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: 1767/15	DATA: 17/09/2015	
LOCAL: Plenário 9 das Comissões	INÍCIO: 10h27min	TÉRMINO: 13h03min	PÁGINAS: 53

DEPOENTE/CONVIDADO - QUALIFICAÇÃO

MARCONNI DOS REIS BEZERRAS - Diretor do Departamento de Segurança da Informação e Comunicação — DSIC, do Gabinete de Segurança Institucional da Presidência da República — GSI.
OTÁVIO CARLOS CUNHA DA SILVA - Diretor do Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações — CEPESC, da Agência Brasileira de Inteligência — ABIN.
PAULO ROBERTO DE ARAÚJO CASTRO VIANNA - Chefe da Divisão de Operações do Centro de Defesa Cibernética do Exército — CDCiber.

SUMÁRIO

Debate sobre segurança institucional no Brasil.

OBSERVAÇÕES

Houve exibição de imagens.
Houve intervenção fora do microfone. Inaudível.
A reunião foi suspensa e reaberta.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Bom dia.

Declaro aberta a 13ª Reunião Ordinária de audiência pública da CPI dos Crimes Cibernéticos.

Encontra-se à disposição dos senhores membros cópia da ata das 12ª reunião, realizada no dia 15 de setembro de 2015.

Pergunto se há necessidade de leitura da ata.

O SR. DEPUTADO SANDRO ALEX - Peço dispensa, Sra. Presidenta.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Fica dispensada a leitura da ata, a pedido do Deputado Sandro Alex.

Em discussão a ata. *(Pausa.)*

Não havendo quem queira discuti-la, em votação. *(Pausa.)*

Aprovada.

Comunico o recebimento dos seguintes documentos: Ofício nº 32/15, de Brasil Internet, que solicita prazo adicional de 15 dias para envio das informações financeiras e fiscais solicitadas pela CPI na reunião do dia 27 de agosto de 2015.

Ordem do Dia.

Audiência pública.

A reunião de hoje tem como pauta a realização de audiência pública sobre segurança institucional, em atendimento ao Requerimento nº 29/15, de autoria da Deputada Alice Portugal, e ao Requerimento nº 38/15, de autoria do Deputado João Arruda.

Convido para compor a Mesa o Sr. Marconni dos Reis Bezerras, Diretor do Departamento de Segurança da Informação e Comunicações, do Gabinete de Segurança Institucional da Presidência da República; o Sr. Otávio Carlos Cunha da Silva, Diretor do Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações da ABIN; o Coronel Paulo Roberto de Araújo Castro Vianna, Chefe da Divisão de Operações do Centro de Defesa Cibernética do Exército.

Cada convidado terá 15 minutos para sua exposição. Após as apresentações, será passada a palavra ao Relator, aos Sub-Relatores e aos autores do requerimento. Os convidados respondem a esse bloco de indagações. Em seguida, na ordem da lista de inscrições, os senhores membros poderão interpelar os

convidados. Os expositores responderão mais a esse bloco, podendo haver réplica e as considerações finais.

Feitos esses esclarecimentos, vamos iniciar a audiência.

Vamos iniciar ouvindo o representante do Gabinete de Segurança Institucional — GSI — da Presidência da República.

Com a palavra o Sr. Marconni dos Reis Bezerras, Diretor do Departamento de Segurança da Informação e Comunicações.

O SR. MARCONNI DOS REIS BEZERRAS - Exma. Sra. Deputada Mariana Carvalho, Presidente desta CPI; Exmo. Sr. Deputado João Arruda e Deputada Alice Portugal, autores dos requerimentos já citados; Exmos. Srs. Parlamentares presentes; minhas senhoras, meus senhores, um bom-dia a todas e a todos.

Eu gostaria que projetassem alguns eslaides que eu trouxe para mostrar aos senhores, atendendo ao requerimento que foi apresentado ao Gabinete de Segurança Institucional, no sentido de falar sobre algumas ações do gabinete em prol do combate ao crime cibernético, sobre o que nós temos feito.

O Gabinete de Segurança Institucional, hoje, é aqui representado pelo Diretor do Departamento de Segurança da Informação e Comunicação. Também, logo após a minha fala, deve tecer alguns comentários o Dr. Otávio, falando pela Agência Brasileira de Inteligência, que também é vinculada ao Gabinete de Segurança.

Eu coloquei nos eslaides ali algumas informações que seriam úteis para os senhores levarem em consideração. Aguardo a projeção. *(Pausa.)*

(Segue-se exibição de imagens.)

O primeiro eslaide mostra a estrutura do nosso Gabinete de Segurança Institucional. Ali eu destaquei os setores do nosso gabinete que tratam do tema *Segurança da Informação.* Nós temos no gabinete o Departamento de Segurança.

Então, esta é a estrutura do nosso Gabinete de Segurança Institucional. Eu destaquei ali, em amarelo, apenas os pontos sobre os quais eu vou tecer alguns comentários e que dizem respeito aos locais onde, no gabinete, é tratado o tema *Segurança da Informação*.

Ali é o DSIC, que é o Departamento de Segurança da Informação e Comunicação, o Departamento que eu dirijo. É de competência da CREDEN também temas relacionados à segurança da informação e segurança cibernética. Na

CREDEN, o nosso Ministro exerce a Presidência da Câmara de Relações Exteriores e Defesa Nacional; no Conselho de Defesa Nacional, o nosso Ministro é o Secretário-Executivo desse Conselho. Também está na competência do CDN ações voltadas para a segurança da informação. É na qualidade de Secretário-Executivo do Conselho de Defesa Nacional que o nosso Ministro homologa as normas publicadas na área de segurança da informação para toda a APF, que eu vou comentar um pouco mais adiante.

Ali também, na estrutura do nosso gabinete, como eu já comentei, temos as Secretarias que tratam da atividade-fim do gabinete e a Agência Brasileira de Inteligência, que também lida com segurança da informação e comunicação principalmente no seu centro de pesquisa para a segurança das comunicações. O Dr. Otávio depois vai tecer alguns comentários a respeito do que vem sendo desenvolvido ali no CEPESC.

Ali está a estrutura do nosso Departamento de Segurança da Informação e Comunicação com as três Coordenações que nós temos. O Departamento foi criado em 2006. A primeira Coordenação, a da direita, embaixo, trata do Núcleo de Segurança e Credenciamento, que está mais voltado para as questões da Lei do Acesso à Informação; ele é o órgão central do sistema de credenciamento, instituído pela lei do acesso do Governo brasileiro, e é o órgão encarregado de credenciar pessoas e empresas para o tratamento de informação classificada. Essa é a atividade principal do Núcleo de Segurança e Credenciamento.

A Coordenação-Geral de Tratamento de Incidente de Redes, onde está o nosso CTIR Gov — Centro de Tratamento de Incidente de Redes de Governo, monitora as grandes redes do Governo Federal. Tudo que é “.gov”, “.mil”, “.leg”, “.jus” é monitorado diuturnamente por essa equipe incessantemente, na busca de tentativas de ataques, tentativas de pichações, de sítios etc. Todo tipo de incidente que ocorre com as redes de Governo é tratado pelo CTIR Gov. E a Coordenação de Gestão de SIC é uma Coordenação mais voltada para normatização, capacitação, conscientização, seminários. Nós trabalhamos junto com a APF para essas questões voltadas para a gestão de segurança na informação. Essa Coordenação trabalha estreitamente com o Comitê Gestor de Segurança da Informação, que está naquele vínculo com o nosso Departamento. As reuniões do Comitê Gestor de

Segurança são coordenadas pelo Diretor do DSIC. É o Diretor do Departamento que coordena as reuniões e é de onde nascem as normas publicadas, voltadas para a segurança da informação.

Ali são apenas alguns momentos dessas reuniões mensais do Comitê Gestor de Segurança. Esse Comitê é composto por dezessete Ministérios. Ele foi instituído no Decreto nº 3.505, de 2000, e compunha inicialmente em torno de doze Ministérios, mas outros foram sendo agregados. Hoje nós temos dezessete membros titulares e suplentes desses Ministérios, que se reúnem mensalmente, toda segunda e quarta-feira de cada mês, ali no anexo do Palácio do Planalto, para abordar, normatizar algum tema relevante na área de segurança da informação. O nosso Ministro tem procurado, todos os meses, fazer abertura desse avento. Dali saem, então, aquelas normas, sobre as quais já comentei. Vou tecer um pouco mais de detalhes, à frente, a respeito das normas do Comitê Gestor de Segurança.

Ali mostra apenas algumas ações que estão em andamento, no momento, no âmbito do Comitê Gestor: Guia de Boas Práticas do Planejamento de SIC; Autodiagnóstico; são atividades que constam da nossa estratégia de segurança cibernética, publicada agora, no dia 12 de maio de 2015, no *Diário Oficial*. Algumas metas já foram levadas para o Comitê Gestor, e já está em andamento o cumprimento dessas metas com a participação do Comitê Gestor.

No próximo eslaide, eu coloquei a legislação em vigor que ampara o nosso trabalho no Gabinete de Segurança na área de segurança da informação. É o Decreto nº 3.505. Eu já o comentei. Esse decreto, em 2000, já determinou que todo órgão e entidade da APF já elaborasse a sua política de segurança da informação. Isso foi o mandamento desse decreto em 2000. Ele também instituiu o Comitê Gestor de Segurança da Informação, que vem se reunindo até hoje.

Eu destaco ali a Lei nº 12.462, que define a estrutura da Presidência e dos Ministérios. Nas mudanças de Governo, essa lei vem sendo atualizada e mantida, entre outras competências do Gabinete, aquela de coordenar a atividade da inteligência federal, por parte da ABIN, e as atividades também de segurança da informação. Então, esse é o nosso amparo legal no GSI para coordenar, no âmbito da APF, essas questões de segurança da informação.

O próximo eslaide tem apenas outras referências na legislação em vigor. A Lei do Acesso, como os senhores bem sabem, de 2011, foi regulamentada com aqueles dois decretos, um voltado mais para o acesso à informação e à transparência, e o segundo decreto sobre o tratamento da informação classificada.

Quanto ao Decreto nº 8.135, o Gabinete de Segurança teve participação quando ele foi regulamentado pela Portaria nº 141. Essa portaria definiu as condições para que houvesse dispensa de licitação. O Gabinete fez constar que a dispensa da licitação poderá até ocorrer, desde que sejam observadas as disposições relativas à segurança da informação, numa possível contratação de um órgão público.

No próximo eslaide, tem ali os três amparos, as três referências na legislação brasileira que tratam mais detalhadamente das questões do crime cibernético, que é o objeto principal aqui desta CPI.

A Lei nº 12.735, a Lei Azeredo, a Lei nº 12.737, que é a Carolina Dieckmann, e o Marco Civil da Internet, leis sobre as quais o Gabinete foi consultado em alguns momentos e teve alguma participação no texto final desses dispositivos legais.

No próximo eslaide, eu cito alguns acórdãos do TCU. O Gabinete de Segurança Institucional elabora, juntamente com o Comitê, todo esse normativo, esse arcabouço legal que define as regras de segurança para a APF, mas ele não tem poder de polícia. Então, o TCU tem sido um grande parceiro, um grande colaborador do Gabinete no sentido de cobrar de toda a administração. Nas auditorias que o TCU faz, o referencial são as normas do Departamento de Segurança e do Comitê Gestor, que estão em vigor, são as normas cobradas pelo TCU.

Eu cito ali principalmente o Acórdão nº 1.233, que é de 2012, que diz que as normas do GSI não são facultativas, mas, sim, obrigação da alta administração de todos os órgãos. Esse acórdão também nomeou os doze OGS, os Órgãos Governantes Superiores, especialistas em diversos setores no Governo Federal. Na área de segurança da informação, ele foi eleito, nesse acórdão pelo TCU, como órgão governante superior nas ações em questões de segurança da informação.

O Decreto nº 3.051, que já é de 2014, enfatiza as questões de planejamento, que também são obrigatórias, e o planejamento de SIC é motivo de uma das normas

do Comitê, que é a Norma nº 02. Destaco ali que o TCU recomendou também que o GSI elaborasse uma estratégia de geral de segurança cibernética, segurança da informação. Como fruto dessa recomendação, no final do ano passado, o GSI começou a trabalhar. Em maio deste ano, no dia 12, foi publicada então a estratégia dessa versão 1.0 de segurança cibernética e segurança da informação para toda a APF.

Ainda no Acórdão nº 3.051, que é o próximo eslaide, também o TCU faz um comparativo com o levantamento feito em 2012 e o que ele observou em 2014. Em questões de gestão de acidente, 75% dos órgãos apresentam falhas. Na questão de Gestão de Risco de Segurança da Informação, também se constatou que 85% dos órgãos apresentavam falhas naquela auditoria realizada no ano passado.

Pelo Acórdão nº 3.117, o TCU, em novembro, fazendo esse comparativo de 2012 com 2014, constatou que houve melhoria, houve evolução em relação ao cenário de 2012, nos aspectos de Política de Segurança da Informação. No final de 2014, 68% dos órgãos já tinham a sua política de segurança formalizada. O Comitê Gestor de Segurança da Informação é mandamento de uma das normas do nosso Comitê também. Sessenta e dois por cento dos órgãos já instituíram o seu Comitê Gestor. O Controle de Acesso, que era de apenas 26%, em novembro de 2014 já tinha 52%. O TCU constata que, apesar de ter ocorrido essa melhoria, estamos ainda longe do ideal. Há muito o que fazer ainda. A adoção da prática ainda está distante do esperado, segundo palavras do TCU.

No próximo eslaide, eu coloquei uma definição que está na nossa Instrução Normativa nº 01, que é uma normativa de 2008, que define o que seria a segurança da informação e comunicação. Essa é a dica, meus senhores, que nós temos passado para toda a administração pública federal. A segurança da informação e comunicação são ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade. Nessas quatro palavras tem muita tecnologia envolvida, muito trabalho de pesquisa e desenvolvimento vem sendo feito, não apenas pelo GSI, como também pelo CEPESC e vários órgãos da APF nesse sentido, mas muitos procedimentos envolvidos estão aí também. Então, não é só tecnologia. Segurança da informação é muito também de procedimentos, de comportamento das pessoas. Nós costumamos sempre dizer que o elo mais fraco

nessa cadeia da segurança da informação são as pessoas, e com as pessoas que nós temos trabalhado intensamente no sentido de capacitar, conscientizar, formar gestores de segurança de informação para toda a APF.

No próximo eslaide, tem uma rápida visão das redes de segurança. É um trabalho feito por aquela coordenação nossa do CTIR Gov, em que as 320 grandes redes do Governo Federal são monitoradas diuturnamente. Nós temos mais de 180 equipes de tratamento de acidentes de rede em todos os órgãos da APF. Eles tentam detectar o incidente lá na ponta. Quando não conseguem, eles repassam esse incidente para o CTIR Gov tratá-lo. São resolvidos 98%, sendo 55% deles em até 24 horas. Não são resolvidos todos, porque independem muitas vezes da ação do CTIR Gov, independem de ações na ponta. Nós notificamos aquele que foi atacado ou tentamos identificar o atacante, mas a solução para esse incidente muitas vezes independe da nossa vontade.

