Relatório Completo

Cibersegurança e Confiança

Realizado em 15/07/2015
Salvador, BA

Relatores da Trilha: Mariana Maia Ruivo e Rodrigo Nunes Souto
Relatório revisado por: Monica Maia Ribeiro e Ricardo Matheus
Data: 17/10/2015
versão: 2.0

1. INTRODUÇÃO

A Trilha 3 – **Cibersegurança e Confiança** do V Fórum da Internet no Brasil e Pré IGF Brasileiro 2015 foi realizada no dia 15 de julho de 2015 no Fiesta Convention Center em Salvador (BA).

Foi coordenada pelo Conselheiro do CGI.br, **Lisandro Granville** e teve como painelista representando a Academia, **Paulo Sérgio Licciardi Messeder Barreto** (Escola Politécnica da USP), o Setor Empresarial pelo **Marco Carnut** (*Tempest Security Intelligence*), o Setor Governo representado pelo **Coronel Ricardo Camelo** (CDCiber – Centro de Defesa Cibernética – Exército Brasileiro) e o Terceiro Setor pelo **Silvio Rhatto** (Coletivo Saravá).

A abertura dos trabalhos iniciou com um discurso do coordenador da trilha, que explicou os procedimentos adotados, no qual, cada painelista convidado disponha de vinte minutos para suas exposições iniciais. Após as apresentações, a plenária foi aberta aos participantes, que dispunham de três a cinco minutos para fazerem suas considerações.

Assim, o presente relatório divide-se em parte:

1. Temas discutidos;
2. Exposição dos Painelistas;
3. Intervenções e debates dos(as) participantes;
4. Exposição dos Participantes nos Grupos de Aprofundamento;
5. Anexos

2. TEMAS DISCUTIDOS

2.1. Tema 1: Relação Confiança e Cultura

- Fatores culturais na relação de confiança da(o) brasileira(o) e seus reflexos nas questões de cibersegurança.

2.1.1. Consensos

- As culturais influencias nas questões de cibersegurança;
- Dificuldade em definir confiança e segurança.

2.1.2 Dissensos

- Segurança para realizar compartilhamento das informações, com base na confiança.

2.1.3 Pontos a Aprofundar

- Não foi explicitado.

2.2. Tema 2: Soberania Computacional

- Soberania do Brasil em relação ao domínio de tecnologia;
- Soberania individual no uso da tecnologia.

2.2.1. Consensos

- Não foram explicitados.

2.2.2 Dissensos

- Há discordância sobre o Brasil ter soberania computacional e produzir tecnologia.

2.2.3 Pontos a Aprofundar

- Não foi explicitado.

2.3. Tema 3: *Software* Livre

- Confiabilidade do *software* livre na cibersegurança.

2.3.1. Consensos

- O uso de *software* livre:

  - É fundamental para fortalecer a segurança computacional.
  - Não é isento de vulnerabilidades.
  - Tem muito a ser desenvolvido na área de cibersegurança;
- O uso de *software* proprietário é um problema de segurança e soberania computacional.

2.3.2 Dissensos

- Não foram explicitados.

2.3.3 Pontos a Aprofundar

- Necessidade de domínio de tecnologia de *software* livre;
- O estudo de cibersegurança e *software* livre nas universidades;
- Necessidade de criação de equipes de desenvolvimento de *software* livre com foco na sustentabilidade e auditoria em áreas críticas.

2.4. Tema 4: Registro de Metadados e *Logs*

- Artigos 13 e 15 do Marco Civil da Internet, sobre registro de *logs* de acesso;
- Tempo de guarda e acesso aos metadados.

2.4.1. Consensos

- Os provedores não tem conhecimento e/ou formação para garantir a segurança dos dados coletados;
- Análise de tráfego é uma técnica barata e eficiente com capacidade de extrair bastante informação;
- A pessoa que está disposta a cometer um crime usará criptografia e anonimização para se proteger e, quem é leigo (a), não estará protegido (a).

2.4.2 Dissensos

- Necessidade dos *logs* para investigação:
  - Positivo: as autoridades investigativas precisam dos *logs* para rastrear pessoas que cometem crimes;
  - Negativo: os *logs* podem ser forjados, assim, podem não servir como evidência de um crime;
  - Negativo: precisamos pensar em outras formas de investigar e combater os crimes.

2.4.3 Pontos a Aprofundar

- Os artigos 13 e 15 do Marco Civil da Internet infringem a presunção de inocência?
- Preocupação em relação à segurança dos dados pessoais;
- Consequências da guarda dos *logs*;

- Possível uso dessas informações como ameaça e controle da sociedade;
- *Lobby* das empresas para garantir seus lucros com base nos dados pessoais;
- Necessidade de levar em consideração a opinião dos diversos setores da sociedade;
- Uso de criptografia como proteção aos *logs.*

2.5. Tema 5: Nuvens Computacionais

- A utilização de nuvens computacionais.

2.5.1 Consensos

- A nuvem só é confiável se ela for sua;
- Uso de nuvem pode ser vantajoso ou perigoso depende de como e para que ela está sendo utilizada;
- *Bitcoin*, quando bem implementado, é uma nuvem confiável, pois possui criptografia de ponta a ponta, sendo tecnologia inovadora.

2.5.2 Dissensos

- Alternativas de solução para o uso da nuvem:
  - Criar sua própria nuvem ou usar nuvem criptografada de ponta a ponta, *versus*
  - Dar maior foco para gestão de riscos do uso de nuvem contratada de terceiros.

2.5.3 Pontos a Aprofundar

- Salientar diferenças entre computação e armazenamento de nuvem.

2.6. Outros temas:

- Realização de cruzamento de dados de crimes cibernéticos com os dados registrados pelo CGI.br para a verificação da importância de realizar *logs* de acesso;
- Armazenamento de dados e conectividade das empresas de telecomunicação;
- Deficiência gerencial das empresas de telecomunicações em relação à gestão de dados;
- Marco Civil da Internet proíbe a terceirização da coleta e armazenamento de dados de acesso e exige que sejam guardados em ambiente seguro e protegido;
- Não há, no Marco Civil da Internet, provisão relativa à segurança dos dados pessoais;
- Um ponto chave de cibersegurança passa pelos *backbones* e como eles saem do Brasil;
- Cooperação entre Ministério da Defesa e Polícia Federal em assuntos relacionados a crimes cibernéticos;
- O Brasil está preparado para uma possível ciberguerra.

3. EXPOSIÇÕES DOS PAINELISTAS

A Trilha 3 – **Cibersegurança e Confiança** teve a apresentação de quatro painelistas que representavam quatro setores diferentes.

