SUFRAMA

SUPERINTENDÊNCIA
DA ZONA FRANCA DE MANAUS

www.suframa.gov.br

Clipping Local e Nacional On-line

Nesta edição 6 **matérias**

Coordenação Geral de Comunicação Social - CGCOM

Manaus, segunda-feira, 7 de maio de 2012

VEÍCULO
DIÁRIO DO **AMAZONAS**

EDITORIA

TÍTULO

Samsung vai produzir Galaxy SIII no Polo Industrial de Manaus

ORIGEM
INICIATIVA DO PRÓPRIO VEÍCULO DE COMUNICAÇÃO

ENFOQUE
DE INTERESSE

VEICULAÇÃO
LOCAL

Aparelho foi anunciado pela sul-coreana na quinta-feira

Manaus - Principal concorrente do iPhone, smartphone da norte-americana Apple mais vendido no mundo, o Samsung Galaxy SIII será fabricado no Brasil, nas fábricas de Campinas e de Manaus.

A informação é do vice-presidente de telecomunicações da Samsung no Brasil, Michel Piestum, que esteve em Londres na última quinta-feira para o lançamento do aparelho, segundo reportagem do jornal O Estado de S.Paulo.

Maior fabricante mundial de celulares, após desbancar pela primeira vez a finlandesa Nokia (em ranking elaborado desde 2004) no começo deste ano, a Samsung vai colocar o Galaxy SIII à venda no **mercado** europeu, asiático e na América Latina, incluindo o Brasil, no dia 29 de maio nas versões 3G e HSPA+ e nas cores grafite e branco, segundo o site Info. A informação inicial é que o aparelho custará R$ 1.899 por aqui. A versão 4G fará sua estreia na América do Norte em junho.

O novo 'smartphone' funciona com o sistema Android e tem uma tela de12,2 cm, 22% maior que a do antecessor, o Galaxy S2, com o qual a empresa sul-coreana desbancou a finlandesa Nokia como líder mundial do setor.

Entre os novos aplicativos do Galaxy S3 figuram, especialmente, funções de câmera inteligente que utilizam a tecnologia de detecção ocular e melhoram os controles de reconhecimento vocal.

Projeções para o ano

Em uma entrevista à agência DowJones Newswire, o chefe de comunicações celulares da Samsung, J.K. Shin, anunciou que o grupo espera vender este ano mais de 200 milhões de smartphones, inclusive modelos a um preço inferior aos US$ 150.

A Samsung, fortemente ligada ao sistema Android do Google, também planeja lançar em setembro um novo aparelho que utilizará o sistema de exploração da Microsoft.

Na categoria de smartphones, segundo a Info, a liderança continua firme nas mãos da Apple. A Samsung está posicionada em segundo lugar e a Nokia, em terceiro.

SUFRAMA SUPERINTENDÊNCIA DA ZONA FRANCA DE MANAUS	VEÍCULO O ESTADO DE SÃO PAULO		EDITORIA
	TÍTULO **Crise global já afeta as exportações**		
	ORIGEM INICIATIVA DO PRÓPRIO VEÍCULO DE COMUNICAÇÃO	ENFOQUE DE INTERESSE	VEICULAÇÃO NACIONAL

A crise global está afetando as **exporta**ções brasileiras, que,nomês passado, tiveram recuo de 8% em relação a abril de 2011. É a primeira queda na comparação de 12 meses desde novembrode2009.

Além dos planos de austeridade europeus e da desaceleração chinesa, os **exporta**dores estão sendo prejudicados pelo protecionismo da Argentina.

VEÍCULO
O ESTADO DE SÃO PAULO

EDITORIA

TÍTULO

Exportações travam com queda de preços de commodities e menor demanda global

ORIGEM
INICIATIVA DO PRÓPRIO VEÍCULO DE COMUNICAÇÃO

ENFOQUE
DE INTERESSE

VEICULAÇÃO
NACIONAL

Os efeitos da crise global, principalmente da recessão na Europa e da desaceleração da China, já são visíveis nasexportações brasileiras. Três fenômenos interligados atingem os embarques do Brasil: queda dos preços das commodities, menor demanda de clientes importantes e o aumento do protecionismo.

No mês passado, o **Brasil** exportou 8% a menos que em abril de 2011. É a primeira queda nesse tipo de comparação desde novembro de 2009, quando o mundo ainda vivia o auge da turbulência econômica. De janeiro a abril deste ano, as **exporta**ções brasileiras subiram só 2%,uma brutal desaceleração frente a alta de 17,5% acumulada em 12 meses.

Os planos de austeridade adotados pelos governos da Europa fizeram despencar investimentos, salários e geraram desemprego recorde.Na China, o ritmo da economia ficou mais fraco.O resultado é uma redução do consumo nas duas maiores regiões **importa**doras do planeta.

O pessimismo já levou a Organização Mundial do **Comércio** a cortar a previsão de crescimento das trocas globais em 2012 de 5% para 3,7%. O ano promete ter o segundo pior resultado em duas décadas.Em fevereiro, o **comércio** global contraiu 0,3%. Só 2009, o pior ano em sete décadas, com queda de 12% do **comércio**, foi mais negativo que 2012.