Ali, apenas a título de exemplo para os senhores, está um gráfico que nós tentamos atualizar trimestralmente no site do DSIC e que dá uma visão geral da situação de ataques, de todos os tipos de ataques que ocorrem nas redes de Governo, com uma ênfase maior ali no abuso de sítio. Onde consta abuso de sítio, lê-se pichação de sítio de *sites* do Governo. Em segundo lugar, páginas falsas, também do Governo Federal. Diariamente, novas páginas falsas são publicadas, e o nosso CTIR Gov tem que fazer a notificação, solicitando a retirada desse *site* falso do ar.

No próximo eslaide está todo o arcabouço normativo da nossa coordenação de gestão SIGs juntamente com o trabalho do Comitê Gestor de Segurança, já publicado, em vigor e disponível no nosso *site* da Internet. A primeira normativa é de 2008. Depois vieram mais duas instruções normativas. Nós temos 21 normas complementares publicadas. São complementares àquela Instrução Normativa nº 01. Destaco ali as mais importantes, em que os órgãos têm procurado trabalhar mais em cima. A questão da política de SIC, a implementação da sua equipe de tratamento de incidentes de redes, gestão de incidente de redes. A última é a Norma nº 21, "*Coleta e preservação de vidências e incidentes de segurança de rede da APF,*" que está mais relacionada a esse trabalho preventivo do crime cibernético, realizado pelo GSI. Nós não realizamos no GSI combate ao crime cibernético, mas

nós realizamos um trabalho preventivo de combate ao crime cibernético. Essa norma foi elaborada com o apoio da Polícia Federal, de vários agentes, dos tribunais de justiça de São Paulo, vários órgãos da Justiça trabalharam conosco elaborando essa norma que está em vigor e em utilização por todos os órgãos.

No próximo eslaide, há apenas outras publicações de caráter bem geral a respeito da segurança da informação. São publicações de 2010. A nossa estratégia, como eu comentei, foi publicada agora em maio de 2015. São publicações que estão disponíveis para todos os órgãos da AAPF recomendando, enfatizando e solicitando que todos observem esses quesitos de segurança publicados e em vigor.

O próximo eslaide mostra o fruto da atuação da nossa Coordenação de Gestão em toda a APF. Em termos de servidores sensibilizados, mais de 50 mil. Isso no período desde o início da atuação do DSIC, de 2008 até os dias de hoje. Mais de 6 mil capacitados, 300 especialistas em gestão — são gestores de segurança da informação. Foram formados num acordo, num convênio realizado entre o GSI e a UnB, aqui em Brasília. Foi um curso no nível de mestrado. Esses 300 gestores já foram formados e apresentaram seus trabalhos finais. Este ano tivemos a formatura da última turma, mais de 114 alunos formados. Então, é a massa crítica de gestores de alto nível que nós temos disponibilizado para toda a APF. Temos continuado trabalhando nesse sentido de formar mais pessoas.

Esses alunos geraram um arcabouço de mais de 2.200 estudos de casos dos seus órgãos especificamente. A maioria dos trabalhos está disponível também no nosso *site*, porque muitas vezes o problema detectado por um determinado órgão pode ser utilizado para outros setores também. Temos realizado incessantes Oficinas de Colóquios Técnicos, voltados sempre para essa questão de capacitação e conscientização dessas questões de segurança da informação.

O próximo eslaide tem algumas ações realizadas pela nossa coordenação do Núcleo de Segurança e Credenciamento. Nós ali credenciamos os gestores de segurança, conforme determinado pela Lei do Acesso e seus decretos. Os gestores de segurança e credenciamento que vão dar prosseguimento na estrutura de tratamento da informação classificada no âmbito dos órgãos.

O órgão nível 1, que é o Ministério ou equivalente, já foi habilitado, e estamos já em pleno desenvolvimento da sua estrutura interna no Ministério das Relações

Exteriores e Ministério da Defesa. Temos realizado em vários órgãos, sempre que solicitados, em apoio a essas questões de tratamento da informação com essa coordenação.

Acordos internacionais também para a troca de informação classificada são necessários quando uma empresa brasileira assina um contrato com uma empresa internacional, contrato esse no qual envolva a troca de informação classificada. Então, a empresa brasileira precisa ser credenciada. Isso só ocorre com determinado país se nós tivermos um acordo formalizado. O Ministério das Relações Exteriores tem trabalhado em conjunto conosco. A assinatura desse acordo sempre é feita sob coordenação do Ministério das Relações Exteriores.

No próximo eslaide, eu teço alguns detalhes a respeito da nossa estratégia, que eu já comentei, publicada agora em maio de 2015. Está ali a missão da nossa estratégia. Consta da estratégia dez objetivos estratégicos e 38 metas estratégicas no seu período de vigência, que é de 2015 a 2018. Essa estratégia foi homologada agora com a Portaria nº 14, de 11 de maio, e publicada no *Diário Oficial* nº 88, do dia 12 de maio. No próximo eslaide, eu mostro o mapa estratégico que consta dessa estratégia. Esse mapa estratégico foi elaborado com a metodologia do Balanced Scorecard, que é o que tem de mais evoluído nessa questão de planejamento estratégico.

Ali estão os objetivos. Aqueles dez objetivos estratégicos foram concentrados em quatro dimensões. Uma dimensão, que é a base de tudo, na área financeira; numa outra dimensão, dois objetivos voltados para o aprendizado, crescimento e inovação; quatro objetivos voltados para os processos internos de Governo; e outros dois objetivos voltados para resultados para a sociedade, no que a sociedade poderá se beneficiar também dessa estratégia, em termos de segurança da informação.

Esta é apenas uma visão geral para os senhores terem ideia desse mapa estratégico que consta da nossa estratégia que está no *site* do DSIC.

No próximo eslaide, nós colocamos um modelo de governança sistêmica de segurança da informação e segurança cibernética que também consta da estratégia. Ali o órgão central, instituído na estratégia, que é o GSI, amparado no decreto, na lei que define a estrutura da Presidência da República, com a competência nossa na

área de coordenar as atividades de segurança da informação. Então, ele está ali como órgão central dessa questão, em toda a APF.

Os órgãos gestores, que estão ali nos níveis A e B, que são Ministérios, órgãos subordinados e órgãos setoriais e seccionais dentro de cada Ministério. Ali as instituições colaboradoras. Ali entra academia, o setor público, o setor privado, empresas, etc., que também colaboram, interagem com esse órgão central. E instâncias de assessoramento e apoio à decisão. Eu já citei bastante aqui o Comitê Gestor de Segurança da Informação. Eu destaco ali a Câmara Multissetorial, que foi instituída pela nossa estratégia. O próximo eslaide, inclusive, mostra o cumprimento de metas em andamento. Uma delas é a instituição da Câmara Multissetorial.

Uma portaria desta semana a nossa mídia já está publicando com a instituição dessa Câmara Multissetorial. Da Câmara participarão empresas privadas, setores, academia, etc., que poderão interagir e colaborar na evolução dessa estratégia.

Ali eu destaco a Meta 1, que é definir uma metodologia e mecanismo de autodiagnóstico. Cumprindo essa meta, que já era para 2015, já foi publicada também agora, no dia 25 de junho, uma portaria do nosso Ministro instituindo o Grupo de Trabalho no âmbito do Comitê Gestor de Segurança para definição dessa metodologia que vai ser aplicada em toda a APF.

Ali eu destaco também a Meta 7, que é propor um guia de boas práticas. Isso aí também já foi publicado numa portaria do Comitê Gestor para que um grupo do Comitê... São especialistas de todos os Ministérios, daqueles dezessete Ministérios que eu comentei. Esse grupo de especialistas, então, vai estudar esse tema e trazê-lo para apreciação do Comitê e possível publicação de um novo normativo.

No próximo eslaide está ali a Meta III, que é articular e estabelecer um programa no PPA 2016-2019 que contemple conjuntamente as telemáticas de SIG, de segurança da informação e segurança cibernética. Em função dessa meta, que é prevista para 2015, já fizemos uma articulação com vários setores e conseguimos inserir questões de SIC em quatro programas junto a quatro Ministérios: o Programa Defesa Nacional, que é um programa do Ministério da Defesa; o Programa Democracia e Aperfeiçoamento da Gestão Pública, que é um programa do Ministério do Planejamento; o Programa Ciência, Tecnologia e Inovação, do MCTI; e o

Programa de Relações Exteriores, que é do Itamaraty. Também nesses quatro programas já conseguimos, com a colaboração, com a participação e autorização do Ministério do Planejamento, inserir ações de SIC nesses planejamentos estratégicos desses órgãos, que já foi aprovado e já está em vigor.

A Meta IV eu também destaco, que foi articular e formalizar uma função orçamentária. Era uma aspiração do Comitê e de vários membros do Comitê de que isso fosse obtido, mas já evoluiu. Estivemos participando de algumas reuniões com a SOF, do Ministério do Planejamento. Eles se prontificaram a fazer uma apresentação, que foi feita para o Comitê Gestor de Segurança, trazendo uma solução alternativa, que é a criação de um Plano Orçamentário Reservado de SIC e Segurança Cibernética para toda a APF. Já foi criado também um Grupo de Trabalho no Comitê Gestor para se aprofundar mais nesse tema — é um pessoal mais especializado na área financeira — e possivelmente implementar essa sugestão que partiu da SOF, que, segundo palavras da SOF, foi também uma solução adotada no próprio âmbito do Tribunal de Contas da União. Também foi uma solução adotada por eles lá nessas questões de segurança da informação.

Não sei como vai meu tempo. Já esgotei? É o penúltimo eslaide. Já estou acabando.

Ali eu destaco apenas os principais fatores daquilo que eu falei, resumindo o que precisa ser feito em termos de segurança da informação para toda a APF. Os fatores críticos de sucesso seriam a priorização na agenda de Governo e sensibilização nacional. É algo que nós temos tentado fazer juntamente com a..., pela nossa coordenação de gestão e com a colaboração do comitê gestor. Recrutamento, fixação e capacitação de profissionais — nós temos capacitado lá. Já foram 300 gestores formados, mas nem todos continuam trabalhando nas suas áreas de atuação. Então, é algo que a gente precisa realmente trabalhar em cima. Há necessidade de uma política nacional. Já publicamos a estratégia de segurança cibernética e segurança da informação. Já estamos estudando a possibilidade de levar à CREDEN a possibilidade de aprovação de uma política nacional de segurança da informação. Parcerias com operação e participação social são ações que foram intensificadas agora com a publicação da estratégia. A participação social, por intermédio da Câmara setorial, vai ser muito incrementada. A

coordenação executiva do órgão central com a publicação agora da estratégia eu também acredito que deva ganhar força e vai ser intensificada e centralizada essa coordenação. A questão orçamentária é fundamental, mas também já foi atendida em parte pela..., uma das metas da nossa estratégia que já está em andamento.

Meus senhores, finalizando, eu projeto ali apenas a nossa visão de futuro do Departamento de Segurança da Informação. É uma atividade que nós temos realizado. Como o próprio TCU já comentou, muito foi feito, mas muito ainda tem que se fazer. Nós dependemos de retorno dos Ministérios, de todos os órgãos e entidades da APF para o cumprimento dessas normas.

O próximo eslaide finaliza.

Eu agradeço a atenção e a paciência de todos e coloco-me à disposição para alguma pergunta.

Muito obrigado.

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

Concedo a palavra ao Sr. Otávio Carlos Cunha da Silva, Diretor do Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações.

O SR. OTÁVIO CARLOS CUNHA DA SILVA - Bom dia.

Em primeiro lugar, eu gostaria de agradecer o convite formulado à ABIN para nós podermos fazer essa apresentação.

Eu queria agradecer à Sra. Deputada Mariana Carvalho e a todos os Deputados presentes.

Senhores ouvintes, gostaria muito de repetir uma coisa que eu venho falando há algum tempo. Eu diria que essa questão de segurança da informação, hoje em dia, com o novo *hype* que tem agora, chamado cibernética — todo mundo fala isso —, é 60% de pessoas, 20% de tecnologia e 20% de perseverança. Nós precisamos ter muita perseverança. No meu caso, eu venho trabalhando há alguns 30 anos nessa área, desde 1982, quando nós criamos esse Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações, CEPESC, subordinado à ABIN na estrutura do GSI. Desde 1982 nós desenvolvemos soluções, àquela época, para a segurança das comunicações para a administração pública federal, principalmente para os órgãos que detêm as informações e tratam delas com informações classificadas.

No âmbito dessa evolução que eu venho percebendo, desde 1982 até os dias de hoje, a questão de crimes cibernéticos insere-se de uma maneira muito rápida, o que causa uma série de problemas de adaptação das instituições, adaptação da população e, principalmente, adaptação da legislação. É necessário mais legislação, mais ensino. Eu acredito que, com a legislação que nós expomos hoje, com algumas, digamos, melhorias ou acertos e com muito mais educação, nós temos condição de diminuir esse fosso que existe entre a população, os usuários normais, e os criminosos, porque eles vivem disso. E a população precisa da Internet.

Quando eu falo em comunicações, incluo desde a época do telex, a época do teletipo — que poucos aqui devem ter usado — até os dias de hoje. Nós estamos falando em Voz sobre IP, com todos nós estamos conectados, no mínimo, a um ou dois celulares, *tablets*, computadores. A situação tem evoluído para a seguinte questão: no que vamos dar segurança, em tecnologia, no usuário final ou na conjunção dos dois? Isso é muito difícil, mas não apenas no Brasil, é difícil no mundo inteiro. Esse não é um problema específico nosso, é um problema que atinge todos os países do mundo.

Então, a nossa *expertise* desde o início foi desenvolver criptografia e soluções em segurança da informação e das comunicações. Criptografia hoje se tornou uma palavra — acho até ótimo — bem comum, todos falam sobre criptografia. E realmente, quanto mais as pessoas entenderem o que vem a ser criptografia melhor, principalmente em termos do usuário comum.

Graças a Deus, nós temos no Brasil um centro que trabalha com isso. No mundo, nós podemos contar, em média, 10 a 15 países que detêm essa capacidade de desenvolver sua própria criptografia, a criptografia que hoje colocamos como sendo criptografia de Estado. Toda a legislação tem nos amparado, principalmente a LAI e os outros decretos que vieram em função dela.

Mas não adianta desenvolver a melhor criptografia, não adianta desenvolver a melhor solução para a segurança de informação e cibernética, se não conseguirmos fazer com que isso permeie a sociedade e chegue ao usuário final.

