a Crimes Cibernéticos.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Concedo a palavra ao Sr. Leonardo Boselli da Motta.

O SR. LEONARDO BOSELLI DA MOTTA - A grande preocupação do Ministério do Planejamento é justamente com a segurança das redes de Governo e dos serviços que estão sendo executados e prestados lá tanto aos órgãos, quanto aos cidadãos.

Atualmente, há um trabalho da STI junto às principais empresas de Governo, SERPRO, DATAPREV e TELEBRAS, para que elas possam atuar, cada vez mais em conjunto, cada vez mais integradas, não só na questão da integração das redes de Governo, quanto também na das próprias equipes dessas empresas, que cuidam do tratamento dos incidentes.

A STI deu início a um projeto em parceria com o INMETRO para desenvolver um sistema de homologação e certificação de ativos de tecnologia da informação. Nós vamos realizar, a partir do mês que vem, uma consulta pública às empresas e a todos que quiserem participar acerca de alguns critérios de auditoria e serviços prestados, que estão descritos no Decreto nº 8.135 e na Portaria Interministerial nº 141. O Decreto trata justamente da comunicação segura e da dispensa de licitação nas contratações que possam trazer algum risco à segurança nacional.

Nós já definimos e publicamos alguns padrões de auditoria e queremos estendê-los não só para o serviço que vai ser disponibilizado agora, o serviço de

correio eletrônico, como também para os outros serviços descritos na própria portaria, como compartilhamento e sincronização de arquivos, mensageria, videoconferência e voz sobre IP. Esses serviços são utilizados pelos órgãos e podem trazer risco à segurança nacional no caso de vazamento de informações.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Concedo a palavra ao Dr. Eduardo, para as suas considerações.

O SR. EDUARDO ARTHUR IZYCKI - A pergunta remonta à possibilidade de antecipação de um ataque terrorista ou um ataque conduzido pela Internet.

É importante observar que a antecipação de um ataque dessa natureza requer um trabalho preventivo, que não necessariamente vai ser conduzido pela autoridade policial que atua, por excelência, após a consumação do fato delitivo.

Por essa razão, vai recair sobre órgãos de defesa e órgãos de segurança cibernética a incumbência da prevenção do ataque em si.

Se me fosse permitido fazer uma sugestão, eu diria que a legislação hoje, sobretudo a legislação que tipifica o crime de invasão de dispositivo informático, tipifica a conduta em que o sujeito viola um dispositivo sem o consentimento do seu titular, sem necessariamente graduar o dolo, o objetivo do sujeito que o faz. Isso, na prática, inviabiliza que medidas de segurança e de defesa cibernética antecipem vulnerabilidades.

Cito um exemplo: o ano de 2014 foi profícuo em grandes vulnerabilidades que afetaram diversos sistemas de maneira copiosa. O pessoal do Ministério do Planejamento certamente vai se lembrar do Heartbleed, que foi um *bug* no desenvolvimento da camada de criptografia. A detecção desse *bug*, dessa vulnerabilidade, requereria por parte de um terceiro, se não fosse feito pelo próprio administrador da rede, a prática do tipo penal. Requereria que o sujeito tentasse explorar aquela vulnerabilidade, obtivesse um dado específico da memória disponível daquele servidor para que ele pudesse dizer: *"Sim, esse servidor hoje se encontra vulnerável".* Não me refiro ao servidor público, mas ao servidor eletrônico.

Isso poderia dar início a uma ação imediata e de emergência para a correção daquela vulnerabilidade, que não dependeria da atenção do próprio administrador cujo trabalho de defesa e de segurança seria feito de maneira proativa e preventiva. No entanto, a lei não toma o cuidado de excluir essa atuação das entidades.

Eu não falo em nome da agência nesse sentido, mas eu tenho certeza de que outros órgãos responsáveis gostariam muito que esse tipo de atuação fosse considerado de maneira normativa, ou melhor, que uma medida legislativa considerasse esse pormenor. Esse é um detalhe muito técnico, eu sei, mas certamente ajudaria e, respondendo à pergunta, preveniria sim um ataque conduzido pela Internet.

Obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Dr. Eduardo.

O SR. DEPUTADO SILAS FREIRE - Sra. Presidente, V.Exa. me permite a palavra?

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Concedo a palavra ao Deputado Silas Freire.

O SR. DEPUTADO SILAS FREIRE - Eu requeiro a V.Exa. que solicite aos nossos consultores que façam a leitura deste seminário para que sejam registrados em um documento os relatos aqui expostos e enviados não só ao Comitê Olímpico, como também a seleções e a comitivas que virão ao País, demonstrando a preocupação desta CPI e desta Casa e o preparo e a integração que essa equipe tem no País.

Nós temos que mandar isso para eles e para veículos de comunicação, mostrando a nossa preocupação, porque, de fato, há todo um trabalho. É claro que pode haver surpresas, mas está sendo feito todo o possível para atender o necessário.

Muito obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Fica feito aqui o registro, fazendo o pedido aos consultores para avaliarem isso, elaborarem esses documentos e registrarem essa questão até mesmo nos nossos relatórios finais.

Dessa forma, estudamos as condições e registramos as sugestões para as Olimpíadas, que têm que deixar seu legado.

Trata-se de segurança nacional. Precisamos estar preparados para ser sede de vários eventos de forma segura, anulando a imagem de insegurança que há no País e que, infelizmente, está sendo passada para o exterior. Sem dúvida, o trabalho desta CPI está relacionado a esse tema.

Sugiro a criação de comissões que debatam continuamente o assunto, até porque os crimes cibernéticos avançam muito rápido.

Os senhores podem contar com esta CPI e com este Parlamento, que pretendem trabalhar para proteger os brasileiros e os estrangeiros de qualquer ataque no meio cibernético.

Quero, mais uma vez, agradecer a presença de todos e, em especial, do Delegado Elmiz pela sua disponibilidade, do Dr. Leonardo por ter se colocado à disposição, do Dr. Eduardo por contribuir para esta Comissão Parlamentar de Inquérito e dos Deputados autores do requerimento.

Nada mais havendo a tratar, declaro encerrada a presente audiência pública, antes convocando reunião da Comissão para a próxima quinta-feira, dia 31 de março, às 10 horas, para o último debate sobre os direitos da mulher.

Informo que, na próxima reunião de quinta-feira, faremos também apresentação do relatório da CPI.

Obrigada a todos.

Está encerrada a reunião.