Tatiana Prazeres, secretária de **comércio** exterior do **Ministério** do **Desenvolvimento**, admite que 2012 será um ano difícil para as **exporta**ções,mas ressalta que outros países também enfrentam a mesma situação, como África do Sul, Chile e Coreia do Sul. A previsão do governo é que as **exporta**ções brasileiras cresçam 3,1% este ano, muito abaixo da alta de 27% de 2011.

A queda na demanda global atingiu os volumes e os preços das commodities, avariando um dos motores do crescimento do **comércio** exterior do Brasil. Das 23 principais matérias-primas **exporta**das pelo País, 16 tiveram queda na quantidade embarcada e 18 redução nos preços. As **exporta**ções de produtos básicos caíram 7,2% no mês passado. O desempenho só não foi pior por causa dos preços recordes da soja e das vendas de petróleo.

As **exporta**ções brasileiras recuaram para quase todos os destinos **importa**ntes no mês passado, com exceção dos Estados Unidos, país que absorve cada vez mais petróleo do Brasil. As vendas caíram 2,9% para a China, 8,5% para a União Europeia e 17,3% para a América Latina.

Protecionismo.

O **Brasil** vinha mantendo um bom desempenho nas vendas para a Argentina, principalmente de manufaturados. Nos últimos meses, esse canal de venda também foi comprometido. Em abril, os embarques caíram espantosos 27%, porque a Argentina adotou medidas protecionistas que quase fecharam seu **mercado**.O governo brasileiro está preocupado e deve-se reunir esta semana com autoridades argentinas.

VEÍCULO
CORREIO BRAZILIENSE

EDITORIA

TÍTULO
Tablets nos negócios

ORIGEM
INICIATIVA DO PRÓPRIO VEÍCULO DE COMUNICAÇÃO

ENFOQUE
DE INTERESSE

VEICULAÇÃO
NACIONAL

Clientes em loja de Cingapura: uso de aparelhos móveis nas empresas cresce em todo o mundo

O empresário do **Brasil** já usa mais dispositivos móveis de acesso à internet como tablets e smartphones em suas atividades comerciais do que os dos Estados Unidos. Enquanto na América Latina esse percentual chega a 67%, puxado pelo **mercado** brasileiro, na América do Norte não passa de 53%. Como se não bastasse essa diferença, 79% dos empreendedores do país estão interessados em ampliar o uso desses equipamentos para fazer negócios e elevar a produtividade dos trabalhadores, mediante a adaptação de programas já usados em computadores de mesa.

Os dados fazem parte de uma pesquisa inédita abrangendo 6.225 empresas de 43 países, encomendada pela Symantec Corporation, multinacional norte-americana de sistemas de segurança on-line. O levantamento do grau de mobilidade das empresas procurou avaliar como a adoção de tecnologias voltadas para a telefonia de terceira e quarta gerações está redefinindo a computação nos locais de trabalho. Enquanto 88% já usam os aparelhos para e-mail, só 57% o empregam na força de vendas. Um dos grandes focos no futuro, por exemplo, está no uso do GPS pelas equipes.

Riscos

Na média mundial, 71% das empresas afirmam estar buscando aplicações móveis ajustadas às suas necessidades. Um terço do total adiantou que já implementou ou está implementando essas mudanças. É uma realidade sem retorno e na qual as empresas esperam obter os melhores resultados. Mas também é grande a preocupação com os novos riscos de segurança para as informações , diz André Carrareto, gerente de engenharia de sistemas da Symantec Brasil.

Ele reconhece que o preço de produtos e programas ainda é uma barreira ao **desenvolvimento** do setor, mas acredita na tendência de barateamento. O executivo lembra que 48% dos entrevistados no mundo consideram a mobilidade um desafio e outros 41% veem nos dispositivos móveis um dos principais riscos na área de tecnologia da informação. A tendência é pouco menor na América Latina, onde 39% mencionou a mobilidade como risco. O desafio é, então, equilibrar riscos e benefícios da mobilidade.

As preocupações vão desde a possibilidade de roubos ou perda dos dispositivos a vazamento de dados, passando por acessos não autorizados a áreas exclusivas ou propagação de vírus e programas maliciosos por toda a rede da empresa. Entre as alternativas sugeridas pelos especialistas está o **desenvolvimento** de lojas de aplicativos para os funcionários da empresa e **desenvolvimento** de modelos próprios de navegação nos aparelhos móveis. (SR)

VEÍCULO
YAHOO! NOTÍCIAS BRASIL

EDITORIA

TÍTULO

PIB brasileiro pode crescer só 3% este ano

ORIGEM
INICIATIVA DO PRÓPRIO VEÍCULO DE COMUNICAÇÃO

ENFOQUE
DE INTERESSE

VEICULAÇÃO
NACIONAL

BRASÍLIA. Ao mexer na remuneração da caderneta de poupança, a presidente Dilma Rousseff pode ter tirado o maior entrave que existia para a queda das taxas de juros no Brasil. A estratégia, no entanto, não será suficiente para fazer a economia crescer os 4,5% que Dilma quer este ano. Mesmo que agora o Banco Central (BC) possa reduzir a taxa básica de juros da economia para um percentual inferior a 8,5% - patamar fixado como limite para as mudanças na correção da caderneta- o Produto Interno Bruto (PIB) brasileiro não terá uma alta maior que 3% ou 3,5% em 2012, avaliam técnicos do governo.