Eu estive ontem com dois representantes da Microsoft, que me passaram uma apresentação muito interessante. Eles estão tratando, na sua área de crime cibernético, do que eles chamam de proteção às pessoas que são tidas como se

fossem inocentes. Quem são os inocentes nisso? Somos todos nós que não temos um nível de conhecimento tecnológico para entender as ameaças que realmente estão por trás de cada Internet Banking, de cada página que é enviada por *e-mail*, de cada clique que damos numa imagem. Essas são as grandes ameaças.

A população faz isso de maneira natural, não está preocupada. Quando você vai fazer o *download* de um determinado programa, você sempre clica em *Yes* e não lê nada. Agora mesmo, sobre o *update* do IOS 9.1, que é necessário — e quem tiver equipamento da Apple, por favor, faça isso o mais rápido possível —, uma vulnerabilidade muito séria foi descoberta, por isso o IOS está sendo colocado à disposição desde ontem. Então, as pessoas sempre clicam em *Yes, Yes, Yes* e *Agree*.

Numa apresentação em que eu tinha um tempo mais extenso, eu abri o *disclaimer* de uma dessas empresas que fornecem *softwares.* Ali dentro estava dizendo o seguinte — isto é uma tradução minha*: "Nós da Microsoft comemos no almoço maçã e jantamos maçã. E nem todo mundo gosta de maçã. Mas, tudo isso, comemos maçã".* Acreditam os senhores e senhoras que isso faz parte de um *disclaimer* sério? Pois todo mundo clicou em *Agree*, todo mundo foi lá e disse que concordava.

Com relação a esses detalhes, nós usuários ficamos pensando assim: "*Será que isso é verdade?"* Mas é verdade, porque estava escrito. Você clica em *Agree*, mas não sabe com o que está cooperando, para o que está clicando *Agree*. Quando você está numa conta de Internet Banking, quando você coloca determinado dispositivo de um banco na sua máquina, você sabe exatamente o que aquele dispositivo está fazendo dentro da sua máquina?

Então, é com esses detalhes que ficamos preocupados, nós que trabalhamos na área técnica e temos a responsabilidade de desenvolver soluções de segurança para o Governo Federal e algumas outras organizações fora do Poder Executivo. E por mais que desenvolvamos soluções de altíssimo nível de segurança, não há como fazer com o que o usuário seja inteligente o suficiente ou tenha certa maldade. Normalmente o usuário é inocente: se ele tem um problema a resolver, vai apertar o botão que for preciso para resolvê-lo. Ele tem seu o *token* e tem a sua senha, porque é uma questão de dupla autenticação, e vai fazer isso de maneira natural,

porque tem necessidade de pagar a conta, ou de ver o seu saldo, ou de transferir dinheiro. E quando ele abre o *e-mail*, quem lhe diria que vem um determinado *phishing?*

Todos os senhores sabem, a grande maioria hoje sabe o que é *phishing*, de tanto que se fala em *phishing*, que são aquelas mensagens enganosas. Anteontem eu recebi de um amigo — nessa área nós temos uma rede colaborativa muito forte — um *phishing* de determinada empresa de telecomunicações dizendo*: "Você, cliente Fulano de Tal, que está com o seu plano assim, assim e assim, por favor, clique aqui para ganhar um upgrade imediato do seu plano".* Mas no momento em que a pessoa clica, todas as suas informações estão sendo roubadas pelo crime.

Por falar em crime, eu estive aqui na terça-feira e achei excelente a apresentação do pessoal da criminalística. Eles partem de um pressuposto e nós partimos de outro. Eu brinco muito — é uma forma de dizer — dizendo que eles trabalham depois de o crime ter acontecido, eles tentam fazer a prevenção, o que é muito difícil. Nós trabalhamos ao contrário: nós no CEPESC e na ABIN tentamos incutir na cabeça de todos os usuários a importância de se proteger, de se precaver. Nós temos que ter uma ação proativa. Não adianta reclamar só depois que há um morto. Eu não quero me transformar num IML, eu não quero trabalhar com cadáveres, eu quero trabalhar com uma pessoa que tenha problema, para ela não cair na rede do crime.

Com eu disse, o pessoal do crime não tem a Lei 8.666, não tem a IN 04, não tem uma série de restrições. E nós todos, como servidores públicos federais, temos que atender a todas essas regulamentações, o que impacta o desenvolvimento. E qual seria o desenvolvimento ideal para todo pessoal que trabalha na área de pesquisa e desenvolvimento? *"Olha, eu quero liberdade. Eu não preciso de muito dinheiro, eu preciso de gente, gente e gente. Eu preciso de cabeça, eu preciso de cérebros."* Quando me perguntam quanto dinheiro eu quero, eu digo: *"Não, me perguntem quantas pessoas eu quero. Em vez de me perguntar de qual orçamento preciso, pergunte qual é o meu problema".* E o grande problema que hoje nós encontramos é que o usuário não tem ainda uma visão clara do problema dele, ele só vai ter isso depois que se tornou mais um número na linha de estatística mundial.

Dentro do CEPESC, nós desenvolvemos uma série de recursos criptográficos, que são utilizados pelos que nós chamamos de nossos clientes não prioritários, mas que realmente têm uma necessidade muito grande de trabalhar com informação classificada. Seriam eles a Presidência da República, obviamente a própria ABIN, o GSI, as Forças Armadas, o Ministério das Relações Exteriores.

E fora do âmbito do Executivo Federal, há o Tribunal Superior Eleitoral, para quem, há 17 ou 18 anos, desenvolvemos criptografia e damos apoio no processo eleitoral. Quero deixar bem claro que o nosso sistema é para proteger transferência de boletins de urna. Nós nos atemos apenas à questão da segurança da comunicação entre todo ponto de eleição, todo tribunal regional e o Tribunal Superior Eleitoral. Nós não trabalhamos na contabilização, porque há todo um processo muito bem separado e muito bem, como dissemos, compartimentado, para evitar que todos tenham conhecimento de tudo. Então, se eu não tenho necessidade de conhecer alguns processos, eu não entro nesse processo.

Além dessas soluções, nós fornecemos também soluções e apoio aos grandes eventos. Nós participamos desde o pré-início dos Jogos Pan-Americanos, apoiando o Ministério do Esporte durante a realização dos Jogos Pan-Americanos e na implementação de todas as redes. Nós ficamos, digamos assim, quase como assessores do Ministério do Esporte com relação à segurança de comunicações e de rede de todos os eventos ocorridos nos Jogos Pan-Americanos. Foi a mesma coisa na Rio+20, na Copa das Confederações e na Copa do Mundo. E agora nós já estamos trabalhando com o pessoal do Rio 2016, para as Olimpíadas.

Eu não sei quantos dos senhores e das senhoras aqui presentes têm noção da complexidade de um grande evento, principalmente Olimpíadas. Não é uma coisa trivial. Eu acredito que, no período dos Jogos Olímpicos de 2016, nós vamos ter um grande volume de ataques e de crimes, na tentativa de usar cartões de crédito de usuários de outros países, roubar senhas, implementar *phishings*. Isso vai crescer num volume muito expressivo. Então, nós temos que nos preparar e antecipar as proteções que iremos oferecer a todos esses usuários que são — entre aspas — "inocentes", estão aqui apenas para fazer turismo e assistir aos Jogos Pan-Americanos.

Então, a segurança entra com um perfil baixo, quer dizer, ela não tem que ser impeditiva do uso da tecnologia. Mas ao mesmo tempo, não se pode, de maneira nenhuma, colocar da seguinte forma: "*Não, se nada mais deu certo, tira a segurança e vamos tentar nos comunicar"*. Existem casos e mais casos em que nós trabalhamos durante esses grandes eventos, pois são inúmeros. Crimes são perpetrados antes, durante e depois dos eventos. Há páginas que sofreram pichação durante o evento da Rio+20 e continuaram sem conserto por, pelo menos, 18 meses. E nós insistentemente dizíamos: *"Por favor, consertem esse erro na sua página, porque isso vai gerar um problema muito sério e vai ocasionar problemas de crimes que vão acontecer, querendo vocês ou não".*

Então, a nossa ideia aqui é passar para os senhores que existe um centro que há 30 anos se dedica a executar esses desenvolvimentos. Nós, com muito orgulho, detemos essa criptografia nacional. Eu ouvi muito falarem de criptografia na terça-feira. Eu fico muito satisfeito em ouvir as pessoas dizerem que estão quebrando criptografia. E ao mesmo tempo, estou tranquilo porque, na nossa área, quem quebra não fala, quem quebra não diz que quebrou, quem quebra continua usando quebrada. Então esse é o grande pulo do gato para a área profissional que trabalha com criptografia.

O FBI hoje tem um problema muito sério, porque Google, Facebook, WhatsApp, todos esses aplicativos estão empregando agora criptografia nas suas comunicações. E a grande questão é: como eu faço para usar uma prova de crime sem abrir a criptografia, porque o direito de abrir é nenhum, não há uma legislação que obrigue a isso.

Eu estive participando de uma conferência agora nos Estados Unidos, chamada Black Hat, em que cinco painéis estavam tratando, em dias diferentes, da questão de venda de *softwares* para outros países. Essa venda de *softwares* seria a parte ofensiva da cibernética, o que não é o nosso caso, pois só trabalhamos na parte defensiva e de suporte. Mas a grande questão é: eu, do Brasil, não posso mais comprar algumas ferramentas que são vendidas no mercado americano, se não for autorizado pelo Departamento de Comércio e pelo Departamento de Estado dos Estados Unidos. Isso significa — é uma questão muito séria — que eles vão bloquear a possibilidade de alguns países terem acesso a esses *softwares.* Para

trabalhar em defesa, é preciso saber como se vai ser atacado. Mas com isso, não se sabe o nível de ataque que pode sofrer, então, não se pode construir soluções para se defender desses ataques. Isso está sendo feito de maneira muito clara e bem discutida dentro do mercado americano, voltando à época de 1978 ou 1979, quando a comercialização de criptografia no mundo era toda controlada e restringida pelo Governo americano.

Os senhores vejam o quanto isso é sensível e o quanto isso influi, não no resultado final do crime, mas na prevenção do crime. E eu acho que a grande solução para crime cibernético é trabalhar na prevenção. Depois que já aconteceu o crime, o máximo que vamos conseguir é ir atrás dos criminosos e tentar desvendar esse emaranhado de problemas. Então, a minha sugestão seria: vamos trabalhar na prevenção. E nós nesse Centro temos trabalhado na segurança das comunicações, nas segurança cibernética esse tempo todo.

Eu vi já passei 23 segundos do meu tempo e não gostaria de usar o tempo de mais ninguém. Mas coloco-me à disposição dos senhores para qualquer questão que for necessária.

Muito obrigado.

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

Concedo a palavra ao Coronel Paulo Roberto de Araújo Castro Vianna, Chefe da Divisão de Operações, do Centro de Defesa Cibernética do Exército.

O SR. PAULO ROBERTO DE ARAÚJO CASTRO VIANNA - Exma. Sra. Deputada Mariana Carvalho, em nome de quem eu cumprimento os demais integrantes da Mesa, Srs. Deputados, senhoras e senhores aqui presentes, em nome do Chefe do Centro de Defesa Cibernética, General Carvalho, que não pôde estar presente, tendo em vista outros compromissos assumidos, eu agradeço o convite da Comissão.

Pretendo apresentar aqui, de forma breve, o nosso trabalho no Centro, já que imagino que o Centro de Defesa Cibernética é uma organização não conhecida por boa parte dos senhores aqui. Então, a minha intenção é fazer uma breve exposição sobre o nosso trabalho, para que possamos identificar a nossa colaboração nessa temática de crimes cibernéticos.

Vou solicitar a permissão para fazer a apresentação em pé, para que eu possa ver os eslaides.

(Segue-se exibição de imagens.)

Este primeiro eslaide mostra algumas atividades do nosso Centro. A nossa preocupação sempre é voltada para a capacitação. Então, corroborando o que já foi falado aqui pelo Sr. Otávio, da ABIN, nós imaginamos que não basta apenas a tecnologia, nós temos que investir nos nossos talentos, nos nossos recursos humanos.

Aqui vemos os documentos norteadores da defesa nacional: nós temos a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional. Eu faço aqui um destaque para a Estratégia Nacional de Defesa, documento emitido em 2008, que destacou o setor cibernético como sendo um dos três de grande importância, juntamente com o espacial e o nuclear, e designou esse setor para o Exército Brasileiro.

Então, conforme eu havia falado, a Estratégia Nacional de Defesa definiu que o setor nuclear ficaria a cargo da Marinha do Brasil; o setor cibernético, a cargo do Exército Brasileiro; e o setor espacial, a cargo da Aeronáutica. O nosso Centro de Defesa Cibernética nasceu em 2010, fruto da Estratégia Nacional de Defesa de 2008, que estabeleceu a priorização para o setor cibernético e definiu que ele deveria ser estruturado no âmbito do Exército. O Centro foi criado como núcleo em 2010 e posteriormente, em 2012, passou a ser uma organização militar dentro do Comando do Exército.

Dentro da Estratégia Nacional de Defesa, nós podemos resumir algumas ideias-forças. A Estratégia fala nas Forças Armadas com capacidade para atuar em rede; na segurança contra ataques cibernéticos; e por fim, na busca de iniciativas conjuntas entre Forças Armadas, Academia e empresas brasileiras. Aqui eu destaco que isso é o nosso farol, é a nossa intenção o tempo todo. Sempre vislumbramos que esse papel não deve ser apenas das Forças Armadas, que nós precisamos interagir, precisamos da cooperação da Academia e das empresas na busca dessa defesa cibernética. E por fim, os equipamentos, as tecnologias geradas devem ter uma utilidade dual, não somente para o meio militar, mas também para o meio civil.

Ainda dentro da ideia de resumo estratégico, esta figura simboliza um átomo, em cujo núcleo estão os talentos humanos. Como eu falei, nós investimos muito nos talentos humanos, na capacidade dos recursos humanos, para que possamos atingir o nosso objetivo, cumprir a nossa missão. Como elétrons desse átomo, estão a inteligência, a parte de doutrina, a parte de operações e também a parte de ciência, tecnologia e inovação. Emoldurando essa figura, estão a segurança da informação e as comunicações, já tratadas aqui pelo General Marconni, a mobilização da capacidade cibernética e também o amparo legal para o emprego cibernético.

Neste eslaide vemos a missão do Centro: coordenar e integrar são os verbos que definem as nossas atividades de defesa cibernética. Posteriormente eu vou fazer uma diferenciação entre os termos “segurança” e “defesa”, mostrando como nós encaramos isso no âmbito do Ministério da Defesa. Então, a missão do Centro é coordenar e integrar as atividades de defesa cibernética no âmbito do Ministério da Defesa, consoante com o disposto no decreto que aprovou a Estratégia Nacional de Defesa. O nosso trabalho é simbolizado por essa coordenação e integração de todos os entes que estão envolvidos no âmbito da defesa. E destaco que o Centro atua no âmbito da defesa do Ministério da Defesa.