O painelista do terceiro setor, **Sílvio Rhatto**, falou sobre a necessidade dos usuários e usuárias desenvolverem a capacidade de se proteger da soberania computacional, bem como que pensar em segurança é pensar risco. Em seguida, o **Coronel Ricardo Camelo**, representante do governo pontuou que a defesa cibernética nasce da segurança da informação e que confiança é um termo subjetivo.

O representante do Setor Acadêmico **Paulo Sérgio**, tratou das curvas elípticas como um próximo passo da evolução da criptografia, provendo acesso seguro e tendência de substituição da criptografia RSA. Por fim, **Marco Carnut**, representante do setor empresarial, tratou do termo segurança como bastante amplo e que necessita de especificação para ser debatido, também colocou a importância dos usuários e das usuárias de reclamarem aos fabricantes para que assumam a responsabilidades pela falhas dos programas nos termos de uso.

A) Exposição Paulo Sérgio - Setor Acadêmico

O representante do Setor Acadêmico iniciou sua fala agradecendo ao convite realizado pelo CGI.br para participar do painel, disse que sua ideia é apresentar alguns detalhes que a Comunidade Acadêmica de Segurança, mais especificamente, de criptografia, em alguns aspectos criptográficos da segurança da informação, da segurança em redes, a fim de se ter um início de discussão para futuros debates. Seu foco foram as curvas elípticas; pois a criptografia baseada em curvas elípticas tem se mostrado bastante eficiente além de estar sendo adotada por grandes provedores de serviço em nuvem, que oferecem acesso seguro.

Ao tratar de “seguro” deixou claro que não pretende entrar em nenhum detalhe da segurança específica de protocolos, como o *Dynamic Light Scattering* (DLS) ou do *Secure Sockets Layer* (SSL). Apontou que aqueles que o seguem no Twitter sabem que os slides que preparou na manhã da apresentação já não estão mais atualizados, pois já surgiu ao meio-dia a notícia de um novo ataque contra o algoritmo *Rivest Cipher 4* (RC4); não precisa ser *National Security Agency* (NSA) para quebrar, mas aparentemente, um computador e 75 horas, o que dá aproximadamente três dias, tendo gravado uma comunicação cifrada com RC4, pode-se recuperar toda essa informação. Não é um ataque teórico, é um ataque bastante prático.

Apesar disso, declarou que há muitos outros problemas que a Comunidade Acadêmica está bastante preocupada. Existe, especificamente, a tendência de substituição da criptografia baseada em RSA por algoritmos criptográficos baseados em curvas elípticas, em inglês, *Elliptic Curve Cryptography* (ECC). Exemplificou o caso daqueles que tem uma conta no Gmail, pois podem verificar que o Google, já faz algum tempo, trocou a RSA; basta acessar a conta no Gmail, clicar no cadeado e observar os detalhes do

certificado que eles estão usando criptografia com curvas elípticas, conforme a norma 1CX9.62. É possível verificar também que a curva elíptica que está no final – curva elíptica padronizada pelo *National Institute of Standards and Technology* (NIST), dos Estados Unidos – é a curva P256.

Pontuou que uma dúvida comum é o porquê de eles estarem usando, agora, a criptografia com curvas elípticas, em vez de usar o algoritmo de criptografia RSA, que é muito mais popular. Observando uma comparação simples no gráfico apresentado dos tamanhos de chaves que são precisos para atingir o mesmo nível de segurança, disse que é possível ver que os tamanhos de chaves do algoritmo *Advanced Encryption Standard* (AES) são equivalentes aos tamanhos (128, 192, 256 *bits*) de uma chave de algoritmo simétrico. Para obter o mesmo nível de segurança proporcionado pelo AES, é preciso uma curva elíptica com o dobro do tamanho, exatamente um fator dois. Para o 128 *bits* basta usar uma curva de 256 *bits* – e então surge aquela curva P256, que o Google está usando; a curva do NIST.

Paulo Sergio disse acreditar que para alcançar o mesmo nível de segurança com o RSA, seria preciso usar uma chave de 3.072 *bits* e isso já está fora do padrão que se encontra em autoridades certificadoras. É muito mais comum estar recolhido na legislação, as curvas de 2.048 *bits* menos a raiz, que seria uma chave RSA 2.048, a autoridade certificadora, principalmente a raiz, tem uma chave maior, 4.096 *bits*, mas mesmo assim é uma curva, uma chave RSA de 4.096 *bits* não atinge, sequer, o nível de segurança do AES 192 – pra isso precisaria de uma chave muito maior, e os tempos de processamento vão se tornar impraticáveis quando se tem um volume de usuários do porte dessas empresas, desses provedores de serviço em nuvem.

Colocou como questão para os participantes: quais curvas e quais algoritmos devem ser utilizados? Ao trocar o RSA por uma coisa nova; o quê que se pode usar? O Google, assim como muitas empresas e instituições, está usando as curvas do NIST. Essas curvas foram acolhidas, simultaneamente, há quinze anos numa série de normas internacionais. Disse que para terem sido padronizadas nestes 15 anos, significa que essas curvas foram projetadas com a tecnologia, com o conhecimento que existia no final dos anos 90 e, mais concretamente, essas curvas do NIST foram construídas por um funcionário dessa empresa.

Pontuou então, que há um problema: de onde vieram estas curvas? Mostrou alguns números que tirou do padrão que especifica a curva P256, aquela que pode se ver no certificado do Google. Disse que nesta chave de números se consegue justificar tudo, exceto um número que aparece sem nenhuma explicação. E perguntou de onde vem este número? Respondeu que ninguém sabe. Ele apareceu por “mágica”. Segundo o NIST e a NSA é apenas um número gerado ao acaso, um número aleatório. Enquanto todo o resto pode ser calculado por funções matemáticas.

Falou que ainda há mais problemas com isso, uma vez que a NSA conhece muito bem do assunto de criptografia; é necessário reconhecer que eles têm um *know-how* incrível; um *know-how* público bastante grande hoje em dia. Colocou-se que se por um acaso eles

conhecerem alguma vulnerabilidade em uma família de curvas elípticas, que só se manifesta em uma curva a cada um trilhão de curvas, eles podem perfeitamente usar este conhecimento que só eles tem, e ficar gerando curvas – eles também tem capacidade de processamento para fazer isso – vulneráveis que só eles conhecem, mais ninguém, e que podem ser acolhidas no padrão. Isso não foi demonstrado, mas isso já foi apontado em 1999; hoje em dia, há razões mais do que suficientes para cogitar esse tipo de postura. Disse que para garantir que uma curva é segura, são necessários critérios melhores e a Comunidade Acadêmica vêm debatendo isso com mais intensidade há dois anos, aproximadamente, por causa da revelação do Edward Snowden.