- Taxa de crescimento do ano já está dada - diz uma fonte.

Os reflexos da queda dos juros na economia só aparecem num prazo mais longo, em torno de 12 meses. Mesmo assim, a presidente continua pressionando sua equipe a trabalhar para incentivar a atividade por meio do aumento da oferta de crédito e do consumo.

Por isso, a equipe econômica tem como missão levar adiante uma agenda para estimular a renegociação de financiamentos de clientes com bancos (inclusive em contratos habitacionais) de forma que esses empréstimos se tornem mais baratos.

O governo pode criar uma espécie de ranking de juros e de tarifas que permita aos clientes **monitor**arem constantemente onde buscar melhores condições para seu financiamento. Também pode passar permitir a cobrança de algum pedágio de quem quiser migrar seu contrato de instituição, especialmente se ele estiver no início do prazo.

O governo também continua cobrando das instituições privadas a redução do spread (diferença entre o que o banco paga para captar dinheiro e o que ele cobra do cliente) e estudando medidas que permitam essa queda, como ajustes na implementação do cadastro positivo. Nesse caso, os técnicos avaliam, por exemplo, a possibilidade de permitir uma única autorização do correntista para o uso das informações do banco de dados.

Outra proposta é a facilitar a renegociação de dívidas atrasadas, com o parcelamento dos impostos incidentes na operação. Hoje, essa possibilidade já existe para pessoas físicas, com dívidas abaixo de R$ 30 mil e crédito agrícola. A permissão para que pequenas e médias empresas possam oferecer recebíveis (contratos pelo fornecimento de bens ou prestação de serviços) como garantias de crédito também são propostas que têm o aval da área técnica.

A equipe econômica defende essa agenda para que a presidente consiga terminar o mandato com uma taxa de crescimento de 5%. As ações são todas para que os juros continuem caindo. Na avaliação de uma fonte, as mudanças na poupança vão permitir que "a Selic caia de elevador".

De acordo com o relatório de conjuntura da consultoria LCA, a economia brasileira deve crescer apenas 0,5% no primeiro trimestre de 2012 em relação aos três meses anteriores. Mas para chegar aos 4,5% desejados, o número deveria estar acima de 1%. Segundo a LCA, a partir do segundo semestre, a atividade "deverá apresentar recuperação mais consistente (ainda que gradual), sobretudo quando se fizerem sentir plenamente os efeitos sobre a atividade econômica da redução acumulada da Selic".

Também contribuirão para esse quadro, a desvalorização da taxa de câmbio doméstica e também os incentivos concedidos pela segunda etapa do programa **Brasil** Maior. Entre eles, está a desoneração da folha de pagamento de 14 setores da indústria.

VEÍCULO
FOLHA.COM

EDITORIA

TÍTULO

Rio+20 é teste para novo centro de defesa cibernética; leia entrevista com general

ORIGEM
INICIATIVA DO PRÓPRIO VEÍCULO DE COMUNICAÇÃO

ENFOQUE
DE INTERESSE

VEICULAÇÃO
NACIONAL

NELSON DE SÁ

ENVIADO ESPECIAL A BRASÍLIA

Na entrevista abaixo, o general José Carlos dos Santos, comandante do CDCiber (Centro de Defesa Cibernética), detalha a implantação do novo órgão, que faz sua estreia na Rio+20, a Conferência da ONU para Desenvolvimento Sustentado, a partir de 20 de junho, reunindo cerca de uma centena de chefes de Estado e governo.

Folha - Vejo que o sr. está com "Cyber War", de Richard Clarke. Acabou de ler? José Carlos dos Santos - Estou no finalzinho. Às vezes uso até como fonte de consulta, porque apresenta muitos conceitos doutrinários e mesmo históricos, sobre o que ele considera que já começou, que é a guerra cibernética, embora eu não concorde. Até a questão do termo, ele é mais impactante...

É bom para vender livro. É. Mas o que nós temos, na realidade, é uma nova arma, a arma cibernética. É uma arma de guerra, mas essa é bem diferente das demais, principalmente porque não tem fronteiras, há dificuldade de identificar o atacante. Realmente é um novo campo de batalha.

Clarke diz que um episódio de derrubada de energia no Brasil teria sido um ataque.