A nossa competência é recente, já que nossa subordinação foi mudada dentro do próprio Comando da Força e passamos a ser um órgão de assessoramento direto e imediato do Comandante da Força. Então, temos que assessorar o Comandante do Exército e o próprio Ministro de Estado da Defesa nas atividades do setor, formulando doutrina e obtendo e empregando tecnologias; planejar, orientar e controlar as atividades operacionais, doutrinárias, para desenvolver essas capacidades cibernéticas; e, por fim, executar atividades de exploração cibernética, em conformidade com as políticas e diretrizes do Ministério da Defesa.

Esta figura ilustra o que eu havia falado anteriormente sobre o que nós consideramos segurança, defesa e guerra cibernética. Então, dentro da doutrina estabelecida nas Forças Armadas sobre a defesa, nós chamamos de segurança cibernética quando estamos no nível político, que é o nível mais elevado, como o General Marconni tratou muito bem aqui. Ele está no nível da Presidência da República e dos gabinetes de segurança institucional. Quando falamos em defesa

cibernética, estamos no nível estratégico. Esse nível é tratado pelo Ministério da Defesa, sendo que o Centro é o responsável por conduzir essa defesa cibernética. E quando falamos em guerra cibernética, estamos no nível operacional e no nível tático, que são estabelecidos por ocasião de exercício ou mesmo em situação de crise, quando há um comando operacional, e mesmo nas Forças componentes, a Marinha do Brasil, o Exército e a Aeronáutica. É apenas uma questão de definição de termos. Nós encaramos dessa forma e usamos esses termos de forma diferenciada.

Dentro daquela ideia de desenvolver capacidades e na preocupação de ligação com outros setores que cuidam do setor cibernético no próprio País, nós, há alguns anos, vimos estabelecendo algumas parcerias com o Ministério da Ciência e Tecnologia e Inovação em algumas áreas temáticas. Este eslaide mostra algumas áreas temáticas que vieram sendo discutidas por mais 3 ou 4 anos, desde que o Centro foi criado, e que hoje já frutificaram.

Mais no alto, ali à esquerda, está a Escola Nacional de Defesa Cibernética — ENaDCiber, que foi criada este ano e por enquanto é somente um núcleo, com a intenção de capacitar e formar talentos humanos nessa área. Vislumbramos que essa Escola, mesmo estando dentro da organização do Comando do Exército, deve ter a participação de todos, dos civis principalmente, não deve ser somente de militares.

À direita está outra área sobre a qual nós também já temos alguma coisa no nosso Instituto Militar de Engenharia, a computação de alto desempenho voltada para a defesa cibernética.

Aqui em baixo, está a segurança em ambientes computacionais. Também estamos procurando, nessa cooperação com o MCTI, desenvolver produtos nessa área de segurança de ambientes, como *firewalls*, antivírus e computação em nuvem, para que possamos ter produtos nacionais em que possamos confiar, sem ter aquela preocupação constante de que aquele produto, por ser estrangeiro, não é confiável.

Por fim, à esquerda e embaixo, está o Sistema Modular de Defesa Cibernética, que é planejado para utilizarmos nas nossas operações nos grandes eventos de que vimos participando, nos quais podemos desdobrar equipamentos e

equipes para atuar numa certa operação ou num certo ambiente, visando à proteção daquelas redes daquele ambiente.

A portaria do final do ano passado foi voltada para aquela temática de segurança de ambientes computacionais mostrada no eslaide anterior. E a parceria entre o MD e o MCTI busca isto: o fomento de soluções nacionais em defesa cibernética; a criação de laboratórios de análise de programas maliciosos; e a gestão técnica, negocial e de governança desses outros dois. Esse é um projeto que já está acontecendo desde o final do ano passado, no qual nós estamos em parceria com o MCTI.

O Programa de Defesa Cibernética na Defesa Nacional é outro que também foi criado recentemente, no final do ano passado, quando se criaram algumas estruturas de muita importância. Eu até já falei de uma delas, que é a segunda que está ali, a Escola Nacional de Defesa Cibernética.

Antes da Escola Nacional de Defesa Cibernética, aparece a figura do Comando de Defesa Cibernética, que por enquanto está somente na condição de núcleo, mas posteriormente vai aumentar a sua capacidade. O Comando foi criado com a intenção de absorver todas essas estruturas, inclusive o próprio Centro. Então, a previsão é que o Centro de Defesa Cibernética passe a ser uma estrutura desse Comando, que englobará a Escola Nacional; um sistema de homologação e certificação, para que possamos homologar e certificar produtos e serviços nessa área; um programa para desenvolver essa temática nas Forças armadas; o Observatório de Defesa Cibernética; e o apoio à pesquisa e desenvolvimento de projetos de defesa cibernética.

Finalizando a minha apresentação, nós vemos a atuação do Centro em grandes eventos. Desde que o Centro foi criado em 2010 e se definiu como organização militar em 2012, nós vimos participando dos grandes eventos, envolvidos não só com a defesa, mas também com a segurança. Por ocasião dos grandes eventos, o Centro recebe a incumbência de também coordenar os trabalhos de segurança cibernética. Então, nós passa a ter uma incumbência maior. Nós contamos com o apoio do Gabinete de Segurança Institucional, da DSIC e de todos os demais órgãos e entes desse setor cibernético, e passamos a coordenar os trabalhos. Assim foi na Rio+20, assim foi na Copa das Confederações, na visita do

Papa, na Jornada Mundial da Juventude, na Copa do Mundo, e assim será no próximo grande evento, as Olimpíadas no Rio de Janeiro.

A nossa missão nos Jogos Olímpicos vai ser coordenar e integrar, em ambiente interagências, as ações de segurança e defesa cibernética contra ações cibernéticas hostis, na garantia da segurança dos Jogos Olímpicos Rio 2016.

Eu destaco mais uma vez que o sucesso que temos tido nesses grandes eventos — e certamente teremos nesse próximo grande evento — decorre principalmente pela atuação colaborativa. Sozinhos, nós jamais teríamos conseguido alcançar a nossa meta, o nosso objetivo. Então, o trabalho se dá por meio desta ação colaborativa: diversos entes envolvidos na segurança cibernética ou na defesa do setor cibernético colaboram, e nós conduzimos, então, a coordenação.

Finalizando, nós temos como desafio a capacitação e o aperfeiçoamento dos nossos recursos, para realizar ações cibernéticas eficientes, eficazes e efetivas, com ampla atuação interagências e com foco na sensibilização e conscientização da sociedade para a importância da segurança e defesa cibernéticas.

Eu volto a destacar as palavras do Diretor do DSIC sobre a importância de conscientizar a sociedade dessa temática do crime cibernético. Srs. Deputados, eu acho que é muito importante conscientizar a nossa sociedade dessa temática, o simples usuário do *tablet*, do *smartphone*, de qualquer dispositivo eletrônico tem que ter consciência. Conforme o Sr. Otávio falou, isso se trata muito mais de pessoas do que de equipamentos. Então, nós temos essa preocupação.

Algumas palavras-chaves: inovação, segurança da informação e comunicações, segurança e defesa cibernéticas, capacitação, coordenação, integração, confiança e colaboração.

Nesse trabalho que fazemos ao longo dos grandes eventos, percebemos que confiança é fundamental. Se eu não consigo a confiança daquele ente, como a que hoje nós temos com relação ao DSIC e à ABIN, eu não vou conseguir trabalhar com ele. Quando nós passamos a confiar um no outro, nós passamos a ter um rendimento muito maior.

Esta figura ilustra a atuação do Centro dentro desse papel colaborativo. Diversos entes estão aí representados, sendo que é o trabalho de todos eles que leva ao sucesso do nosso trabalho. Aí estão listados o Ministério da Defesa, através

do Estado-Maior Conjunto; as Forças; a Polícia Federal, com a Seção de Repressão aos Crimes Cibernéticos; o SERPRO; o Ministério das Relações Exteriores; a ABIN; o Gabinete de Segurança Institucional; a ANATEL; empresas da área de tecnologia da informação e comunicações; infraestruturas críticas, tais como Itaipu; o Ministério da Ciência, Tecnologia e Inovação; o meio acadêmico, através das diversas universidades que estão à direita. Em destaque ali à direita, estão o NIC.br, o CGI.br e o CERT.br. É o Comitê Gestor da Internet, através do CERT, que gerencia a Internet no nosso País.

Portanto, esta é a principal atribuição nossa: o trabalho de coordenação de todos esses entes, em particular durante os grandes eventos. E no dia a dia, eu destaco que o Centro cuida da defesa e atua no âmbito do Ministério da Defesa.

Agradeço a atenção.

Muito obrigado.

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

Encerradas as apresentações, vamos fazer apenas um bloco de perguntas e depois passar para as respostas.

Com a palavra o Deputado Leo de Brito.

O SR. DEPUTADO LEO DE BRITO - Sra. Presidente Mariana Carvalho, eu gostaria de saudar todos os Deputados e Deputadas aqui presentes e também os nossos expositores, agradecendo-lhes pela importante contribuição para esta Comissão.

Eu tenho algumas perguntas a fazer para os nossos expositores. Primeiro indagarei o Sr. Marconni dos Reis Bezerras, do GSI, a respeito do caso NSA. Como foi tratada essa situação no âmbito do Gabinete de Segurança Institucional? Como vocês descobriram? Quais providências foram tomadas? Houve algum tipo de falha relacionada a esse caso?

Dr. Otávio, nós temos feito um debate importante sobretudo a respeito dos aspectos preventivos relacionados aos crimes, uma vez que as estatísticas e as exposições de várias pessoas que vieram aqui mostram que a prática de crimes na Internet é algo, digamos, epidêmico. Qual é a sua opinião a respeito da utilização de *softwares* livres no sentido de prevenir crimes cibernéticos? Esse é um ponto. E pegando um pouco da sua experiência na área, qual o seu conceito a respeito do

que é um crime cibernético? Essa também foi uma dúvida que surgiu logo no início da nossa CPI. Acho que é uma coisa importante. Qual o seu conceito a respeito do que é um crime cibernético? Eu acho que isso é uma coisa importante aqui.

Outro aspecto que tem sido muito debatido aqui na Comissão é a respeito da questão da individualização do IP, do ponto de vista da segurança, da prevenção dos crimes cibernéticos e também para descobrir os crimes cibernéticos. É correto dizer que a utilização do IPv6, que também já foi tratado em outras audiências aqui, em conjunto com a criptografia e a utilização de assinaturas digitais podem garantir a segurança necessária para evitar ou diminuir os riscos de crimes cibernéticos, principalmente no ambiente do setor público? É outra questão.

Eu vejo que também os órgãos estão envolvidos e gostaria de que também V.Sa. se aprofundasse a respeito dos preparativos. Como é que estão os preparativos, do ponto de vista da segurança, em relação às Olimpíadas? Seria esse mais um ponto.

E, no caso do Coronel Paulo Roberto, a pergunta que eu tenho é a seguinte: se já identificaram no Exército alguma tentativa — o senhor falou sobre guerra cibernética — de ataque no caso de situações relacionadas intimamente à questão da Defesa Nacional, até mesmo de Estados; se outros Estados, por exemplo, se utilizaram de algum mecanismo de ataque à Defesa Nacional relacionado à questão cibernética.

A outra questão é se existe alguma estatística de crimes ou tentativa de cometimentos desses crimes, e se podemos estar tranquilos em relação à nossa segurança institucional, inclusive se as ferramentas que estão disponíveis são, digamos assim, suficientes para garantir essa segurança institucional.

São várias perguntas. Teria até mais algumas, mas vamos priorizar os demais Deputados que também vão fazer outras perguntas.

Muito obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Com a palavra o Deputado Silas Freire.

O SR. DEPUTADO SILAS FREIRE - Deputada Mariana Carvalho, Sra. Presidente; demais Deputados; senhores convidados, expositores, eu gostaria de fazer uma pergunta à Mesa, para quem puder nos responder depois. Eu vou ter

dificuldade de continuar presente e vou ter que pedir aqui a fita da nossa audiência pública.

Eu queria perguntar sobre o mundo sombrio do *deep web*, que é o chamado esgoto da Internet. Nós não temos qualquer controle disso. Nós sabemos que, no *deep web*, hoje, assassinatos, sequestros e crimes são combinados e acontecem. Aqui é a Internet, para os senhores entenderem, e aqui embaixo é o esgoto, que está no subterrâneo e se chama *deep web*. Estão usando agora um aplicativo, que podemos chamar de *software*, o Tor, que justamente dificulta a identificação. E a pergunta vai se sugerir em cima tanto do *deep web* como do Tor.

Eu vou fazer alguns levantamentos e, se eu não puder ficar, porque tenho que registrar presença, vou depois pegar a resposta. O que é o *deep web?* É bom que a Comissão saiba e quem puder responder da Mesa, muito bem. É legal? Pergunta dois: qual é a realidade do *deep web* no Brasil? Como podemos nos proteger desse esgoto da Internet? Sobre o programa Tor: o programa usado para ter acesso ao *deep web* e para uma proteção. Só para simbolizar a gravidade, se eu estiver com o programa Tor instalado, eu vou enviar uma conversa à Deputada Mariana Carvalho. Essa conversa passará por vários computadores, a fim de que os senhores não identifiquem os terminais que estão conversando. Isso é muito grave, muito grave! Não há identificação! Está sendo usado por grandes potências militares, os senhores sabem, por jornalistas, por espiões. Por isso, nós temos interesse de saber como o Brasil está lidando com isso.

E a outra pergunta já é específica ao Dr. Otávio Carlos, que disse que esteve com a Microsoft agora numa reunião. Nós queremos saber sobre o programa PhotoDNA, a gente quer saber se é usado pela Polícia no combate, por exemplo, ao crime de pedofilia, certo? E se nessa reunião o senhor chegou a discutir com a Microsoft também sobre o PhotoDNA, está certo?

São essas as nossas colocações, muito obrigado.

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

Concedo a palavra ao Deputado Celso Jacob.

O SR. DEPUTADO CELSO JACOB - Sra. Presidente, senhores participantes, numa parte, eu fui contemplado, e noutra parte, não. Então, para não ficar repetitivo

e fazer as mesmas perguntas, eu vou focar numa coisa que o Sr. Otávio falou: ataque e defesa.

O que nós estamos desenvolvendo para esses ataques? O ataque é de vários tipos, como o das redes sociais mencionado pelo senhor. E acho que falta da nossa parte um programa educacional de esclarecimento à população. Todo mundo tem acesso hoje a celular, às redes sociais; um computador comum é vendido facilmente, divide-se em dez vezes e se compra. E as pessoas não têm acesso à informação de como utilizá-lo, esse é o grande erro nosso. Nós estamos distribuindo isso e as pessoas têm acesso, não sabem, muito mal sabem mexer e saem abrindo *e-mail* de tudo quanto é tipo e criando uma confusão geral. E a gente não está conseguindo trabalhar essa parte educacional, de informação. Eu acho que todo mundo que recebesse um computador tinha que receber as informações dizendo o seguinte: *"Olha, cuidado com isso, cuidado com aquilo, previna-se disso..."*, porque isso iria resolver muita coisa no sentido geral.