Citou outro exemplo bastante popular, o *Bitcoin*, que também utiliza curvas elípticas. Eles usam uma curva que tem esse formato. Para se ter um *feeling* do que é uma curva elíptica, o representante da academia opera com uma estrutura algébrica mais complicada, tendo uma sopa de letras. A curva do *Bitcoin* é perigosíssima caso não seja bem implementada. Se for cometido um pequeno erro, é possível quebrar a segurança do *Bitcoin* em 62 segundos, utilizando qualquer notebook convencional, pois o próprio painelista declarou ter feito o teste.

Paulo comentou que isso foi trazido a atenção em 2013, via Twitter, apontando um trecho da implementação do *Bitcoin* que tinha um comentário que dizia que um determinado teste só estava lá para garantir a norma, mas que ele não fazia ideia do porquê. O problema nesse caso é que o próximo desenvolvedor vai ler este comentário – aliás, este é o único comentário em 500 linhas de código – e vai falar: “Ah, isso daqui é uma coisa puramente teórica. Por que vou fazer isso?”, e vai colocar este código apenas na versão de depuração, e não na versão em produção. No momento em que fizer isso, é possível fazer um programa que roda no próprio celular e quebra a segurança do *Bitcoin*. Acha que essa curva é péssima, e que não houve um planejamento no tipo de curva que foi adotado. Ele teve a impressão que foi escolhida essa curva para evitar aquela do NIST, mas não foi uma boa escolha. Será que é plausível este tipo de problema? Sim. Problemas de implementação, ele crê que são a maioria desses ataques que ganham logotipo, ficando popular: começaram com o *Heartbleed.* Erros de código e código mal feito são causas muito comuns de vulnerabilidades.

Na questão de algoritmos e padrões, disse que a NSA também sabotou um gerador de números aleatórios, baseados em curvas elípticas. Através de documentos vazados pelo Snowden, foi possível saber que a NSA pagou U$ 10 milhões para uma empresa de grande porte adotar este gerador como padrão. Melhores explicações estão a disposição em um documento em pdf.

Apontou que o esse tipo de vulnerabilidade é conhecida como *backdoor*, uma porta dos fundos. Tendo como padrão nessa norma, o *Special Publication* 900-90ª, explicou que durante sete anos, o algoritmo do NIST foi removido no ano passado por causa da revelação do Snowden. O painelista colocou que curvas e algoritmos são problemáticos. A questão é: o que se vai fazer? Se procurar na Internet o “*Cryptoform Research Groups*”, é possível ver que fazem meses, mais exatos 08 meses, que está tendo uma discussão com uma intensidade extraordinária: disse que tem gente xingando a família do outro; de

tão acaloradas que estão as discussões, do que fazer, quais são as curvas que se tem à disposição, em que pé que está o conhecimento, como é que se sabe que isso daqui é seguro ou eficiente, vai conseguir atender a demanda ou não.

Colocou que o Internet Engineering Task Force (IETF) está seguindo esse caminho também, tendo uma interação grande entre esses dois grupos. Pontuou que evidentemente, serão enfrentados obstáculos muito sérios se comprovar que as curvas do NIST tem mesmo este problema – mesmo que não tenha, a IETF já comunicou que não há como usar aquelas curvas. O próprio NIST já está dando sinais de que vão trocar. Vai ter problema de migração, como *bugs*, mas vai ter grandes vantagens também.

Finalizou citando que os trabalhos acadêmicos publicados estão mostrando que a atual tecnologia é de primeira linha e que se consegue obter desempenho em nível de segurança muito maior do que se conseguia na época em que as curvas do NIST foram projetadas, mesmo sem levar em conta o *backdoor* ou não.

O coordenador da mesa, o Conselheiro Lisandro Granville, passou a palavra ao representante do Terceiro Setor.

B) Exposição Sílvio Rhatto - Terceiro Setor

O representante do Terceiro Setor iniciou sua fala agradecendo ao convite do CGI.br para participar do Fórum e propôs tentar conceituar o tema da trilha, cibersegurança e confiança, numa perspectiva não só da sociedade civil, não só de ativistas, mas uma perspectiva mais ampla, porque acredita que existe, por um lado, uma impressão de que é possível obter segurança e privacidade total; por outro lado, nos últimos dois anos, pelo menos a cada dia as pessoas tem sido minadas por essa ideia. Parece-lhe que efetivamente a cibersegurança e confiança são utopias, citou que por outro lado, concordar com o representante da academia que o que se faz basicamente hoje em dia é enganação. A *National Security Agency* (NSA) não consegue trapacear matemática, mas consegue trapacear os usuários e as usuárias. Portanto, para se pensar em confiança é necessário pensar em risco, bem como é necessário analisar também na capacidade crítica de pensar o que se está fazendo, usando e adotando.

Disse que em relação ao nível de implementação criptográfica, apontou ser necessário pensar em como essa enganação pode estar presente em todos os níveis da comunicação mediada por sistemas digitais, não só no *link*, mas no que hoje se chama de nuvem e até nos próprios dispositivos. E a essa capacidade de perceber se está sendo enganado ou não, e evitar essa enganação, denominou de soberania computacional; não é apenas uma soberania nacional e também não é aquele conceito de soberano de existir um rei único soberano que governa, mas uma soberania, uma capacidade de cada organização, de cada pessoa, de cada grupo, de ter um pouco de controle, de ter uma capacidade de atestar, de verificar se a sua infraestrutura está comprometida ou não, o quanto se está sendo enganado, o quanto está sendo *hackeado*.

Colocou que usuários e usuárias estão sendo encaminhados para um mundo em que, apesar de tecnologias como o IPv6 estarem disponíveis, ainda experimentalmente, mas no futuro, já mais difundida, os computadores estão se transformando cada vez mais em terminais de acesso para uma nuvem em que usuários e usuárias não controlam. Não controlam quase nenhuma etapa de processo de fabricação, nem de uso e de alteração desses dispositivos, portanto conclui que se encontra num momento muito perigoso porque pra enviar uma mensagem de uma pessoa para a outra, um grupo a outro, não está lidando só com uma pilha de criptografia, está se lidando com diversas camadas, múltiplos pontos de distribuição de mensagens; e imagine-se que em cada ponto desse tem no mínimo um indivíduo querendo enganar outra pessoa. E esses indivíduos não são necessariamente pessoas, os usuários e usuárias caminham para um sistema automático de enganação.

O representante do Terceiro Setor citou seu trabalho já de alguns anos, de treinamento de segurança, para grupos e pessoas, para ativistas políticos, em que se tenta fazer o possível pra minimizar, esse fator de enganação, porém só se consegue relativo e modesto sucesso em nível individual se os grupos e as pessoas têm uma vontade e tempo pra despender.