Ele cita, sim, um apagão no Brasil, mas não entra em muitos detalhes. Cita vários casos semelhantes nos Estados Unidos. É uma vulnerabilidade. É uma ameaça, sim, porque, com a automação dos sistemas, a telemetria pela internet está sendo cada vez mais comum. Hoje, a distribuição de energia é baseada em uma central de controle, em que você pode ligar, desconectar, desviar, pode redistribuir, tudo por uma rede de computadores. O sistema mais conhecido para controle industrial é o Escada, da Siemens, que permite o controle de hardware por meio de um software, de forma reduzida é isso. Como todo software pode ser alvo de um ataque cibernético, nós consideramos, sim, no futuro, essa possibilidade. Mas imaginarmos que haverá um ataque ao país, derrubando sistema elétrico, eu acho uma hipótese um pouco distante. Nós teríamos de estar num contexto de guerra, em que houvesse interesses adversários tentando paralisar nossa **produção** industrial paralisando nossa distribuição de energia elétrica. Mas teoricamente é possível, sim, causar um dano grande a um sistema de distribuição elétrica, principalmente pela automação e pelo uso intensivo, cada vez maior, das redes de computadores para controlar sistemas industriais, energia, tráfego aéreo.

Outro dia mesmo, como cliente, eu sofri o problema de uma companhia, cujo sistema caiu. Alguém pode até dizer, "ah, foi um ataque hacker". É possível, é possível. A partir do momento em que a gente fica dependente das redes de computadores, tudo é possível. Isso leva as empresas, as agências governamentais, as Forças Armadas a ficarem atentas e buscar maneiras de nos precavermos contra essa hipótese.

Mais recentemente, Clarke afirmou que o episódio Stuxnet, o vírus que atacou no Irã, foi a abertura da caixa de Pandora. É. E outras coisas piores virão.

Márcio Neves/Folhapress

O general José Carlos dos Santos, comandante do CDCiber (Centro de Defesa Cibernética)

Aquele vírus focava...

Especificamente o sistema Escada.

Exatamente. O **Brasil** tem usinas nucleares desenvolvidas em projetos com a Alemanha. É uma das coisas que o sr. estuda hoje?

Nós estamos começando a estudar o assunto. O assunto é totalmente transversal, interessa não só à Defesa, mas à sociedade como um todo. Não conheço o sistema que controla Angra, mas, de qualquer forma, a distribuição da energia passa por esse sistema Escada. Então esse assunto está se tornando, sim, um assunto de preocupação de várias agências. Nós estivemos recentemente, no ano passado, na Eletrobrás para conversar sobre o assunto. Fizemos uma visita também ao sistema financeiro, no caso, a área de segurança do Banco do Brasil, trocando ideias sobre isso. E temos já algum trabalho, do próprio Rafael Mandarino, do GSI (Gabinete de Segurança Institucional da Presidência da República), alertando para essa hipótese e a necessidade de

conscientizarmos gerentes de TI, empresas, agências, para que seja tomada alguma medida de proteção desses sistemas.

O Exército hoje trabalha por projetos. Ele tem alguns projetos denominados estratégicos. O setor cibernético é um deles; o Proteger, que trata exatamente da proteção das infraestruturas críticas, aquela preocupação com a segurança física, proteção das hidrelétricas, dos gasodutos, torres de transmissão, é outro; o Sistema de Proteção de Fronteiras, Sisfron, é um outro projeto estratégico; a viatura blindada Guarani, que implica no reequipamento de toda a força terrestre, um produto nacional. Enfim, temos sete projetos estratégicos e somos um deles. Eles se entrelaçam, a partir do momento em que esses sistemas de transmissão, de telemetria, de controle e **monitor**amento passam pelo setor cibernético. Como **monitor**ar de forma segura? Como não termos esses nossos sistemas invadidos por pessoas não autorizadas? É uma preocupação inicialmente no aspecto gerencial, de que há necessidade de prover essa segurança. Então, eu acredito que, na evolução, nós teremos uma integração de todos os sistemas, em alguma central, vamos supor, do **Ministério** da Defesa para os sistemas militares e de alguma agência civil voltada para essa estrutura.

Nessa estrutura, em que parte entra o CDCiber?

O CDCiber é o dever de casa do Exército. Porque, com a Estratégia Nacional de Defesa, os setores cibernético, nuclear e aeroespacial foram colocados no mesmo patamar de importância estratégica para o país. E no prosseguimento dos estudos sobre o assunto o Exército recebeu a incumbência de integrar e coordenar, no âmbito das Forças Armadas. O CDCiber foi uma dedução, do Comando do Exército, de uma missão que ele tinha que cumprir.

E vai ser integrado com Aeronáutica e Marinha?

O **Ministério** da Defesa ainda não decidiu como isso vai ser feito, apenas definiu que o Exército é responsável pela integração e coordenação no âmbito das Forças Armadas. Da mesma forma que a Marinha o é para o setor nuclear, e a Força Aérea Brasileira, para o setor espacial. Dividiu as tarefas. Nosso **Ministério** da Defesa é relativamente novo. Ele distribuiu as tarefas como uma forma de otimizar os procedimentos, de melhor aproveitar os recursos. E o que estamos fazendo, em termos de coordenação e integração, é estudar o modelo de outros países, procurando as fontes de consulta que temos a respeito. Temos diversos modelos, mas todos eles apontam para uma necessidade de integração de Forças Armadas, e essa é a intenção do **Ministério** da Defesa: que no futuro possamos ter um setor cibernético integrado. E esse papel de sugerir medidas, propor ações, elaborar projetos, é do Exército.