Agora, há esses ataques mais graves, como falou o nosso colega aqui, esses tipos de ataques perigosos que podem comprometer nossa segurança nacional, comprometer programas sérios, programas de bancos, mais institucionais. O que nós estamos fazendo para combater isso? São dois pontos. Que se fale de uma forma técnica bem popular, para que nós possamos entender isso. O popular tem que ser urgente, para ontem, tem que haver esses projetos de esclarecimento educacional, de como utilizar rede, de como utilizar celular.

E o outro: o que nós estamos fazendo em relação a esses grandes ataques que podem pôr em risco a nossa segurança?

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Deputado Celso Jacob.

Concedo a palavra ao Deputado Daniel Coelho, Sub-Relator desta Comissão.

O SR. DEPUTADO DANIEL COELHO - Obrigado, Sra. Presidente.

Queria aqui fazer algumas perguntas aos três debatedores. Inicialmente, ao Sr. Marconni, queria perguntar como se dá a atuação do centro de tratamento e de resposta aos incidentes ocorridos nas redes de computadores da administração pública federal e se cabem ao trabalho que V.Sa. realiza também os abusos cometidos dentro das redes por servidores do Governo Federal.

Nós acompanhamos casos, como os que aconteceram com os jornalistas Míriam Leitão e Carlos Alberto Sardenberg, que tiveram o seu Wikipédia modificado por computadores que fazem parte da rede do próprio Governo. Então, quero saber se essa ação faz a defesa do sistema da rede, mas também se ela atua nos possíveis abusos cometidos por servidores ou usuários da própria rede.

Também quero perguntar se compete ao Departamento de Segurança da Informação e Comunicação — DSIC, do GSI — Gabinete de Segurança Institucional, avaliar tratados, acordos ou atos internacionais relacionados à segurança da informação e comunicações. Considerando isso, eu pergunto a V.Sa. se o órgão avaliou a adesão do Brasil à Convenção de Budapeste, que disciplina a troca de informações sobre crimes cibernéticos entre os Estados membros, se há estudos nesse sentido e quais os obstáculos para a efetiva adesão do Brasil ao instrumento.

Queria perguntar ao Sr. Otávio Carlos Cunha da Silva: segundo consta do sítio do Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações — CEPESC, na Internet, à ABIN, por intermédio do órgão, compete a criação e implementação, em *software* básico, de modos criptográficos destinados a proteger o transporte dos resultados eleitorais entre as urnas e os computadores totalizadores; autenticar e validar digitalmente os arquivos, códigos e programas executáveis da urna eletrônica e do sistema de voto; bem como implementar e executar os protocolos de estabelecimento e gerenciamento das chaves criptográficas.

Diante disso, eu indago a V.Sa. se o programa de desenvolvimento pelo CEPESC é entregue e compilado ou se ele é aberto ao Tribunal Superior Eleitoral, TSE. Ao entregar o programa do TSE, são encaminhadas as chaves para o acesso do *software* de forma que se possa proceder à ampla análise dos comandos nele existentes? Então, eu peço a V.Sa. que responda isso. Se não tiver a informação de pronto, peço buscá-la até o fim da audiência e fornecê-la à Presidência, o que será de grande valia.

Também pergunto ao Coronel Paulo Roberto de Araújo Castro Vianna: quais são, na opinião de V.Sa., os principais desafios para implementação de um sistema efetivo de segurança e de defesa cibernética no Brasil? Também pergunto ao

Coronel se os crimes cibernéticos são combatidos de forma adequada no Brasil e, em caso de dificuldades, quais são as maiores deficiências e em quê os órgãos de segurança pública brasileira precisam avançar.

Agradeço aos debatedores e à Presidente. Aguardo pelos esclarecimentos.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Deputado Daniel Coelho.

Concedo a palavra ao Deputado Rafael Motta, também Sub-Relator desta Comissão.

O SR. DEPUTADO RAFAEL MOTTA - Obrigado, Deputada Mariana Carvalho. Queria cumprimentar os nossos convidados, parabenizando também a Deputada Alice Portugal e o Deputado João Arruda por esses requerimentos de convite a essas autoridades, saudando o Sr. Marconni, o Sr. Otávio e o Coronel Paulo.

Deputada Mariana, mais uma vez aqui, há a nossa preocupação na nossa sub-relatoria. Nós sabemos que são quatro temáticas superimportantes sobre as quais nós devemos, realmente, gerar um relatório consistente. E essas audiências públicas têm sido de grande valia para poder realmente dar legitimidade a esse relatório, que vai ser apresentado nesta Comissão. O tempo é exíguo, então, temos que correr contra o tempo; enquanto nós estamos discutindo, diversos crimes estão sendo cometidos na Internet, no mundo virtual.

Queria me dirigir basicamente ao Sr. Otávio, que aqui representa a GSI. Mas não queria me restringir apenas a ele, gostaria de saber, primeiro, fazendo um posicionamento, se o sistema de fiscalização da ABIN... Sabemos da eficiência e do rigor que são cometidos por aquela instituição, mas nós queremos saber qual é a participação da ABIN nas investigações dos crimes de pedofilia na Internet. Se existe interação entre os diversos órgãos, como a ABIN colabora nas investigações da Polícia Federal; se existe alguma forma de interação com as demais instituições. E qual a forma em que é feita essa investigação, existe algum sistema, algum equipamento que possa acessar e retirar do anonimato esses potenciais criminosos que vemos no cotidiano cometendo crimes na Internet?

Também em relação aos tratados internacionais, sabemos que a ABIN tem a missão de revisar esses tratados, e o que pode fazer a GSI para modernizar esses

termos, esses acordos e coibir a prática de pedofilia nas redes sociais? Nós tivemos aqui diversos exemplos de convidados em que nós vimos que existe a prática clara, não precisa ser acessado nenhum tipo de *deep web* ou *darknet*, o mundo no anonimato, mundo virtual, mas nós sabemos que é cometido realmente até mesmo na *surface web*, que é conhecida também, aquela que é conhecida por todos, da qual temos livre acesso.

E aproveito também, Deputada Mariana, para fazer um posicionamento. Estive agora de manhã — inclusive me atrasei devido a esse compromisso —, com o Deputado Fernando Coelho e com o Deputado JHC, num café da manhã na Embaixada do Reino Unido e, inclusive, externei o posicionamento desta CPI ao Embaixador Alex Ellis, que nos convidou para essa interação entre Parlamentar e jovens. Na Embaixada do Reino Unido, fiz uma exposição sobre como se encontra a nossa CPI, Deputado, querido amigo Leo. Pedimos também que, se a Embaixada pudesse contribuir, Deputado Celso, com a nossa CPI, para que nós pudéssemos, realmente, também ter uma interação com as instituições internacionais com a CPI. Citamos a Scotland Yard, a própria Interpol, e o Embaixador, de forma muito humilde e solícita, disse que estaria à disposição para esta CPI, Deputado Sandro Alex.

Aqui deixo o nosso posicionamento, dizendo que a nossa sub-relatoria está trabalhando. Já estamos em contato com os Consultores e com esta Presidência, para elaborar um sub-relatório e, a partir daí, gerar um relatório consistente e que dê resultado prático desta Comissão.

Obrigado, Deputada Mariana Carvalho.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigado, Deputado Rafael Motta.

Concedo a palavra ao Deputado Sandro Alex, também Sub-Relator desta Comissão.

O SR. DEPUTADO SANDRO ALEX - Muito obrigado, Sra. Presidente.

Deputado Rafael Motta, nós vamos precisar dessa cooperação internacional quando formos tratar dos crimes de ordem financeira, que vamos abordar com mais profundidade na nossa CPI.

Sra. Presidente, agradeço a presença dos nossos convidados e quero deixar um comentário. Tenho percebido que nós temos apresentações à disposição do

organograma, dos cargos, das funções, e isso é relevante, mas sinto falta de números consistentes para a CPI do que realmente os senhores estão fazendo, ou seja, dos processos que estão em andamento, das dificuldades.

A CPI tem o trabalho de contribuir para essas investigações. Nós, em algumas audiências, percebemos aqui a dificuldade que os setores da Justiça têm em buscar as evidências, as provas, os *logs*. Eu gostaria de saber de vocês o número de processos, mesmo aqueles em segredo. Nós precisamos ter as informações do trabalho efetivo de vocês. Essas disposições são encontradas facilmente nos *sites* dos órgãos em que vocês trabalham. Enfim, eu gostaria de saber sobre funcionários envolvidos, afastados, queremos saber sobre a nossa segurança nacional, o número de processos em que os senhores trabalham. Já houve perigo realmente à Presidência da República? Invasões? Houve disposições de crimes contra a ordem nacional, contra a segurança pública? Há investigações que estão sendo realizadas? Há quadrilhas que vocês estão tentando desmantelar? Há cooperação com os outros setores, como Polícia Federal? Nós precisamos desses números.

Eu gostaria de pedir, Presidente, que V.Exa. solicite as informações a respeito desses processos que eles trabalham. Quantos são esses processos, Sr. Otávio? Coronel, nós precisamos saber do levantamento. O número de pessoas que trabalham nessas instituições, nesses *logs* é suficiente? Relativamente, estamos com um investimento recente, de 2008 para cá, como a maioria do senhores relatou. O número de pessoas que trabalham nessas investigações, nessas pesquisas, no desenvolvimento, é suficiente? Nós estamos com falta de orçamento? Qual a previsão para o ano que vem? Enfim, nós queríamos esse quadro, para que a CPI pudesse auxiliar nos trabalhos. Acredito que isso ainda não foi exposto aqui. E esses dados são muito importantes para o encaminhamento de trabalho de um relatório que vamos apresentar, pedindo modificações, atualizações, investimentos, cobrança aos outros órgãos.

Em algumas audiências, foi dito aqui da dificuldade na quebra de informações de algumas empresas que atuam no País, como o Facebook. Como vocês veem tudo isso, essas dificuldades? Nós já tivemos casos, por exemplo, de invasão na Presidência da República. A própria Presidente já se sentiu ameaçada. Já tivemos

ameaça? Esses dados são relevantes para nós. E sinto falta dessas informações nesta CPI. Eu gostaria que os senhores nos passassem o volume de processos e as informações, ainda que em segredo, para que pudéssemos ter a noção real de como está esse trabalho e em quê podemos melhorá-lo.

Obrigado, Presidente.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Deputado Sandro Alex. Por meio desta Comissão, faremos essa solicitação. Até mesmo como Presidente, acato a solicitação do Deputado Sandro Alex.

Apesar de ter me sentido um pouco contemplada com a pergunta do Deputado Leo de Brito, quero fazer uma pergunta em relação à questão de grandes eventos. Eu gostaria de saber — e acho que o Sr. Marconni pode acabar respondendo, e o ser Otávio pode ajudar na resposta —, se, no caso de um grande evento, como as Olimpíadas ou até mesmo a Copa do Mundo, vocês recebessem um comunicado através de WhatsApp de que poderia estar sendo planejado para a abertura um ataque terrorista, principalmente aqui, tendo em vista que estamos sediando cada vez mais grandes eventos no nosso País, como é que seria o procedimento adotado por vocês. Nosso País está preparado para isso? Gostaria de fazer essas perguntas, mais ou menos no sentido da pergunta do Deputado Leo de Brito.

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

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Com a palavra, Deputado Silas Freire.

O SR. DEPUTADO SILAS FREIRE - Há pelo menos 5 anos, o Dr. Otávio falou do papel da agência de proteger a transmissão de votos e não a computação. Mais ou menos, 4 a 5 anos atrás, nós nos deparamos com o episódio do Rio de Janeiro, onde a denúncia foi basicamente de transmissão de dados de uma região do Rio de Janeiro. Essa transmissão “poderia”, entre aspas — pelo menos foi o que se levantou na discussão —, modificar o voto dado ao Silas e dá-lo a determinado outro candidato antes de chegar à computação, ou seja, seria feito na transferência. Há inclusive indícios de que *hackers* teriam declarado, que, na transferência de dados, poderia ter uma interceptação, e eles transferirem, não muitos, mas uma

quantidade de votos, o que poderia tumultuar uma eleição. Isso foi silenciado no País. E eu acho que esta CPI precisa também desses dados.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Deixo também registada a solicitação desses dados, a pedido do Deputado Silas Freire.

Concedo a palavra ao Sr. Marconni dos Reis Bezerras.

O SR. MARCONNI DOS REIS BEZERRAS - Bom, meus senhores, eu vou tentar tecer alguns comentários de maneira geral sobre o que foi abordado.

Começando pelo caso NSA, também chamado de caso Snowden. O que eu tenho a dizer é que, como já foi até fruto de alguns comentários em audiências públicas anteriores, aquele evento trouxe o assunto à mídia, trouxe as questões da fragilidade, da vulnerabilidade das redes à mídia. O Snowden fez com que esse assunto fosse para o *Fantástico.* E os senhores sabem que o que vai para o *Fantástico* todo mundo assiste. Do mais alto nível ao mais baixo, todos assistem. E, aí, esse assunto começa a ser prioridade. Autoridades que deveriam investir no setor percebem que não investiram o suficiente, não capacitaram pessoas e passam a capacitar. Isso causou uma grande reviravolta nessa questão da segurança da informação. Essa eu vejo como vantagem desses efeitos Snowden-NSA: trouxe o assunto à mídia, e ele foi priorizado.

Naquela oportunidade, vários Ministérios se mobilizaram. Houve reuniões conjuntas. O Gessi participou de algumas reuniões com outros Ministérios, com o MCTI, com a Casa Civil. O que fazer para proteger mais as redes em relação ao que já vinha sendo feito? Eu tenho a dizer aos senhores o seguinte: isso ocorreu alguns anos atrás, poucos anos atrás, mas o que a NSA já vinha fazendo nas redes não apenas no Brasil, mas no mundo inteiro... Esse assunto é de muitos anos atrás. O Otávio pode até falar um pouco mais do histórico disso de algumas décadas atrás. Ele esteve aqui participando e, naquela oportunidade, já relatava tentativas de invasão de dados de redes no Brasil por intermédio de sistemas da NSA.

Naquela oportunidade, nós participamos de uma reunião conjunta, provocada inclusive pelo Ministro Mercadante, quando estava ainda no Ministério de Ciência e Tecnologia. Ele convidou ao Brasil um escritor renomado americano, ex-funcionário da NSA, James Benford.