Concluiu que deixar de usar celular e comprar um computador em que julga que seja menos infiltrado por *backdoors*, só usar *software* livre, trabalhar com criptografia de ponto a ponto, com verificação de ambos os pontos etc., é muito interessante para mitigar o problema. Só que isso começa a operar uma série de restrições e são restrições que são muito complicadas quando se quer ganhar em escala, ou seja, quando realmente se quer democratizar e fazer com que todas as pessoas, todos os grupos, todas as instituições tenham um acesso à soberania digital, e não apenas de inclusão digital, de pessoas incluídas, porque essa é a agenda do Facebook; sabe-se que a agenda do Facebook é baseada na enganação, por exemplo, assim como a agenda do Google e de grandes empresas da área. O painelista apontou a importância de uma inclusão com soberania, com certa autonomia, com uma garantia de que o usuário e a usuária não vão ser enganados.

O coordenador da mesa, o Conselheiro Lisandro, passou a palavra ao representante do Setor Empresarial.

C) Exposição Marco Carnut - Setor Empresarial

O representante do Setor Empresarial iniciou sua fala agradecendo ao CGI.br pelo convite e se apresentou como diretor técnico da *Tempest Security Intelligence*, uma empresa que foi criada em Recife há 15 anos atrás e está atuando no mercado de segurança de sistemas de informação, com uma atuação bem ampla, fazendo diversas coisas. Achou importante mencionar a área em que atua porque quem trabalha na área de segurança faz uma série de coisas, como teste de penetração – que é simular uma invasão e tentar invadir o sistema dos outros – em que se tem uma oportunidade única, que pouca gente tem, que é que a de lidar diariamente com as vulnerabilidades dos sistemas.

O painelista colocou que costuma ver todos os dias o lado negro da informática; aquele lado que as pessoas não gostam de admitir que existe. Apontou que essas coisas existem, pois ele tem visto e pode dizer. Colocou que na área de segurança existem – o painelista quis pegar essa ideia do representante do terceiro setor – muitas abordagens na área de segurança; muitas maneiras de abordar o problema. Disse que segurança, inclusive, é uma palavra difícil, porque é uma palavra que significa muita coisa diferente, para pessoas diferentes, em momentos diferentes. É difícil até às vezes estar falando de segurança no aspecto, por exemplo, do qual o professor Paulo, representante da Academia, falou: o de segurança criptográfica; tem muitas grandes empresas que não dão importância para segurança criptográfica. Elas estão interessadas em segurança contra indisponibilidade, portanto ela não quer que o sistema caia, porque eles preferem ser invadidos e depois se desculparem, do que os usuários e as usuárias não consigam acessar o banco de Internet ou não consigam passar o seu cartão de crédito.

Pontuou que existem dimensões completamente diferentes de segurança. Segurança significa coisas diferentes para pessoas diferentes; algumas pessoas estão preocupadas com privacidade e sigilo, autenticidade – como é o caso das preocupações criptográficas. Já a maior parte das empresas tem uma preocupação muito baixa com essas coisas. A preocupação deles já é disponibilidade. Exemplificou que se caso alguém chegar a um fabricante de *no-break* e bateria, eles vão dizer que trabalham na área de segurança: segurança para que não caia energia elétrica, que por sua vez, é importante para a disponibilidade dos computadores – o insumo principal deles é energia elétrica. Então, segurança é um assunto meio difícil de discutir.

O painelista defendeu que a primeira coisa que se tem que fazer, na área de qualquer tipo de segurança, é tentar responder a seguinte pergunta: seguro contra o quê, exatamente? Tentar ser específico, o mais específico que puder, quanto quais são as preocupações com segurança. O que se gostaria que não acontecesse? O que gostaria de se garantir que acontecesse. Acha que ás vezes não dá para fazer garantias absolutas, quase nunca dá, então se tenta fazer garantias mais ou menos probabilísticas.

Citou que o representante da Academia, pode dizer que quase tudo em criptografia é probabilístico, pouca coisa há de ser genuinamente certo, em que pese o poder da matemática e dos teoremas. Sugeriu para os debates que o participantes pudessem definir o que querem dizer por segurança, o que é a segurança, o que gostariam que não acontecesse, bem como o que acontece na Internet e que os perturba.

A partir desse viés introdutório, o painelista fez uma analogia: se alguém vai num restaurante e o garçom o trata mal e a comida estava ruim, essa pessoa não volta lá, essa pessoa acaba reclamando e às vezes denuncia para a Vigilância Sanitária, mas a principal coisa que se pode fazer é não voltar mais no restaurante. Passa uma mensagem muito clara e funciona! Os restaurantes que não fazem comida boa e não tratam bem, eventualmente perdem clientes e vem a falir. Se comprar um carro e esse carro tem um defeito de fabricação no projeto, a montadora arca com o reparo, com a troca, entretanto, contratou-se o desenvolvimento de um sistema *web*, ou se comprou um sistema operacional proprietário de alguns grandes *players* fabricantes que tem no Brasil, mas se

tem um sistema operacional com uma vulnerabilidade violenta e essa vulnerabilidade violenta que nada mais é do que uma falha de projeto, como uma falha de projeto de um carro ou de qualquer outra coisa, essa vulnerabilidade violenta permite, por exemplo, que um *malware*, que um vírus, um *worm*, se aproveite dessa vulnerabilidade para tomar controle remoto do computador da usuária e do usuário.

Pontuou sobre essa história do pessoal da informática falar termos complicados, *malware*, vírus, *worm* etc., na verdade, o *worm*, o *malware* e o vírus, nada mais são do que uma sabotagem remota. É uma tecnologia um pouco diferente, mas o conceito é o mesmo: sabotagem, mas o *malware* nada mais é do que uma sabotagem remota e tecnicamente rebuscada, sofisticada, de uma forma que o usuário e a usuária não percebam. Tem um *malware*, por exemplo, chamado *CryptoLocker*, que também deve ser muito caro ao professor Paulo, ele também deve ter visto muitos casos sobre isso, porque ele usa a criptografia, que é uma tecnologia do bem, para o mal.

Explicou que há uma invasão da máquina, criptografando todos os arquivos com um algoritmo de criptografia e então há um *screenshot* (foto da tela) dizendo que os arquivos pessoais foram cifrados, e assim estão inacessíveis naquele momento. Se houver o desejo de decifrar, para pagar o resgate, o chamado "*ransomware*". Disse que *Ramson* em inglês quer dizer resgate, no sentido de resgatar o refém. Os dados ficam reféns do interpretador dessa coisa, isso é um crime. Contou a história que uma vez o Departamento de Polícia, salvo seu engano, de Baltimore, dos Estados Unidos, foi invadida pelo *CryptoLockers*, havia uma vulnerabilidade que permitiu que fosse invadido e o criptólogo invadiu todos os dados da polícia e a polícia parou. Chamaram os especialistas em TI que disseram: "olha, o *backup* está meio atrasado, e eu sugiro que vocês paguem". E para o painelista aconteceu uma coisa extremamente humilhante de que a polícia foi forçada a pagar para os bandidos, que é uma antítese profunda do que a polícia deveria fazer: a essência do trabalho policial é não cooperar com os bandidos.