A primeira preocupação nossa foi adquirir expertise, então em 2010 foi ativado o Núcleo do Centro de Defesa Cibernética. O Exército, para criar um novo órgão, precisa modificar a sua estrutura regimental, e isso só é feito mediante uma chancela presidencial. Foi feita uma proposta de criação do Centro de Defesa Cibernética, atualmente essa proposta está no **Ministério** do Planejamento, Orçamento e Gestão, que logicamente estuda as implicações orçamentárias e de planejamento integrado do governo, e de lá vai para a Casa Civil, para a sanção presidencial. É um processo um pouco longo, começou em 2010 e ele não se concluiu ainda. Nós estamos aguardando. Independente desse decreto, o Exército ativou um núcleo em 2010 e esse núcleo começou a elaborar um programa para a implementação. Esse programa inicial era constituído de oito macro-projetos, bastante ambiciosos, mas necessários. Na parte inicial, de capacitação, começamentos já em 2010 a capacitar o nosso pessoal, realizando cursos.

No IME (Instituto Militar de Engenharia)?

Em várias instituições. Por exemplo, o GSI há três anos tem promovido um curso de gestão de segurança de informação e comunicações, que é oferecido às agências governamentais e ao **Ministério** da Defesa. É um curso de especialização, com duração de cerca de 400 horas, feito em parceria com a Universidade de Brasília. Tivemos a formação da terceira turma neste ano, para gestores de alto nível, 180 profissionais. Também alguns cursos de nível técnico, inclusive com empresas estrangeiras. No ano passado, por exemplo, a Offensive Security ministrou um curso aqui para militares das três forças, para segurança ofensiva. O que é segurança ofensiva? Você tem que conhecer as técnicas de ataque, para poder melhor defender as suas redes. Atacar redes não é essa a nossa política. A nossa política é de defesa, até coerente com a postura do país. Então nós formamos um núcleo de cerca de 30 militares, nas operações de segurança de rede, conhecendo os instrumentos de ataque. Também um curso voltado para defesa cibernética/guerra cibernética. Aí usamos o termo guerra porque é voltado para operações militares. Essa parte de capacitação é um dos grandes projetos.

Outro é de defesa cibernética. Os primeiros investimentos do Exército foram no sentido de incrementar, melhorar a capacidade de defesa das nossas redes corporativas. E como isso pode ser feito? Adquirindo, por

exemplo, produtos na prateleira, "on the shelves". O Centro Integrado de Telemática do Exército, que é um órgão central, é o responsável pela instalação, exploração e manutenção de uma rede de telemática que permeia todo o território nacional, ligando mais de 600 organizações militares. Nós temos as nossas redes corporativas que precisam de uma certa confidencialidade e mesmo de segurança de que os ativos de informação terão o acesso dificultado a pessoas não autorizadas. E isso é feito capacitando nosso pessoal, comprando produtos de prateleira. Um dos mais conhecidos, para defesa de rede, é o IPS ou sistema de prevenção de intrusão. É um produto que está aí à venda e tem sido adquirido para a proteção das nossas redes. Por exemplo, uma página do Exército hospedada numa empresa terceirizada é menos segura do que uma página hospedada no nosso sistema interno. Uma empresa privada normalmente não tem investido tanto, até por uma questão de custo-benefício, como nós temos investido em segurança da informação. Nós inclusive temos sofrido alguns ataques de hackers, paralisando nossa página, e assim que possível essa página do Exército vai migrar para as nossas redes corporativas. Uma vez a cada dois, três meses, ela é paralisada por um ataque simples de se fazer.

Como é feito o ataque?

Um servidor tem uma determinada capacidade de atendimento de requisições. É o acesso à página, quando você digita o endereço ele vai acessar aquele servidor. Se esse servidor tem uma grande capacidade, ele logicamente vai resistir por mais tempo ao ataque. Mas, com as técnicas hoje de ataque bastante simples, uma delas é o que se chama de negação de serviço distribuído, os hackers conseguem espalhar em computadores de usuários um programinha que, sem o usuário saber, quando ele se conecta, começa a rodar e fazer requisições de acesso à página atacada. Com as botnets, redes de robôs, você consegue fazer milhares e milhares de requisições simultâneas, inundando o provedor, até que ele paralisa. Isso já foi feito e é quase inevitável nas maiores empresas do mundo. As agências de segurança, inclusive NSA, FBI, CIA, já sofreram esse tipo de ataque. A Sony.

Do PlayStation.

O famoso ataque do ano retrasado, do PlayStation. Instituições bancárias, no Brasil. Senado. Esse ataque praticamente não tem limites. E para que a gente consiga algum sucesso temos que investir. Então os investimentos iniciais do Exército foram nesse sentido, de aumentar a segurança das nossas redes.

E vocês fizeram uma licitação, compraram um antivírus da BluePex.