Primeiramente, ele foi visitado por uma comitiva brasileira lá, nos Estados Unidos, porque era um profundo conhecedor da NSA. E foi convidado para vir ao Brasil conversar com altas autoridades aqui. Esteve com a Presidente da República, esteve na Casa Civil e, numa das reuniões de que eu tive oportunidade de participar — e o Otávio também estava presente —, ele falou de tudo que NSA era capaz de fazer, coisas que muitos de nós já sabíamos, qual o potencial da NSA, o que ela pode fazer. Ele apresentou e, no final, diante de tudo aquilo que ele disse que NSA era capaz de fazer, ou seja, tudo: ela pode captar qualquer informação que circula por qualquer meio eletrônico, seja virtual, seja cabo submarino, seja cabo satélite, eles são capazes de captar qualquer informação.

Foi perguntado a ele, naquela oportunidade, por um dos Ministros que estavam presentes: "*Bom, diante de toda essa fragilidade, de todo esse potencial da NSA, o que nós podemos fazer, então?"* Ele respondeu: *"Olhe, só criptografando, só criptografando tudo. Criptografe tudo aquilo que você não quiser que seja interceptado".* E ele deixou bem claro: *"Mas criptografe com algoritmo forte"*. Nesse aspecto, o Otávio pode falar, pelo CEPESC, melhor do que eu o que o Brasil vem fazendo em termos de algoritmo criptográfico de Estado para proteger as informações.

Foram palavras dele. Ele falou: "*Criptografe, mas criptografe com algoritmo seu, não compre de ninguém, porque, se você comprar de alguém, já vem quebrado. Então, desenvolva o seu próprio, aquele em que você confia, e criptografe as informações"*. Esse é um rápido comentário apenas sobre o efeito NSA.

Sobre aquilo que ele denunciou, ele disse que captou dados da Presidência, dados de várias autoridades, toda aquela informação que ele prestou nada teve a ver com o trabalho realizado, pelo menos, em particular, no DSIC, que é esse trabalho de prevenção que nós realizamos. Aquilo que ele denunciou foram dados que já haviam sido captados pela NSA. Ele, como servidor terceirizado, teve acesso às informações e gravou nos computadores da NSA. Quer dizer, não houve por parte nossa, das redes que nós monitoramos, com relação a tentativas de ataque, pichações, etc., esse fato não teve nada relacionado diretamente a isso. Foram dados que a NSA já tinha captado, e ele simplesmente teve acesso a essa base de dados.

Faço apenas mais um rápido comentário sobre o que foi falado aqui também sobre o potencial do nosso Centro de Tratamento de Incidente de Redes — CTIR. Como eu coloquei em alguns eslaides que eu apresentei, o CTIR monitora todas aquelas grandes redes do Brasil, todos aqueles milhões de sítios da Internet, tudo que é "*.gov", ".leg", ".jus", ".mil",* ele monitora com relação à tentativa de pichações e desenvolvimento de *sites* falsos. Há intensa ocorrência. Diariamente, para vários *sites* oficiais de Governo é desenvolvido um *site* falso e, por intermédio de tecnologias utilizadas por esse pessoal malicioso que se utiliza desse artifício, eles desviam a tentativa de acesso a um *site* verdadeiro para um *site* falso.

Existem várias técnicas para isso, o Spamdexing, o Googlebomb, etc. É uma série de medidas que ele pode usar para direcionar para um *site* falso o acesso de uma pessoa que está querendo acessar um *site* oficial. Nesse aspecto, nós diariamente temos notícias. Para os senhores terem uma ideia, alguns anos atrás, para um *site* oficial do Governo brasileiro que gerencia um sistema de consignações foi desenvolvido um *site* falso hospedado na Ilha de Tuvalu, no noroeste da Nova Zelândia.

Em poucas horas, a nossa equipe do Centro de Tratamento de Incidente de Redes detectou que havia esse desvio do *site* verdadeiro para o falso, que estava hospedado lá numa ilha, num paraíso ao noroeste da Nova Zelândia. Nós detectamos, comunicamo-nos, por intermédio de uma rede de confiança que existe entre essas equipes de tratamento de incidente de redes no Brasil e no mundo, com outro responsável pela rede naquela área, e em poucos minutos aquele *site* falso foi retirado do ar. Mas, no pouco tempo que ficou, o *site* solicitava o *login* e a senha dos usuários desse sistema estruturante brasileiro. Então, várias senhas e *logins* foram capturados.

O SR. DEPUTADO RAFAEL MOTTA - Vocês conseguiram rastrear esses *hackers?*

O SR. MARCONNI DOS REIS BEZERRAS - Não tem como identificar. Nós tentamos, quando nós temos indício, mas não cabe ao GSI o poder de Polícia, como eu já comentei. Havendo indícios, nós passamos aqueles indícios que nós temos para a Polícia Federal, e a Polícia Federal vai aprofundar na pesquisa. Nós notificamos a quem foi atacado e passamos os indícios do atacante à Polícia

Federal. Então, comunicamos imediatamente naquela oportunidade ao Ministério responsável por aquele sistema estruturante; ele, imediatamente, bloqueou a senha e o *login* daquelas pessoas que haviam sido divulgadas, e providências outras foram tomadas.

Um outro comentário que foi falado aqui é a respeito dos tratados e acordos no âmbito do GSI. Em um dos eslaides, eu coloquei que esses tratados e acordos, que nós cuidamos juntamente com o Ministério das Relações Exteriores, são acordos de troca e proteção mútua de informação classificada. É algo bem específico que é para o tratamento da informação classificada entre Estados.

Um caso bem típico agora com a Suécia. Foi assinado no ano passado um acordo guarda-chuva, que o MRE chama de Acordo-Quadro. Um acordo entre o Brasil e a Suécia para que empresas dos dois países, que venham a assinar algum acordo que envolva a troca de informação classificada, essas duas empresas dos dois países têm que estar habilitadas, têm que ter credencial de segurança das suas autoridades nacionais de segurança.

E, na legislação brasileira, a lei do acesso instituiu o Ministro-Chefe do GSI como autoridade nacional de segurança no território brasileiro. Então, as empresas brasileiras são, então, habilitadas pela autoridade nacional de segurança brasileira, que é o Ministro do GSI. Então, são acordos dessa natureza.

Com relação à Convenção de Budapeste e outros do gênero, que combatem o crime cibernético, nós temos trabalhado juntos, colaborando de forma apenas colaborativa com o Ministério das Relações Exteriores. Não tenho conhecimento profundo sobre esse tema, mas, pelo que eu sei, a Convenção de Budapeste ainda não prosseguiu porque alguns pontos previstos nela conflitam com a nossa Constituição.

Isso aí os juristas estão estudando. Essa convenção não foi possível ainda por esse motivo e por alguns outros, mas está se estudando um outro caminho para que um outro tratado, em particular, adaptado à nossa Constituição e às condições brasileiras, possa, então, ser acenado em nível internacional.

Aquele evento que eu comentei lá na Ilha de Tuvalu, na Nova Zelândia, aquilo é resolvido no canal técnico.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Só uma perguntinha nesse tema mesmo. O senhor acha que o Brasil não tem motivos para assinar a Convenção de Budapeste, no caso? Quando o senhor fala para haver outros.

O SR. MARCONNI DOS REIS BEZERRAS - Bom. Isso é conhecimento até onde eu sei. Eu não vou me arriscar aqui a dar uma opinião profunda porque não é atividade específica do nosso departamento. Não sei se a Mesa, o Otávio ou o Paulo Roberto poderiam aprofundar esse tema. Eu participei apenas como ouvinte de alguns debates desses que ocorreram no MRE e, até onde eu sei, foram apenas esses pontos abordados, da impossibilidade de assinatura dessa convenção, mas que está se estudando outro mecanismo. Eu soube apenas algum comentário a esse respeito. Não aprofundamos o tema.

O SR. DEPUTADO SANDRO ALEX - O senhor ouviu esse comentário vindo de quem?

O SR. MARCONNI DOS REIS BEZERRAS - De servidores do próprio Ministério das Relações Exteriores.

O SR. DEPUTADO SANDRO ALEX - Do Governo, então?

O SR. MARCONNI DOS REIS BEZERRAS - Do Governo. Do Governo.

O SR. DEPUTADO SANDRO ALEX - O posicionamento que eles falaram lá foi esse.

O SR. MARCONNI DOS REIS BEZERRAS - O posicionamento do Governo que não seria..., havia impedimentos de ordem conflitante com a Constituição brasileira. Foi essa a informação que eu tive, e não sei se o Otávio pode depois complementar isso aí.

A SRA. DEPUTADA MARGARIDA SALOMÃO - Comentários não oficiais?

O SR. MARCONNI DOS REIS BEZERRAS - Como?

A SRA. DEPUTADA MARGARIDA SALOMÃO - Comentários, mas não uma declaração oficial?

O SR. MARCONNI DOS REIS BEZERRAS - Não, não. Isso foi apenas de reuniões que nós participamos de debates no âmbito do MRE, em que nós fomos convidados apenas a participar como ouvintes e foram comentários que apenas observamos.

O SR. DEPUTADO SANDRO ALEX - Mas eram reuniões oficiais?

O SR. MARCONNI DOS REIS BEZERRAS - Olha, eram reuniões em que vários órgãos do Governo participavam. Justiça estava presente, Ministério das Relações Exteriores com vários departamentos internos deles, pessoas da área jurídica brasileira presentes.

Bom, eu destaco aqui apenas o trabalho normativo nosso do Departamento de Segurança da Informação. Nós não temos o poder de Polícia, como já comentei. O TCU tem nos ajudado nessa cobrança. Agora, cabe a cada órgão ou entidade da administração pública, que tenha elaborado a sua política de segurança da informação, o cumprimento desses preceitos elaborados por todo o comitê gestor.

Nós publicamos a norma, e a execução é descentralizada, ela é distribuída. Cada órgão, cada alta autoridade no seu Ministério tem a responsabilidade pelo cumprimento desse normativo.

Apenas com relação aos grandes eventos, que foi também comentado aqui, nós temos colaborado com o Centro de Defesa Cibernética, que está atuando como coordenador de todos os órgãos envolvidos, GSI, pessoal da Justiça, vários Ministérios que atuam junto. O CDCiber está montando uma estrutura grande no Brasil para o próximo grande evento, que é em 2016, e o GSI tem apenas participado como colaborador, por conta do nosso Centro de Tratamento de Incidentes de Segurança de Redes do Governo, nesse trabalho conjunto e colaborativo com o CDC.

Era o que eu tinha a comentar, por enquanto. Muito obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Com a palavra o Sr. Otávio Carlos Cunha da Silva.

O SR. OTÁVIO CARLOS CUNHA DA SILVA - Eu vou começar, como diz o outro, pelo começo. Eu fiz algumas anotações. O meu curso de Taquigrafia está muito velho, então, eu não consigo mais transcrever tudo.

Respondendo ao Deputado Leo de Brito, a utilização de *software* livre é importante, e sempre existiu uma mística de que o *software* livre era a grande solução para a segurança, porque o *software* livre era auditado, a comunidade trabalhava em prol de um nível de segurança, mas o *software* livre tem uma qualidade diferente. Ele tem a qualidade de estar aberto para a auditagem do *software* livre e possibilidade de implementações pela comunidade de *software* livre.

É muito importante. Se não fosse importante, nós não teríamos vários países no mundo utilizando *software* livre. É muito importante.

Mas eu acredito que não é a única ferramenta para se dar e se prover segurança. O *software* livre é importante, mas, da mesma forma que outro *software*, em outras plataformas, Microsoft, Apple, ele tem vulnerabilidades. Vulnerabilidades acontecem realmente no *software* livre.

Crimes cibernéticos...

O SR. DEPUTADO LEO DE BRITO - Quais seriam essas vulnerabilidades?

O SR. OTÁVIO CARLOS CUNHA DA SILVA - As vulnerabilidades, primeiro, quando você encontra, vamos dizer assim, uma falha no *software* livre, porque o *software* livre não é um *software* livre. Na realidade, ele tem vários, como a gente diz, *flavors*, sabores, de *software* livre. Então, você tem um chamado Kernel, que é a parte central do *software* livre comum, e ali em cima você constrói vários tipos, tipo Debin, tipo Ubuntu.

Então, cada um deles tem deficiências naturais, porque são *softwares* complexos, e, quando você desenvolve — esse é o grande problema do desenvolvimento de *software* —, você tem que desenvolver já com a questão da segurança em mente. Não desenvolva alguma coisa para depois você aplicar a segurança, porque desenvolver um *software* não é simplesmente escrever linhas de código, compilar, entregar e rodar.

Então, se você não tiver a filosofia de desenvolver de maneira segura, você não conseguirá o resultado de um *software* seguro. E o que a gente tem visto no mundo é que, primeiro, os *softwares* comerciais têm uma pressão de mercado muito forte, porque cada um está lançando uma versão a cada 6 ou 8 meses, o que significa que o ciclo de desenvolvimento está cada vez menor, e existe um ciclo de produto e um comercial. Então, é uma questão entre o pessoal e o comercial, apertando o pessoal do desenvolvimento, que tem que lançar o produto a cada 6 ou 8 meses.

Então, imaginem uma empresa, onde você tem milhares de pessoas desenvolvendo *software*, e vem o pessoal do *marketing* e diz: *"Olha, a data, querendo ou não, vai ser xis dia, dia 10 de fevereiro de 2016. Até lá vocês têm total liberdade para trabalhar, desde que no dia 10 eu lance o novo produto".*

Para quem nunca foi a uma empresa de desenvolvimento de *software* ou nunca trabalhou com desenvolvimento, eu diria que o início é muito tranquilo, o meio começa a ficar estressante e o final é impressionantemente estressante. Eu vi um livro, que estava colocado aqui, logo antes do início da nossa sessão, e me chamou muito a atenção o título do livro: *"Como tratar a ansiedade"*. Então, esse livro deveria ser entregue para todo mundo que trabalha em pesquisa e desenvolvimento de *software* e desenvolvimento de soluções.

Como tratar a ansiedade? A ansiedade, quando você chegar ao final do seu projeto, eu lhe digo como você trata. Entendeu? Você não dorme, trabalha, trabalha, trabalha, entrega resultado, vai vir problema, vai vir defeito, todos aqueles que você acha que encontrou, e o usuário vai encontrar aquele que você nunca pensou. É isso, essa é a realidade.

Então, o *software* livre, quando você parte para a comunidade... Nós tivemos agora uma grsec, que é uma questão de robustecimento de *software*. Nesta semana, o grsec lançou um anúncio na rede e disse o seguinte: *"A partir de tal dia, nós não vamos mais fazer* update *das versões de segurança"*. Então, todo mundo que está pendurado nessa questão do grsec está no ar, eu diria literalmente no ar, a partir desse dia, não tem mais. É como fez a Microsoft e como fazem outras empresas que dizem: *"A partir de tal dia, eu descontinuo o apoio ao XP"*. Por quê? Porque não tem como dar apoio, porque ela disse que não poderia ficar eternamente dando apoio. É natural, quer dizer, quem tem o viés de desenvolvimento entende.