Recapitulou que o sistema operacional tem uma vulnerabilidade e essa vulnerabilidade é explorada por terceiros. Nessa situação, o quê que o usuário ou a usuária fazem? Nada. Continuam usando aquele produto defeituoso. O fabricante se esconde em alguns artifícios legais, em contextos legais obscuros e alguns deles, muito sem fundamento, para dizer que não é problema dele, pois quando compram certos produtos dos proprietários, tem um contrato de adesão que inglês se chama "*Term of Use and Rights Agreement*", em português, é entendido como "Contrato de Adesão". Em algum ponto do contrato, ele tem dito: "olha, se usar este produto, usa por sua própria conta e risco". O fabricante não aceita qualquer tipo de responsabilidade civil, penal, criminal ou de qualquer natureza pelo uso ou inabilidade de usar esse produto. Ou seja, quando vende o negócio e o fabricante do produto acha que não tem que dar garantia, que não é responsável pelos efeitos daquilo que usa, a posição dos usuários e usuárias é achar isso normal. E o mais importante: os usuários e as usuárias continuam usando esse negócio. Que mensagem está passando para o fabricante desse produto? Se fossem no restaurante e fosse servida comida ruim todo o dia e voltassem lá todo o dia, o que acha que iriam comer no dia seguinte? A mesma comida ruim.

Portanto, acha que é isto que está sendo feito com os sistemas operacionais que é um dos âmagos do sistema – não é o único, mas é um dos âmagos dos sistemas que define como o computador vai funcionar. Há uma aceitação histórica e o painelista sugeriu: não aceitem, troquem de sistema operacional. O painelista admitiu que pode ser complicado e não muito simples trocar um sistema operacional, mas quando um fabricante diz: "cara, eu não estou curtindo essa brincadeira, essa estória de você me mandar o tempo todo instalar, nova versão e sei lá o quê; tá enchendo o meu saco e não está resolvendo o problema". Insistiu para que não aceitem e troquem.

Levantou que há de fato escolha e irão descobrir que numa perspectiva empresarial, se pedirem para a empresa elas tentam atender. Algumas empresas são muito grandes e não vão aceitar; é normal. Mas se uma quantidade suficientemente grande de pessoas reclamar e rejeitar produtos inseguros, produtos com vulnerabilidades, produtos com defeito – a vulnerabilidade é um defeito de fabricação, de concepção, às vezes, de projeto. Não aceitem outras interpretações; as pessoas têm colocado na cabeça que é normal e não é. Vulnerabilidade é incompetência do desenvolvedor. Ele acha que os usuários e usuárias não devem aceitar isso, trocando de produto; e de uma maneira geral, conversando com as empresas, que vão tentar ajudar, vão tentar fazer melhor.

Citou um exemplo simples que viu recentemente: quando se encomenda para uma fábrica de *software* um determinado *software* e tem uma lista gigante de especificações um dos itens do contrato diz: a empresa tem que garantir que esse *software* não é vulnerável, que é um sistema *web*, e que as vulnerabilidades tem que ser garantidas pela "*Open Web Aplication Security Project*", que enumera e tentar dar soluções para as vulnerabilidades mais comuns de aplicações *web*. E o contrato diz também que: "se a sua aplicação tiver, se a gente descobrir, posteriormente, que a sua aplicação tem essas vulnerabilidades, você, desenvolvedor, vai arcar com os danos disso oriundos e com os custos de reparação, por sua conta; não vai ser meu não".

Apontou ser curioso é que isso é exatamente inédito: não se vê isso em licitações. Então recomendou que se peça aos fornecedores, explicitamente, de preferência em contrato, que eles ofereçam algum tipo de garantia sobre a segurança daquele *software*. Repetiu que isso parece mais fácil de falar nesse nível do que realmente de fazer, porque segurança é uma coisa complicada. Ser preciso com quanto ao que se quer de segurança, definir vulnerabilidade, definir quais vulnerabilidades o sistema tem que ser imune.

Finalizou explicando o tema de sua palestra: "a Internet é vulnerável?". Porque os usuários e as usuárias querem e tem aceitado isso, portanto pediu que não aceitem. Disse para que os usuários e usuárias rejeitem produtos vulneráveis, entendam o máximo que puderem a respeito delas, peçam para os fornecedores que entreguem sistemas com garantias explícitas, de oferecerem algum tipo de resistência às vulnerabilidades. A maior parte das vulnerabilidades que se encontram hoje foram descobertas nos anos 80, 90. Atualmente é século XXI, portanto é preciso mudar e evoluir.

O coordenador da mesa, o Conselheiro Lisandro, passou a palavra ao representante do Setor Governamental.

D) Exposição Coronel Ricardo Camelo - Setor Governamental

O representante do setor governamental, iniciou sua fala tentando fazer uma conexão com os demais painelistas, bem como dar uma perspectiva militar ao assunto segurança e confiança.

Colocou que achou interessante a abordagem feita pelo representante da academia, no assunto de criptografia, pois desde o início de sua carreira como engenheiro na área, foi graduado primeiro em engenharia eletrônica, trabalhou na parte de computação, manutenção de equipamentos, e depois, há mais ou menos uns vinte anos, foi para a área de segurança, e uma das cruzes dentro da área militar, era justamente a questão do uso da criptografia, porque sempre foi um elemento, um conhecimento negado; é uma arma, é uma arma desde as eras primordiais, tanto é que a nação mais poderosa do mundo mais ou menos na década de 80, dificultava, ou seja, proibia que algoritmos fossem comercializados com chaves mais extensas, ou os que saíam eram propositalmente mais pesados e só depois de muita pressão da parte econômica foi que isso começou a ser flexibilizado.

O representante do governo levantou que uma das cruzes da área militar, da área de pesquisa, ainda mais em um país que ainda está se encontrando, como o Brasil, o gigante tentando acordar, era justamente produzir esse conhecimento em território nacional. E para ele, quando chegava, por mais modestos que fossem os resultados, e tinha uma aplicação já completa, madura, estrangeira, em que se pedia para adicionar algoritmos, ouviam-se pérolas como: não há problema, desde que mande o algoritmo para o laboratório, se fazem as modificações necessárias e entrega de volta sem problema, mas tem uma segunda opção em que pode pagar, por exemplo, uns U$15 milhões por este aplicativo, que normalmente custaria algumas centenas de dólares e vende todo o código e tudo mais, e que acabava a conversa e a coisa não progredia.