Isso. Ainda na parte de capacitação, para a experimentação doutrinária um dos equipamentos utilizados para treinar o nosso pessoal são os simuladores. Já temos um simulador israelense, da Elbit, que está sendo utilizado e preparado para os cursos que vão ser realizados ainda neste ano. Só que esse é um produto crítico. Então foi feita uma licitação e uma empresa nacional, a Decatron, foi a vencedora para desenvolver um simulador nacional. É uma das tecnologias que consideramos críticas e que devemos dominar. A outra, certamente, é o antivírus. Outra companhia brasileira já começou o **desenvolvimento** do antivírus nacional, que deve receber o nome de DefesaBR, para a defesa das nossa redes. Não só as redes de tempo de paz, as redes corporativas, mas também visando um emprego militar no futuro, na defesa das redes estabelecidas para uma campanha militar. Por que o antivírus é crítico? Porque ele permeia todo o software da máquina. Você tem que ter a certeza de que não tem nenhuma backdoor, nenhum instrumento de captação de ativo de informação. É a mesma preocupação, por exemplo, de quando foi montada a nossa urna eletrônica. Ele tem que passar por um processo de auditoria, para ver seus componentes, se o programa que vai rodar não tem nenhuma backdor ou trapdoor, que são formas de se alterar dados ou capturar dados não autorizados. Então, são dois produtos, mas estão sendo considerados críticos e nós procuramos parceiros para desenvolvê-los.

Falei de capacitação e defesa cibernética, agora a parte de inteligência. Existem hoje ferramentas que nos permitem **monitor**ar uma rede. "Ah, isso é ilegal." Não, você vai **monitor**ar as informações que estão disponíveis na grande rede. Existem hoje ferramentas que indicam tendências. **Monitor**ando as redes sociais, você pode identificar alguma tendência que traga informação **importa**nte para a defesa, como nós tivemos um exemplo nas ocorrências da Primavera Árabe.

Geralmente em busca de palavras, palavras-chaves.

Palavras-chaves. São ferramentas de inteligência em que também investimos. A própria parte de inteligência nos levou a investir na instalação de uma sala-cofre, que provê a segurança lógica e física de ativos de informação. Por exemplo, nossos backups estão física e logicamente protegidos numa sala-cofre. Foi feito um investimento nesse sentido. E,

como eu disse, podemos adquirir ferramentas que nos permitem **monitor**ar o que está acontecendo na rede. Ferramentas que nos dizem, "olha, o acesso está crescendo, não é normal tal nível de acesso". Aí nós vamos convocar nossos técnicos e ver, "daqui a uma hora nossa rede vai cair, a não ser que a gente tome alguma medida para evitar, selecionando os acessos".

E já existe o equipamento?

Já existe, sim. O próprio IPS, que faz de forma automática uma análise de rede e começa a selecionar as requisições. Eu cito até o exemplo do Richard Clarke, na questão da Geórgia. Por ocasião da penetração militar russa, em 2008, houve simultaneamente uma paralisação das páginas governamentais da Geórgia, de modo a impedir talvez uma repercussão do que estava acontecendo, mundo afora, diminuindo protestos etc. Foram alvos selecionados. Os georgianos, a partir do momento em que perceberam, tentaram migrar para outros provedores, baseados fora da Geórgia.

Nos Estados Unidos.

Estados Unidos, ele cita. Então, algumas medidas podem ser tomadas. Isso na parte de inteligência.

Na parte de apoio tecnológico, nós temos o Centro de **Desenvolvimento** de Sistemas. Quando vamos desenvolver um determinado projeto, é lá que vamos contar com engenheiros militares, que vão desenvolver as linhas códigos de acordo com os padrões que podemos estabelecer, de acordo com os requisitos operacionais, técnicos, para um determinado sistema. É um parceiro nos nossos projetos. Na parte de pesquisa, que você perguntou, entra o Instituto Militar de Engenharia. Ele faz pesquisa elegendo temas para os formandos, na área de mestrado, doutorado. Por exemplo, aí avulta de importância o domínio das técnicas de criptografia. São assuntos que interessam diretamente ao setor cibernético. O IME deve fazer uma parceria com a UnB, de modo a que possamos desenvolver projetos que atendam não só aos militares mas também às agências de governo. Como eu disse, é um assunto que permeia toda a sociedade.

Temos outros projetos, um deles é a própria construção do Centro de Defesa Cibernética, o espaço físico. Estamos ocupando, nos próximos dias, o espaço de uma unidade que está sendo extinta, o Centro de Documentação do Exército, numa questão de racionalização interna, que está passando todo o seu acervo para o Arquivo Histórico do Exército, lá no Rio. O espaço foi disponibilizado no final do ano passado e estamos já com as obras bastante adiantadas para ocupar, aqui no próprio QG. Esse é um outro projeto, que é a estruturação do CDCiber. Como a construção de uma sede requer recursos e tempo, essa sede provisória acreditamos que, até a construção do centro, vai nos atender plenamente, até porque ainda não atingimos 40% do efetivo previsto.

E qual é o efetivo que vocês buscam?

Imaginamos um núcleo, porque no nosso modelo de setor cibernético não atuamos sozinhos. No centro propriamente dito, em torno de 130, 140 pessoas.

No final, quando estiver implantado.