Então, no *software* livre existem problemas, você tem que acompanhar listas e listas de segurança e o que a gente chama de Patch, que são os remendos de segurança, aqueles *band-aids* que você coloca no *software*. Eu diria que às vezes os *softwares* têm mais *band-aids* do que deveria ter. Você fecha uma porta e abrem três, e aquilo que você não pensou que fosse acontecer naquele *software* com aquele *band-aid*, você já abriu mais três entradas, e os crimes começam a fazer isso.

É por isso que eu digo que quem não trabalha de maneira estruturada é bom ter muito cuidado e uma equipe muito competente para qualquer *software* que se tenha, qualquer, livre ou não. Essa é uma questão de escolha estratégica de desenvolvimento para empresa.

Segundo, os crimes cibernéticos que o senhor levantou.

Olha, eu acredito que a questão de quanto o *software* livre vai ajudar ou não o impedimento do crime cibernético, nesses anos todos em que eu venho trabalhando com uma questão bem neurótica sobre segurança, a gente é até tachado como neurótico em segurança, eu não vi até agora um plataforma que diga: *"Esta plataforma é imune. Tal software livre é muito forte".* Existe um dos *softwares* livres que é o precursor do *software* livre, em que foram encontradas, nessa plataforma, no final de 2013 para 2014, várias vulnerabilidades. E qual foi a resposta quando perguntaram ao pessoal do desenvolvimento? *"Quando nós desenvolvemos esse software, nós não tínhamos em mente a possibilidade de ataques nessas características do nosso software, porque nós não desenvolvemos o software com essa característica"*. E esse *software* se chama FreeBSD e é considerado talvez um dos *softwares* mais rígidos e puros que há no mercado, e a solução foi essa.

Então, não é uma questão de usar o *software* livre e eu estarei mais ou menos seguro. Infelizmente não é isso, porque, senão, essa seria a bala de prata, todo mundo já teria trocado para o *software* livre, e nós estaríamos aqui bem mais seguros do que estamos atualmente. Esse é outro ponto.

Individualização do IP.

Eu diria que a questão da individualização do IP é uma questão muito séria, você pode tratar essa questão de maneira individual, por exemplo, na sua instituição, em que você vai ter um controle muito grande de quem fez o que e quem mandou que mensagem para quem, mas, ao mesmo tempo, você crava o que eu chamo de *flags*, bandeiras em algumas pessoas.

Se aqui na Câmara, todo Deputado tivesse um IP fixo e eu entrasse na rede da Câmara, eu ia saber muito mais facilmente a quem atacar, como atacar e ficar atacando por um tempo muito grande, porque eu iria naqueles que eu tenho interesse para minha matéria, para o meu objetivo. Então, é outra coisa que tem de ser muito bem calibrada. Isso tudo é uma gangorra, é uma questão de vantagem e desvantagem de onde eu vou implementar os meus níveis de segurança.

O IPv6 é uma realidade — desculpem-me aqueles que ainda acham que o IPv6 pode não acontecer. Não dá, o IPv6 está acontecendo, porque tem que acontecer. O IPv6 está acontecendo de maneira inexorável. A Olimpíada da China

foi toda em cima de IPv6. Tentar mascarar IPv6 com IPv4, com isso ou aquilo, vai piorar a sua vida. Agora, o IPv6, com uma boa criptografia mais certificação digital, eu diria que você está em um caminho muito bom para aumentar o nível de segurança do seu sistema.

Com a critptografia, a gente trabalha esses 30 anos, como eu já mencionei, e, com a certificação digital, eu tive o privilégio de coordenar a equipe que implementou o ITI. Eu fui o primeiro Presidente do ITI no Brasil e, desde o início da criação do ITI, eu dizia que certificação digital é uma *commodity*. Não queira transformar a certificação digital em uma solução, não é. Certificado digital é uma *commodity*, da mesma forma como várias outras ferramentas têm que ser usadas na condução do processo de uma segurança de um sistema. Isso é importantíssimo.

Se o senhor me permite... Eu tratei daquelas questões. Obviamente, a gente tem o problema de restrição de tempo, mas estamos sempre à disposição.

Deputado Silas Freire, V.Exa. perguntou sobre *deep web*, Tor, o que é, se é legal e como proteger o anonimato do Tor e do PhotoDNA.

Sobre a *deep web*, eu vou dar um exemplo aqui para a gente ver aquilo que eu estou falando com relação à questão de educação.

Eu tenho um grande sonho na minha vida: em algum momento, eu tenho que me aposentar, nesse momento em que eu me aposentar, obviamente, não posso ir para a casa, porque minha mulher já disse: *"Não fique em casa, porque eu não quero você aqui, você só vai dar problema"*, e eu vou ser o "já que", já que você está em casa, conserta isso, conserta aquilo, e eu sou péssimo para essas coisas. Então, o meu sonho é trabalhar em um programa educacional para crianças, o que nos Estados Unidos o pessoal chama de K-12, que vai desde o ensino básico, antes do fundamental, na minha época era creche, até os 12 anos — hoje eu tenho uma filha com 12 anos.

Por que eu estou falando isso? Porque, outro dia, minha filha chegou em casa, no almoço, e disse assim: *"Pai, o pessoal da minha sala está discutindo deep web, e você sabe o que é o Cicada?"* Eu digo: *"Sei, minha filha, sei o que é Cicada, sei o que é deep web".*

Eu, como pai, tenho duas opções, uma opção é enfiar a cabeça no chão e dizer: *"Vai estudar, não entra nisso, não faz isso"*, e a outra foi o que eu fiz. Peguei

minha filha e os amiguinhos dela e disse assim: *"Chama os seus amiguinhos para comer pipoca, tomar Coca-Cola, que seu pai vai dar uma tarde de deep web para todo mundo".* Coloquei todo mundo em casa, peguei o computador e fiz vários acessos à *deep web*, fui mostrando a eles o que é importante saber para não ser pego em problemas de *deep web*.

Então, o *deep web* é uma realidade, não tem como fugir, existe de tudo na *deep web*, tudo o que o senhor pode imaginar de mais absurdo.

Eu vi o pessoal do Instituto Nacional de Criminalística e vários Deputados se manifestaram sobre a pedofilia, que é uma unanimidade mundial. Pessoas normais, quando escutam aqueles casos do pessoal da Polícia Federal, ficam revoltadas. O meu sentimento é de revolta que isso aconteça, mas não é o meu, é de todas as pessoas normais, isso é revoltante, e você vê que a pedofilia, dentro da *deep web*, é apenas mais um dos problemas que existem na *deep web*. Nós temos ali torturas sendo transmitidas ao vivo, nós temos ali questões de contratar *hitman's*, como eles chamam, que são pessoas para matar outras. *"Ah, mas isso é muito sofisticado. Aqui em Brasília, a gente chega a determinada área e paga 100 ou 200 reais, e o cara vai e mata o outro".* É, mas no mundo tem várias formas de se fazer isso.

Deep web é legal? A *deep web per si* não é ilegal, ilegal é o que se faz dentro da *deep web*. Por que você entra em uma rede escondida se você está com um plano normal, legal e que não tem nenhum objetivo escuso? Isso você faz na *web* normal, você não precisa de uma *deep web*.

O Tor é feito da mesma forma como são feitas várias outras ferramentas, é para esconder e dar anonimato àquelas ações.

Um rapaz de 26 anos, americano, estava envolvido com isso, foi preso e condenado à prisão perpétua. As pessoas diziam: *"Puxa, pegaram pesado!"*, como dizem. Eu digo: *"Não, eu acho que ele só deu sorte de pegar prisão perpétua, porque ele poderia ser condenado à morte".* O que ele fez, dentro da *deep web*, foi um absurdo.

Então, essa questão de ser legal ou ilegal, para mim, que não sou advogado... Tenho filhas que são advogadas e admiro muito quem tem essa capacidade, porque a vantagem que eu vejo nelas é que você nunca tem uma resposta como tem um engenheiro: um mais um é igual a dois. Não, depende.

Nesse tempo, eu aprimorei a minha parte de engenharia, porque, na área de segurança, não tem uma solução única e não tem aquela camiseta que o pessoal chama de *one size fits all*, quer dizer, uma camiseta que serve para todo mundo, para magrinha, para gordinha, para isso e aquilo. Então, normalmente compram aquela camiseta e fica todo mundo satisfeito, porque vai servir.

O SR. DEPUTADO SANDRO ALEX - Dr. Otávio, quem financia a *deep web*?

O SR. OTÁVIO CARLOS CUNHA DA SILVA - Os grupos de crimes, porque o volume envolvido de dinheiro, os recursos envolvidos são altamente absurdos. Nós não estamos falando em milhões, nós estamos falando na casa de centenas de milhões e milhões. É um negócio fora do normal.

O SR. DEPUTADO SANDRO ALEX - Mas, no Brasil, qual é o tamanho dessa *deep web* e quem a financia?

O SR. OTÁVIO CARLOS CUNHA DA SILVA - Sinceramente, Deputado, eu não tenho condições de responder, porque nós não tratamos da questão de Polícia, nós tratamos da questão estratégica.

O SR. DEPUTADO SILAS FREIRE - Se o senhor me permite, eu quero até pedir à Presidente que nós possamos nos aprofundar na *deep web*, nesse caso inclusive de Polícia no Brasil, como o Deputado acabou de falar. Acho que a gente não tem números, não é?

O SR. OTÁVIO CARLOS CUNHA DA SILVA - Eu não conheço números, no Brasil, não sei quantificar. Sinceramente não tenho como lhe dar um número, como o senhor solicitou há pouco, mas eu sei que a questão é muito complexa. Acredito que o Brasil ainda está muito no crime na área financeira, eu acho que eles não desceram a *deep web* ainda. A área financeira está dando tanto lucro, então por que eu vou no *deep web*, como diz o Deputado, se aqui no *surface web*, quer dizer, no normal, eu estou ganhando tanto dinheiro? Mas, no exterior, o volume de recursos é muito grande.

Eu acredito que essa questão de segurança — de novo — vai passar, é por isso que eu tenho esse sonho de trabalhar nesse projeto. Não é uma questão de ensinar, mas de incutir a ideia de segurança nas nossas crianças e adolescentes. Eu falo isso de maneira totalmente generalizada. Não é para aquela classe que tem acesso a um celular, é para qualquer cidadão brasileiro, nessa faixa de idade. Tem

que ter essa formação. Por mais que a pessoa não tenha recurso suficiente, ela está exposta em centros comunitários, como vemos em várias comunidades, aqui, no Rio de Janeiro, em São Paulo, em que eles têm acesso à Internet. E o que eu vou fazer com um garoto desses na Internet? Ele vai ser um aviãozinho da Internet. Se os senhores me permitem, essa é uma opinião minha, como pessoa individualizada, não tem nada da minha instituição nessa afirmação, mas eles serão aviõezinhos da Internet. Eu faço essa afirmação, porque é muito grave o problema.

O SR. DEPUTADO SILAS FREIRE - Se o senhor me permite, a gente precisa levar a sério também o Tor , tanto as autoridades brasileiras, como o FBI.

Na semana passada, inclusive, foi preso o Sr. Robert, que é, sem dúvida alguma, hoje, o maior traficante *on-line* do mundo, e ele usava esse protetor para proteger os seus compradores. E essa prisão chamou a atenção do FBI.

Então, eu acho que isso pode estar acontecendo no Brasil também. Não podemos imaginar que o Brasil está em outro campo. Podemos imaginar que isso pode estar acontecendo: esse tráfico *on-line.* Estamos combatendo o tráfico de drogas fisicamente, mas ele agora está moderno.

O SR. OTÁVIO CARLOS CUNHA DA SILVA - É. Deputado, se o senhor me permite...

O SR. DEPUTADO SILAS FREIRE - Pois não.

O SR. OTÁVIO CARLOS CUNHA DA SILVA - Essa questão do Tor acho que está fora do nosso controle. Nós não temos controle. É um *software* que já foi distribuído e não foi desenvolvido no Brasil. O seu grupo de desenvolvimento não é brasileiro, e ele está disponível. Não há controle. Então, o que a gente tem que fazer é ter ações eficazes e eficientes.

Havia um parceiro meu de tênis que falava que preocupação não é ação de combate. Preocupação não resolve nada. Então, não adianta você ficar preocupado. Você tem que ter ações pontuais, claras e bem definidas para o combate. Acho que isso, obviamente, está no escopo da Polícia Federal. Eles fazem um trabalho excelente. O pessoal do Instituto de Criminalística teve uma apresentação excelente aqui na terça-feira, eu estava na audiência e gostei muito.

O SR. DEPUTADO SILAS FREIRE - Esse tema não levei à tona até porque é um tema que nós devemos discutir com a Polícia Federal em uma sessão reservada.

O SR. OTÁVIO CARLOS CUNHA DA SILVA - Isso. Eu acredito que sim.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Uma observação: recebemos aqui esta semana vários peritos e até falamos sobre esse assunto, que é de interesse desta CPI. Eles falaram que há um brasileiro que está em Singapura, na Interpol, que é uma pessoa que pode ter conhecimento principalmente sobre esse assunto.

O SR. OTÁVIO CARLOS CUNHA DA SILVA - O grande problema... Foi feita uma pergunta ao General Marconi com relação à atribuição — tecnicamente a gente chama de atribuição. Quem fez? Você descobriu quem executou o crime? Será que outros países estão nos atacando, sem entrar na resposta do General ali? É a questão mais crítica que nós temos hoje na Internet, que se chama "atribuição". É atribuir a alguém a autoria de algum crime. Por quê? Porque não só o Tor, mas várias outras ferramentas fazem com que as pessoas entrem e caiam no anonimato. Nós trabalhamos nessa parte estratégica de *cyber* segurança há alguns anos. Analisam-se a estratégia e ações de outros países. Então, realmente, temos visto que a coisa é muito profissional.

Eu já vi que não vou conseguir responder as perguntas uma a uma, porque há muita coisa, mas uma que eu já vi, toda vez...

(Intervenção fora do microfone. Inaudível.)

O SR. OTÁVIO CARLOS CUNHA DA SILVA - Esse é o ponto, porque toda vez que a gente senta aqui e fala que trabalha e dá apoio ao TSE, vem a grande pergunta: *"Puxa vida!"...*

TSE é um processo que eu digo excelente. Temos muito orgulho de trabalhar em parceira com o TSE, com o pessoal técnico do TSE. Esse não é um trabalho que começou e acabou em um dia, dois dias. É um trabalho de aperfeiçoamento que vem há 17 anos. Todo o processo está sendo aperfeiçoado. E uma das coisas que nós definimos desde o início é que nós íamos nos preocupar com a nossa competência. Nessa área técnica a gente tem que ser bom em alguma coisa, não adianta você querer ser bom em tudo porque você vai ser um generalista, não vai ser bom em absolutamente nada.