Colocou que outro ponto extremamente importante de ser tratado no assunto de segurança, especialmente hoje em dia onde praticamente tudo tem computação, é a questão da confiança. Chega em um determinado momento no uso do aplicativo que é necessário se benzer (se for católico), um *namastê* ou um outro sinal espiritual e seja o que Deus quiser, porque é confiança dali pra frente. Não sabe se tem um atalho matemático, se tem uma sequência de números estranhos que aparecem do nada, ou um *backdoor* que não deveria estar ali, ou é só daquele jeito que dá certo e tem que confiar, sem saber se aquilo tem uma chave que possa abrir as informações.

Coronel Camelo foi diretamente nessa questão de confiança. Citou a fala do representante do Terceiro Setor, em relação a soberania computacional e declarando que foi uma fantástica ideia. E uma das coisas que esclareceu, no que diz respeito a essa parte de segurança e soluções de computação, é que o Brasil tem potencialidade – e

prova isso diariamente –, e que na área de computação, na área de engenharia de *software*, áreas relacionadas a TI, o Brasil conseguiu chegar junto com os maiores do mundo. Para ele, o que falta é a questão de prioridades, de uma boa gestão, de políticas que fomentem melhor isso e uma série de coisas que ficaria de discutindo tarde inteira, indo de A a Z e zerando várias vezes o alfabeto, principalmente no que diz respeito a capacidade desde colocar, usando uma linguagem militar, uma ordem unida, uma organização, um foco nessas soluções.

Destacou que no meio tempo, os talentos brasileiros muitas vezes são canibalizados para outros países, outras nações mais adiantadas, mais organizadas, mais avançadas. Mas se pode chegar; é diferente de um combustível secreto que coloca artefatos em órbita na terra, blindagens invisíveis, mexer com energia nuclear, que é um conhecimento negado, e talvez quando para chegar lá, os pioneiros vão estar em outro estágio de evolução. Em computação, consegue se chegar junto.

Citando a fala do representante do setor empresarial, o painelista abordou a questão dos brasileiros não reagirem. Este acredita que alguns passos modestos já foram dados, com alguns terrenos que foram conquistados a partir do ano passado; ao mesmo tempo, o Brasil tem até se destacado mundialmente como o líder, principalmente na parte de Governança na Internet, então isso tudo tem que ser muito bem refletido por todos, até porque quando se fala em segurança, e voltando para o tema principal, a responsabilidade é de todos. Ele explicou que existe uma característica cultural que, aos poucos, o brasileiro está superando, uma característica cultural que denomina “síndrome do Sassá Mutema”, em que sempre quer um salvador da pátria para ajeitar as coisas no lugar da população.

Destacou que é necessário lembrar que os brasileiros conseguem se superar e ir longe na área de sistemas de informação, de segurança. E no projeto, no Ministério da Defesa, quando se lida com defesa cibernética – é mais um conceito para o IA –um negócio para o qual o Ministério da Defesa está voltado pra lidar, mas cujo fundamento naturalmente é bem em primeiro lugar, segurança cibernética. Mas ainda, o mais fundamental para a área do consenso, usando a palavra da presente trilha, é a segurança da informação.

Tratou de uma política que se chama “Política Cibernética de Defesa”, um documento oficial do governo brasileiro, no nível do Ministério da Defesa, e que estabelece, com muita clareza, que o fundamento de toda a defesa cibernética nasce a partir da segurança da informação, que extrapola muito as partes meramente tecnológicas.. Disse acreditar que após se estabelecer como uma área de consenso, uma área já pacificada, aquela tríade que tem que ser garantida para proteger as informações – a integridade, a disponibilidade, a confidencialidade, e correndo por fora, a autenticidade, mirando na entidade que lida com a informação – é suficiente para que se comece a trabalhar nessa área. Pontuou que outro termo relacionado com a palavra da trilha, que é a confiança, vai muito para o terreno subjetivo.

Disse, também, que o Brasil está vivendo, ainda com todas as dificuldades que se veem nos jornais todos os dias, uma oportunidade muito importante, que é de sediar os grandes

eventos: acha que isso está servindo de aprendizado em muitas áreas, em especial no Ministério da Defesa, que lida com esses grandes eventos e tem trabalhado na parte de segurança cibernética para agregar valor à proteção das redes. E um de seus aprendizados mais importantes é o que se chama de ação colaborativa.

Citou o primeiro grande evento, o Rio +20, em que combinaram e reuniram uma série de trabalhos conjuntos, porém no momento do evento algumas coisas não ocorreram como o combinado, entretanto na Copa das Confederações funcionou de uma maneira melhor, depois na Jornada Mundial da Juventude e depois Copa do Mundo, foi melhorando gradativamente. O atual desafio são os Jogos Olímpicos no próximo ano. Mas o que quis dizer com a questão de colaboração e por que ela vai de encontro da questão do consenso: é o conceito de confiança, considerando um terreno subjetivo, porque as organizações, quando elas começam a trabalhar em conjunto, há um processo que, às vezes, é inaceitável, inacreditável, estranho, mas não acontece só em questões de cultura brasileira ou só no Brasil, acontece fora do país também. Elas não se aproximam com confiança: um desconfia do outro, não sabe se pode compartilhar uma informação, ainda mais na parte de segurança.

Colocou que os administradores de rede, muitas vezes, trabalham da seguinte maneira: administradores de rede e gestores de segurança, tentando garantir a segurança, acabam se auto envenenando, involuntariamente e isso é um processo histórico, que acontece na área de inteligência. Pontuou que outro problema que acontece também é de tentar acabar protegendo demais as coisas e, às vezes negando exageradamente a informação para quem se deve passar, como se a segurança fosse fim nela mesma, e não estivesse a serviço de algo maior, que é, justamente, a gestão da informação, o trato com a informação em todos os seus ciclos de vida.

Declarou que percebeu que a principal lição aprendida é trabalhar e confiar no companheiro da outra instituição, e isso é um fenômeno mundial. Disse que há cerca de três meses, esteve na Holanda e foi painelista num evento de segurança cibernética global, *Global Conference on CyberSpace*, que reuniu delegações do mundo todo e atuou em um painel que falava sobre a atuação dos civis e dos militares, como é esse relacionamento na segurança cibernética. E uma das perguntas que foi dirigida ao painelista pelo representante da delegação coreana foi justamente da confiança: como é que fazem? Porque pra vários países, a ação colaborativa brasileira na área cibernética é bastante impressionante.