No final, quando estiver totalmente implantado. Já estou com 35 e aos poucos estamos crescendo.

Todos militares do Exército, ainda não tem... É, este é o Centro de Defesa Cibernética, por enquanto, do Exército. Se no futuro o **Ministério** da Defesa decidir que vamos exercer também o papel de Centro de Defesa Cibernética das Forças Armadas, é perfeitamente viável e até consta das diretrizes do **Ministério** da Defesa que tenhamos, nesse centro, militares da Marinha e da Força Aérea, como acontece com o Centro de Treinamento para Operações de Paz, no Rio. Hoje no Rio temos uma unidade que prepara militares para missões externas.

Da ONU.

Da ONU. Onde trabalham instrutores e **monitor**es das três forças. E é uma organização do Exército lá no Rio. Imaginamos que isso venha a acontecer também conosco. Isso vai de encontro ao modelo que observamos no exterior. Estive recentemente na Inglaterra, onde fui convidado a fazer uma palestra sobre os nossos projetos na Conferência de Defesa Cibernética e Segurança de Redes, no final de janeiro, e tivemos a oportunidade de fazer uma visita ao **Ministério** britânico da defesa e ao órgão operacional de defesa cibernética, a cerca de três horas de Londres, onde vimos esse ambiente, em que militares das três forças estavam trabalhando em conjunto, mais civis de empresas contratadas. A infraestrutura de telemática é uma coisa em que hoje as empresas estão totalmente envolvidas. Imagina-se que algo semelhante deva ocorrer no futuro, em que teríamos militares das três forças trabalhando em conjunto, e serviços prestados por empresas habilitadas.

O Cyber Command americano está sendo implantado...

Já está implantado.

Sim, mas eles também estão construindo um prédio, que ainda estaria para ser terminado. É, o Cyber Command é de 2009 e eles foram colocados no comando estratégico americano. Na estrutura militar lá, eles têm o comando estratégico e um dos órgãos subordinados é o comando cibernético. Esse comando cibernético tem ascendência sobre os órgãos das quatro forças, porque além de Exército, Marinha e Aeronáutica eles têm lá também os marines, que lá é como se fosse uma quarta força armada.

Mas aí a NSA (Agência Nacional de Segurança) também participa.

Plenamente. O comandante da defesa cibernética americana é o diretor da NSA. É o general Keith Alexander. Ele acumula a função de diretor da NSA e comandante da defesa cibernética.

Houve uma série de discussões sobre os papéis civil e militar na defesa cibernética americana.

Ainda existe isso e me parece que os americanos estão atualmente dando ao DHS, o Departamento de Segurança Interna, a responsabilidade da difusão das práticas de defesa de redes no meio civil, não só as agências governamentais, mas também no setor produtivo americano. Grande parte dos serviços públicos lá são providos por empresas. Na distribuição de energia elétrica, no Brasil, nós temos a Eletrobrás. O nível de privatização nos Estados Unidos é maior, então há uma preocupação de que haja alguma legislação que obrigue as empresas privadas a obedecer requisitos mínimos de segurança. O Richard Clarke expressa bem essa preocupação. Mas isso passa por uma grande discussão política: até que ponto as empresas privadas têm que se submeter às regras impostas pelo governo na segurança cibernética, uma vez que isso requer investimentos de grande porte? Vamos passar esse custo, aumentando os impostos? Há uma discussão grande, lá também, a respeito disso. Mas me parece que está bem definido quem é o encarregado de conduzir o assunto fora das Forças Armadas, seria o DHS, Homeland Security.

No Brasil, esse papel institucional é do GSI, mas, como somos uma iniciativa pioneira, a partir do momento em que o Exército criou o Centro de Defesa Cibernética algumas coisas, principalmente de caráter operacional, o GSI está dividindo conosco. Já estamos colaborando, por exemplo, para o aperfeiçoamento do curso que está sob a gestão do GSI. Estamos em conjunto com a UnB discutindo esse curso, adaptando, aperfeiçoando. A nossa interação com o GSI é grande. Outro exemplo dessa interação é a rede de segurança da informação e criptografia. É uma rede acadêmica que estava sob a coordenação, a supervisão do GSI. O Exército está recebendo a gestão dessa rede, que reúne pesquisadores, universidades, institutos de pesquisa. É uma rede bastante consolidada no meio acadêmico e que pode servir como instrumento de integração do meio militar com o meio civil.

Márcio Neves/Folhapress

Operador realiza testes no Centro de Consciência Situacional, a "sala de crise" do CDCiber

E o papel do Serpro (Serviço Federal de Processamento de Dados)?

O Serpro é um prestador de serviços para várias agências do governo, principalmente na infraestrutura de redes. Assim como o Exército tem seu próprio órgão, que é o Centro Integrado de Telemática, o Serpro o é para alguns órgãos governamentais.

Mas não tem integração? Porque eles cuidam de sites que são atacados.