Então, se nós temos a competência estabelecida de desenvolver algoritmos criptográficos em âmbito de Estado... Eu digo que é muito diferente quando as

pessoas chegam aqui e dizem: *"Não, eu protegi a minha máquina com AES 128, 256".* Eu digo assim: perguntem ao governo americano, ao governo inglês, ao governo alemão, ao governo israelense, ao governo francês se, nas suas comunicações oficiais e nos seus sistemas oficiais, eles se utilizam de qualquer outro algoritmo que não seja desenvolvido por eles e não está publicado. A resposta vai ser unânime: ninguém no mundo, nesse topo que eu estou falando, de Estado, utiliza-se de *softwares* privados ou *softwares* comerciais. Essa é a resposta clara.

Quanto à segunda questão, nesse caso, em particular, do Rio de Janeiro, da transferência dos votos, tão logo nós soubemos da apresentação do rapaz que disse que tinha interceptado toda a comunicação, nós participamos, digamos assim, de uma reunião com a Polícia Federal, com o pessoal do TSE, com todos eles. Participamos de toda essa negociação e dissemos o seguinte: *"Vamos ver o que é, se isso realmente está acontecendo".* A nossa surpresa foi que o rapaz não conseguiu consistência no que dizia. Então, é muito bom se jogar uma questão dessa, como a gente diz, na imprensa, no ventilador, sendo bem popular, e depois não se garantir. Ao final, esse rapaz ainda saiu respondendo a um processo de difamação que o TSE abriu contra ele, e ainda está respondendo. Ele deve até hoje ter se arrependido de ter colocado uma mentira em uma questão técnica tão séria e em uma questão política e estrutural do País, porque nós estamos falando das eleições.

Perdoe-me, porque...

O SR. DEPUTADO DANIEL COELHO - Dr. Otávio, eu só queria fazer uma pergunta bem objetiva...

O SR. OTÁVIO CARLOS CUNHA DA SILVA - Sim.

O SR. DEPUTADO DANIEL COELHO - Se o *software* desenvolvido pela CEPESC é entregue compilado ou aberto ao TSE?

O SR. OTÁVIO CARLOS CUNHA DA SILVA - Isso. Era a resposta que eu ia dar agora, porque o senhor fez bem específica.

O SR. DEPUTADO DANIEL COELHO - Específica, é uma coisa de...

O SR. OTÁVIO CARLOS CUNHA DA SILVA - Nós desenvolvemos o *software.* Nós vamos ao TSE, junto com a equipe do TSE, que é fechada. Nós compilamos esse *software* do TSE, porque o *software* não é nosso, é do TSE.

O SR. DEPUTADO DANIEL COELHO - Vocês desenvolvem, mas é de propriedade deles?

O SR. OTÁVIO CARLOS CUNHA DA SILVA - É de propriedade do TSE.

Outra coisa que é muito importante deixar claro aqui é que, quando esse *software* chega lá, todo *software,* 3 meses antes do processo eleitoral, é aberto para auditoria e escrutínio por parte dos partidos políticos.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Dr. Otávio, eu só vou pedir para suspendermos a reunião por 5 minutos.

O SR. OTÁVIO CARLOS CUNHA DA SILVA - Claro.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Está havendo votação nominal, e precisamos ir ao plenário votar. Já voltamos.

O SR. OTÁVIO CARLOS CUNHA DA SILVA - *O.k*. Obrigado.

(A reunião é suspensa.)

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Reaberta a audiência, retorno a palavra ao Sr. Otávio Carlos Cunha da Silva.

O SR. OTÁVIO CARLOS CUNHA DA SILVA - Bom, eu comentei aqui com a Deputada Mariana Carvalho que, em face do adiantado da hora e pelo fato de nosso colega do CDCIBER ter uma série de questões, e eu também tenho dúvidas sobre uma série de coisas de que fizeram perguntas aqui, eu gostaria de encerrar a minha participação e passar a palavra ao Coronel Viana para fazer a sua apresentação.

O SR. DEPUTADO SANDRO ALEX - Sr. Otávio, o senhor estava falando sobre o TSE.

O SR. OTÁVIO CARLOS CUNHA DA SILVA - É, sobre o TSE.

O SR. DEPUTADO SANDRO ALEX - Da segurança. O senhor considera o TSE seguro ou...? Enfim, o ambiente?

O SR. OTÁVIO CARLOS CUNHA DA SILVA - Olhe, eu considero que o TSE é uma experiência positiva, rica, segura.

O SR. DEPUTADO SANDRO ALEX - Cem por cento segura?

O SR. OTÁVIO CARLOS CUNHA DA SILVA - Não existe 100% de segurança. Qualquer pessoa que se sente aqui na sua frente, ou num jantar, e diga: *"Eu garanto 100%"*, é solução tabajara, eu garanto. Quer dizer, não existe isso, não existe.

O SR. DEPUTADO SANDRO ALEX - E a sua impressão sobre a Smartmatic?

O SR. OTÁVIO CARLOS CUNHA DA SILVA - A Smartmatic? Ah, essa é uma questão de anos, não é? A Smartmatic há muitos anos entrou no processo eleitoral, concorrendo para desenvolver a urna, que não é nosso objetivo. Nós, no CEPESC, na ABIN, nós não desenvolvemos a urna. Nós trabalhamos só na criptografia.

Então, nessa questão — Smartmatic e Diabolô, disputas comerciais e tudo — eu tento não entrar, porque realmente não é minha seara. Meu tempo já é tão pequeno, e eu tenho um alemão correndo atrás de mim todo dia; o alemão chama-se Alzheimer, não é? Todo dia há um alemão tentando me pegar, e eu esqueço muita coisa.

Então, realmente, essa questão eu acho que é muito mais negocial, essa questão da Smartmatic com a Diabolô. Por muito tempo a Smartmatic tentou uma solução. Não sei por que razão ela não ganhou a licitação. Foi-me dito que foi por questões técnicas, foi apresentado em um relatório técnico o motivo por que a Smartmatic não tinha ganho, e tinha ganho, sim, a Diabolô, não é?

Então, o universo em que a gente trabalha é bem compartimentado. Nós não entramos, junto ao TSE, nessas questões, nós não temos essa participação. Por isso, Deputado, eu não tenho como lhe dizer mais sobre Smartmatic e Diabolô. Eu só...

O SR. DEPUTADO SANDRO ALEX - Mas o senhor não recebeu denúncia sobre ela, ou tomou conhecimento de denúncia sobre ela?

O SR. OTÁVIO CARLOS CUNHA DA SILVA - Não. As questões...

O SR. DEPUTADO SANDRO ALEX - Ou participou de reuniões sobre problemas em que ela estava envolvida?

O SR. OTÁVIO CARLOS CUNHA DA SILVA - Não. Nesses anos todos, a única coisa que eu conheço da Smartmatic é o que está na imprensa, aberto, que vem de fontes abertas, o que está na imprensa e eu leio. Nunca tive contatos com o pessoal da Smartmatic. Então, abstenho-me de dar qualquer declaração, porque realmente eu não conheço. O que eu conheço é o que está nos jornais. Então, é o básico. Nunca tive reuniões, nem abertas nem fechadas, com o pessoal da Smartmatic. Realmente, não tenho condição de expor qualquer outra opinião.

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

Concedo a palavra ao Coronel Paulo Roberto de Araújo Castro, Chefe da Divisão de Operações do Centro de Defesa Cibernética do Exército.

O SR. PAULO ROBERTO DE ARAÚJO CASTRO VIANNA - Muito obrigado. Eu vou procurar, então, atender aqui, de forma concentrada, uma série de perguntas que foram feitas, começando com a pergunta relacionada à preparação para os Jogos Olímpicos, o próximo grande evento.

Então, conforme eu havia destacado anteriormente, o Centro tem como missão, tem como atribuição a proteção das redes da Defesa, não é? Quando extrapolamos esse nível nós fazemos o papel de coordenação. Nós já estamos bem adiantados em relação a isso, no âmbito da Defesa existe todo um planejamento, voltado não só para a área de defesa cibernética, mas também para outras áreas temáticas, e nós estamos agora, então, procurando evoluir nessa questão do nível acima, da segurança cibernética, que envolve outros entes, em particular as infraestruturas críticas.

Então, nós temos uma preocupação muito grande com o setor de energia e o setor de transporte, que vão estar atendendo não só a cidade do Rio de Janeiro, mas também as cidades-sede do futebol, mas volto a destacar que nessa área nós não temos uma ingerência direta. Às vezes existe o equívoco de pensar que o CDCiber vai estabelecer uma grande muralha, um grande escudo protetor, e vai conseguir proteger todas as redes dessas infraestruturas, ou mesmo dos demais entes participantes. O responsável pelo ativo é que vai proteger o seu próprio ativo. Nós estaremos protegendo as redes da Defesa, a Rede Operacional de Defesa, que estará sendo utilizada durante o grande evento.

Também relacionada a isso é a pergunta que foi feita pela Deputada Mariana sobre ataques terroristas. Bem, Deputada, existem equipes voltadas para isso, não é? Existem, e se eu não estou enganado é o Ministério da Justiça que conduz a parte de ataque terrorista, com equipes das Forças Armadas, inclusive, e dos órgãos da segurança pública, mas nós passamos para essas equipes qualquer tipo de informação que nós possamos ter sobre isso, sobre alguma possibilidade de ataque terrorista, quer seja do mundo cinético, quer seja mesmo algum ataque cibernético que nós possamos gerenciar. Então, existem equipes voltadas para isso aí.

Sobre a tentativa de ataque de outros Estados, conforme o Dr. Otávio disse, essa é uma questão em que o domínio cibernético se caracteriza como impossibilidade de nós termos certeza de quem está originando aquele ataque, de onde vem aquilo ali. Os senhores devem acompanhar na mídia; volta e meia existem acusações múltiplas de um Estado para outro, dizendo que ataques foram originados em certos países. Então, é muito temerário dizer que houve um ataque originário de algum Estado, que aquilo foi de algum Estado. Sabemos que aparece como sendo de outro país, mas isso não quer dizer nem podemos afirmar com certeza que foi um determinado Estado que praticou o ataque.

Quanto a estatísticas, nós não temos estatísticas exatamente de crimes, já que crime é um assunto que está afeto à Polícia Federal. Então, quando nós verificamos algum indício de crime, nós repassamos esse dado para a Polícia Federal. O que nós temos de estatística é a relacionada ao número de incidentes. Então, isso é... Diariamente, são centenas de milhares de tentativas de ataque ou incidentes de segurança nessa área. Então, isso é um fato; acontece, como o General Marconi comentou, não só nas redes de Governo, mas também há tentativas nas redes da Defesa, e nós temos ferramentas que conseguem proteger-nos disso aí, ainda que, corroborando o que o Dr. Otávio disse, não exista sistema 100% seguro, mas as nossas ferramentas vêm conseguindo deter isso, não é? A nossa rede é uma rede fechada, e nós não temos tido problema em relação a isso aí. Mas não existe sistema 100% seguro, e nós temos procurado desenvolver novas ferramentas e ter ferramentas de proteção.

Quanto à pergunta sobre quais são os principais desafios para implementação da segurança e da defesa cibernética, eu corroboro o que já foi dito pelo General Marconi e pelo Dr. Otávio: isso não é uma coisa simples, não é? Esse tema é muito complexo. É um tema de Estado. Requer o envolvimento de toda a sociedade. E não só uma área, não é só a tecnologia. Envolve capacitação, envolve essa questão de criptografia, de certificação digital, de educação, de normas, é um tema muito complexo, muito amplo, e eu creio que nós temos de evoluir muito nisso, não é?

Na própria parte de crime cibernético existe a necessidade de uma estrutura legal que defina o que é que é isso, o que é que é crime, o que não é crime, na

própria conjuntura internacional, e crimes de um país para outro, não é? Uma pessoa faz num país uma tentativa de ataque que afeta outro país. Ela vai ser julgada naquele país de origem, no país de destino, o que sofreu o ataque, numa corte internacional? Então, isso tudo é muito complexo, não é? Mas eu creio que nós estamos trabalhando no Brasil para desenvolver essa questão da segurança e da defesa, mas temos muito a caminhar ainda. Temos de evoluir muito, em particular nessa questão da educação, do cidadão mais simples até dos órgãos públicos, num nível mais elevado, e também na parte de produtos. Temos de estimular a nossa indústria nacional voltada para desenvolver produtos em que nós temos uma confiança bem mais elevada do que num produto comprado de prateleira que vem de outro país.

Ainda nessa questão, voltando aqui à pergunta que foi feita pelo Deputado Sub-Relator quanto a número de processos...

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Eu só estou pedindo desculpas mesmo. É que está havendo outra votação nominal. Então, por isso é que todos acabaram...

O SR. PAULO ROBERTO DE ARAÚJO CASTRO VIANNA - Pois não.

Bem, sobre o número de processos e sobre o número de pessoas que trabalham ele perguntou se são suficientes e solicitou que nós apresentássemos aqui mais estatísticas, não é? Conforme eu disse, como não é nossa atribuição cuidar de crimes cibernéticos, não apresentamos aqui estatísticas sobre crimes cibernéticos, já que quando existe o indício nós repassamos o dado para quem de direito, que é a Polícia Federal, e depois eu não sei se aquele indício se concretizou como sendo um crime comprovado ou não. O que nós temos de números, de estatísticas, são os nossos números, o número de incidentes com que nós tratamos no dia a dia, nos grandes eventos, mas por ser a temática aqui o crime cibernético, eu não julguei por bem apresentar. E nós estamos sempre com a intenção de colaborar com os demais órgãos que estão aqui presentes, representados pelo General Marconi, da DSIC, pelo Sr. Otávio, da ABIN, pela Polícia Federal. O nosso trabalho é sempre colaborativo.

Sobre o número de pessoas que trabalham, nós temos vindo num crescente, não é? O Centro vem estruturando-se. Conforme eu disse, ele foi criado em 2010.

Ele está num crescente. A demanda é muito grande. Criamos recentemente o Comando de Defesa Cibernética; então, a tendência é aumentar a quantidade de especialistas, de *experts*. E a questão de orçamento, é lógico, vem impactando a nossa missão, mas nós conseguimos adequar, ou readequar o nosso planejamento, de tal forma que o que houve de corte não vai impactar-nos a ponto de impedir a nossa missão. Tivemos de cortar algumas coisas, mas vamos continuar cumprindo a nossa missão.

Então, basicamente, seriam essas as minhas colocações.

Obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigado. Eu agradeço ao Coronel Paulo as suas palavras e a sua participação. E aproveito para agradecer também ao Sr. Otávio e ao Sr. Marconi, que aceitaram o convite desta CPI e trouxeram aqui informações e dados. E vamos aguardar, a pedido do Deputado Sandro Alex, os dados que for possível os senhores repassarem a esta Comissão.

Nada mais havendo a tratar, declaro encerrada a presente reunião, antes convocando reunião ordinária da Comissão para a próxima terça-feira, dia 22 de setembro.

Está encerrada a presente reunião.

Muito obrigada a todos e bom dia.