Não são países de segundo ou terceiro nível, assim, mais modestos de maturidade cibernética, que vão procurar o Brasil, são os países de primeiro mundo. E isso é quase diariamente uma rotina do CDCiber. Declarou que há certa admiração dos representantes de outro países por ser possível falar em Exército, Marinha, Aeronáutica, Ministério da Defesa, Polícia Federal, Agência Brasileira de Inteligência e de Processamento de Dados do Governo Federal, CERT.br, Anatel entre outros, citando apenas alguns exemplos. Acredita ser um processo complexo em que há um consenso que é a necessidade de instituir relacionamentos fortes entre organizações, sendo de extrema importância, bem como fundamental, como uma base, não sendo uma situação ou um processo que passe

de maneira incólume.

No âmbito do Ministério da Defesa, colocou, neste mesmo evento em que esteve presente foi a outro evento paralelo, prévio à essa conferência, que foi a discussão do Manual de Talen, que trata sobre direito internacional para uso da cibernética em situações de guerra. Isso se trata de algo ainda bastante complexo em termos de aplicação, sendo estudado uma versão 2.0 e por ser uma iniciativa do bloco europeu, mas na mesa, nessa discussão, haviam representantes do mundo todo: as Américas, a Ásia, a África e o Oriente Médio. O bloco europeu declarou ter sido uma experiência incrível, bem como percebe-se que é uma necessidade urgente de se estabelecer regras internacionais para lidar com o uso da cibernética; para garantir a segurança, para se ter confiança naquilo que se lida, com o que se publica, no que se baixa e no que se usa, porque percebeu-se, principalmente por causa dos últimos escândalos, que no final das contas nada é confiável. Portanto, concluiu que mais uma vez, o que era antes a criptografia, a matemática para a maioria das pessoas, levou muita gente para a terapia depois do ensino médio.

Mostrou o celular que estava em sua mão, dizendo que não pode usar dentro do CDCiber, sendo obrigado a guardar e a desligar, pois o celular virou um computador que tem como função secundária ser telefone, e é provado, que se alguém quiser espionar, pode invadir com facilidade um aparelho, e gravar o que se está falando, fotografar, acompanhar os seus movimentos, inclusive, mapear rotina diária.

Portanto, ressaltou como essa é uma questão realmente complexa e os países estão enxergando isso, estão batendo cabeça, estão discutindo, nessa reunião em que participou. Citou que algumas discussões básicas que até voltavam a origem: o que é a soberania em cibernética?

As confusões causadas por essa soberania acabam colocando o mundo num mesmo nível e todos preocupados com isso. Algumas nações de primeira linha no que diz respeito à essa dinâmica – por exemplo, China, Rússia, em reuniões que ocorreram no Brasil – que as consequências de uma guerra cibernética são tão graves quanto uma guerra nuclear; quem declarou isso era segundo escalão de autoridade de países de primeiro time nessa área.

Concluiu que nesses pontos há uma necessidade muito grande de aprofundar, de saber como se aplica no direito internacional, se está realmente vivenciando uma corrida armamentista cibernética e o que fazer com isso. Convocou a todos para lutarem, não podendo ser mais realistas que o rei, não podendo faltar com a ética, precisando lutar pelo o que é certo, mas questionou qual é o caminho do rei? Comentou sobre um especialista que trabalhou na Casa Branca por muitos anos e hoje é conferencista e era o chefe da área de contra terrorismo no 11 de setembro. Em sua entrevista, ele fala que quando perguntaram ao Presidente sobre as providências a serem tomadas, o Presidente daquela nação disse: “vamos retalhar, seja quem for”, e o Secretário de Defesa disse: “não, chefe, mas tem os direitos internacionais e isso e aquilo” e para encurtar a estória, “olha, não quero saber. A gente vai fazer o que a gente quiser”.

Apontou que fóruns como o da Internet no Brasil, são extremamente importantes para fazer com que se reflita, que saia da área de conforto e reaja, a soberania e garantia, e que não há nenhum tipo de complexo em relação ao mundo; principalmente nessa área, o Brasil chegou junto, não podendo esquecer que as capacidades brasileiras são muito grandes, portanto é necessário estar engajado nessa luta, seja na parte de ativistas, seja na parte política, seja na parte de testes, seja nas empresas. Desta forma, é possível se ganhar uma real maturidade e, seja no sentido subjetivo, parte emotiva da significação da palavra confiança até a parte técnica, propriamente dita, porque acha difícil, pelos paradigmas atuais, escapar que nesta máquina, o computador, que aqui tem uma tela, da China, um teclado de outro lugar na Ásia, um processador da América do Norte, e assim por diante.

Declarou que as pessoas acabam ficando paranoicas, preferindo ir para as cavernas e abrir mão de toda essa tecnologia Ele acredita que não tem como e que um meio termo para conseguir, seria uma tecnologia intermediária, que para ser construída é necessária que todos parem e reflitam. Vê o fórum como sendo uma dessas oportunidades.

Resumiu sua fala dizendo acreditar que um ponto de consenso, pelo menos da perspectiva que tem lá no Centro de Defesa Cibernética é que ao falar de segurança cibernética, há conceitos paralelos, como segurança de rede, segurança da Internet, crime cibernético etc., mas o fundamento é que a informação, seja ela algo escrito, físico ou o que está a transformar os maravilhosos zeros em “uns”, seja que realmente aprofunde na tríade da integridade, da confidencialidade e da disponibilidade, mas com domínio de conteúdo com soberania, em que possa se construir e confiar, bem como cobrar um resultado. Tem que haver mecanismos que construam essa confiança também institucionalmente, não tão subjetivamente, ainda que com esse caráter não há como escapar.

Em relação a questão técnica, acredita que é um ponto a aprofundar, pois a própria palavra confiança, confiabilidade, serve como atributo para certas áreas da computação relativas a aspectos de sistema, de construção de sistemas; a própria área de criptografia, então, um exemplo fantástico da área de aprimoramento da questão de segurança, no aspecto confidencialidade.

Finalizou declarando que o Brasil está junto com os países de primeiro mundo, não devendo a ninguém.

4. INTERVENÇÕES E DEBATES DOS(AS) PARTICIPANTES

Lisandro Granville *(Conselheiro do CGI.br – Rio Grande do Sul):* iniciou sua fala convidando os participantes a fazerem suas perguntas, em seguida deu início aos debates fazendo uma pergunta para todos os painelistas da mesa, dizendo que no primeiro momento as questões técnicas são aquelas que mais lhe chamam a atenção.

Colocou que ouvem-se casos internacionais que despertam o interesse, e esses aspectos técnicos acabam, talvez, tendo uma relevância bastante grande. Mencionou que o Coronel, representante do setor governamental, falou sobre a questão de confiança – e lhe parece que essa é a questão passa por aspectos culturais também. Imaginou que talvez o jeito dos brasileiros operarem levem a uma situação aonde as entidades acabem tendo mais confiança entre si, se comparado com o que acontece em outros países que tenham outra forma de raciocínio.