As coisas estão acontecendo. Por exemplo, na Rio+20 o órgão encarregado da especificação da rede foi o Serpro, mas nós conversamos bastante antes. Então, estamos trabalhando, tenho recebido aqui o pessoal do Serpro, temos ido ao Serpro e trocado ideias, informações. E vamos estar juntos na Rio+20. O CNO (Comitê Nacional de Organização) da Rio+20 fez uma licitação e uma empresa privada é que vai montar a estrutura de telecomunicações. Nós estamos colaborando na especificação de requisitos de segurança, exercendo uma coordenação dos órgãos. Sob a coordenação nossa, temos o Serpro, a Polícia Federal, temos os órgãos estaduais e municipais. Então, quando se fala em coordenação de redes, um centro de coordenação, a responsabilidade é nossa. É a nossa primeira experiência real, de colaboração com uma agência civil, no caso específico o MRE, responsável pela organização da Rio+20. É um modelo.

O **Ministério** das Relações Exteriores. É, o Itamaraty é o organizador e nós estamos colaborando com a segurança cibernética. Sugerimos o modelo de **monitor**ação da rede, baseado até num modelo utilizado nos Jogos de Inverno de Vancouver, de 2010. Partindo daquele modelo, montamos uma estrutura física e lógica, de modo a colaborar com a segurança.

A Rio+20 é tida como uma espécie de teste de infraestrutura para a Copa do Mundo e os Jogos.

E eu diria que, em termos de repercussão, ele é tão **importa**nte quanto a Copa e os Jogos. Talvez até, em termos de participação mundial, seja mais crítica do que os outros eventos. Porque vai reunir cerca de cem chefes de Estado e governo, presidentes e primeiros-ministros, então tem uma representatividade mundial muito grande. Tem o aspecto de segurança da rede, porque certamente os governos usarão essa rede para trocar informação com suas bases, nos seus países. Os aspectos de segurança da informação e até de disponibilidade dessa rede serão críticos para o sucesso da Rio+20. Estamos procurando colaborar com a organização, sugerindo um modelo de **monitor**ação e até algumas medidas que constaram do edital para a contratação de uma companhia que vai prover a estrutura de telemática. Por exemplo, a estrutura deverá contar com sistemas de prevenção de intrusão. Isso tudo estamos acompanhando.

O chefe do Estado Maior das Forças Armadas americanas esteve no **Brasil** e, no retorno, mencionou como uma das esperanças de cooperação exatamente a defesa cibernética. Como é que está sendo feito esse encaminhamento, não só com os Estados Unidos, mas com outros países?

Além de o setor cibernético exigir uma integração no nível nacional, para que uma defesa seja efetiva há necessidade de integração entre países, porque os tipos de ataques vão se repetir. Os ataques que hoje são feitos às redes americanas ou de qualquer outro país deverão ser os mesmos tipos ou semelhantes. O setor cibernético não tem fronteira. O movimento hacktivista tem até uma nuance filosófica, como os anarquistas no início do século 20, combatendo o controle de governos. Isso hoje passa pela internet também. No movimento hacktivista, os mais conhecidos advogam que a internet deve ser um espaço livre de controle governamental, um espaço de troca de ideias e que qualquer controle governamental vai restringir as liberdades individuais.

Essa discussão é comum no Brasil, nos Estados Unidos. Hoje a Pipa e a Sopa, dois projetos de lei, são uma discussão muito grande nos Estados Unidos, como no **Brasil** está sendo feita uma discussão em relação ao marco civil da internet, que basicamente diz o seguinte, "primeiro temos que cuidar dos direitos do cidadão". E tem o projeto de lei do senador Eduardo Azeredo, que busca proteção para as redes, para os sistemas bancários, procurando responsabilizar não só autores de ataques mas também as prestadoras de serviço. A partir do momento em que se discute se elas serão obrigadas a manter os registros de acesso durante três anos, isso já é encarado, pelos que defendem total liberdade, como uma forma de **monitor**ar o cidadão. É uma discussão filosófica, política.

Que está em andamento.

Está em andamento. A solução vai ter que passar pelo Congresso, porque interfere realmente na vida dos cidadãos, na vida das empresas até, porque manter registro durante anos tem um custo. Tudo isso ainda é motivo de discussão na sociedade. Nós temos, logicamente, acompanhado tudo isso, porque tem implicações diretas na formulação das nossas políticas. Mas de maneira geral a nossa política é de defesa cibernética. É de defesa, de modo a podermos preservar nossos ativos e, numa situação de guerra, evitarmos que as nossas redes caiam, num tipo de ataque que já se teve, negação de serviço, ou mesmo de expropriação de dados confidenciais, numa operação de guerra, que dariam vantagem para o adversário.

Vamos ao CDCiber?

Eu só esclareço que estamos em obras, realmente obras civis. Mas já temos alguma coisa para mostrar. E a primeira delas, que inclusive esperamos ter já em funcionamento na Rio+20, é justamente dar aqui, ao Comando do Exército, condições de verificar em tempo real o que está acontecendo na Rio+20, em termos de **monitor**amento de rede. Estamos terminando a montagem do chamado Centro de Consciência Situacional, que é um centro de decisão ou, por enquanto, de acompanhamento do que se passa na Rio+20. O primeiro emprego dele é daqui a daqui a menos de dois meses.