Pontuou que a confiança pode ter um efeito colateral reverso; aqueles casos onde a parte técnica é bastante forte, mas alguém emprega alguma técnica de engenharia social, e o usuário que confia no atacante, acaba entregando a senha, por mais que internamente a parte técnica esteja resolvida, que é raro, mas de qualquer forma, assume-se essa questão.

Disse para a mesa que gostaria de saber se nas experiências profissionais, se essas questões mais culturais, elas tem sido perseguidas por parte dos usuários que mexem com questões de cibersegurança ou se isso ainda é uma coisa ainda mais dormente e que em algum momento vai se tornar mais relevante.

Coronel Ricardo Camelo (CDCiber – Centro de Defesa Cibernética – Exército Brasileiro): **respondeu** que o brasileiro confia rapidamente, o país é um continente e isso varia conforme a região, mas isso não é radicalmente diferente pelo país e tem efeitos prós e contras. Tem horas que a confiança excessiva e rápida demais faz com que caia em uma armadilha e, por outro lado, às vezes problemas mais difíceis são resolvidos rapidamente. Exemplificou também, que muitos problemas técnicos em grandes eventos como o RIO+20, puderam ser solucionados com o auxílio de outras pessoas, outros técnicos.

Ao mesmo tempo, disse que os brasileiros têm uma tendência de ser muito indisciplinados, exemplificou com um mito de que na guerra determinados grupos de combate permaneciam em sua posição porque tinham recebido uma ordem para tal e como a contraordem não veio, ficou ali e morreram, porque depois veio o bombardeio, veio alguma coisa assim e o soldado brasileiro: “pera aí, o que tá acontecendo? Vamos embora daqui!”. Tinham umas coisas assim, cômicas, mas de modo geral, o procedimento mais sistemático dá mais certo – pelo menos, estatisticamente falando. Disse que no centro mesmo, quando veio essa ordem, quando o chefe diz: “ninguém mais usa celular aqui”, tinham pessoas que não queriam aceitar porque ao se separar do celular, dá mais ou menos uns 15 minutos, a visão começa a ficar turva, as pernas começam a ficar bambas, tem que chamar o SAMU, então, virou um órgão vital. Concordou com o que o Marcos falou, por que certa empresa há 20 anos, mais ou menos, não se importava muito

com pirataria do sistema operacional dela e hoje se importa tanto? Pra criar o vício, pois ás vezes, largar um hábito é uma coisa muito difícil e os brasileiros tem esse lado meio indisciplinado, cultural, então, essa sensibilização precisa, de algumas coisas um pouco mais radicais que ninguém gosta. O painelista salientou que não considera certo, mas, forçar um pouco até que um novo referencial cultural se estabeleça é importante.

Exemplificou com uma reportagem que saiu no *The Washington Post* há uns 6, 7 anos, em que os comandantes, os principais de todos os comandos, os Estados Unidos, o Comando Sul, Atlântico, o Comandante *Cybernetic*, entre outros foram fazer um teste e, na época, os guerreiros cibernéticos americanos, do time do *NSA* e o *USA Cyber Command* passaram pela defesa das redes deles mesmos como se fosse uma piada! Até a autoridade do Pentágono que deu a entrevista comparou com a antiga linha *marginot* francesa na época da guerra em que se fechava a fronteira. Acredita que esse tipo de susto muitas vezes pode mudar a maneira de agir.

Marco Carnut (*Tempest Security Intelligence)***:** respondeu que acha a confiança uma sensação intuitiva, mais uma emoção do que uma coisa racional, então, primeira coisa que acha difícil é ter uma discussão racional a respeito de segurança porque os psiquiatras e os psicólogos ainda estão tentando definir que é segurança: é um atalho evolucionário pra se tomar decisões mais rápidas em que se usava a razão, alguma coisa da natureza humana. Portanto, quando tenta fazer análises de chegar àquela, que tinha falado pra definir bem o que é segurança, ele tenta evitar ao máximo possível usar esse termo confiança devido a sua nebulosidade.

Acredita, entretanto, que a confiança desempenha um papel muito importante e os aspectos culturais da confiança desempenham um papel também muito importante na vida prática devido, exatamente, a esses vieses. A confiança para o representante do setor empresarial é uma série de vieses, que podem ser explorados para o bem ou para o mal. Citou um alguns exemplos, muito se diz – mesmo não sendo em totalidade uma verdade - que aquele incidente do 11 de setembro poderia ter sido evitado se as diversas agências governamentais americanas conversassem mais entre si, então, houve uma ordem presidencial dos Estados Unidos que, na época do Bush, salvo seu engano, dizia: “Ok! Conversem entre si; vocês podem compartilhar a informação”, e eles criaram várias ferramentas, tecnologias e infraestruturas para compartilhar informação. Citou que uma delas foi uma grande Wiki, que virou a *Wikipedia* do pessoal da inteligência. Então, houve uma época em que essa *Wikipedia*, estimava 3 milhões de oficiais de inteligências militares que assinavam essa Wiki. Um deles, foi o Bradley Manning, que horrorizado com a quantidade de hipocrisia que ele viu naquela Wiki, copiou para um CD e mandou para a *WikiMix*. Então, o excesso de segurança e a resultante centralização da informação para fins de facilitar o compartilhamento viabilizaram um dos maiores vazamento de informação da história, que talvez não tivesse acontecido se a política fosse outra. Entende que, se por um lado o Coronel Camelo acha mais útil que haja um compartilhamento de informação – ele certamente conhece a dificuldade do trabalho dele – isso pode ser em certas situações uma faca de dois gumes.

O painelista disse que gostaria de ver uma melhoria de segurança nos setores das forças armadas e governamentais em relação, por exemplo, ao setor empresarial e até

acadêmico. Os acadêmicos parecem que tem uma fala melhor com o governo e com militares, e ele como representante do setor empresarial sente que o brasileiro não gosta do brasileiro. O brasileiro, frequentemente, prefere comprar produtos americanos do que comprar produtos de brasileiros, o que lhe parece um contrassenso porque é uma ótima maneira de se submeter a exonerabilidade do serviço dele.

Citou que talvez o representante do governo saiba informar, por exemplo, se existe algum roteador de Internet ou algoritmo genuinamente brasileiro nos roteadores desses que ele disse que custariam U$ 15 milhões para substituir os algoritmos, como no *backbones* das Forças Armadas, do Governo ou de outro lugar que ele conheça. Ele disse que apenas conhece a Internet toda feita de Cisco, *juniper* e awake.

Questionou como pode se falar em soberania se a tecnologia brasileira é subjacente das comunicações e de domínio tecnológico de outro país? E quando a indústria brasileira se levanta ao desafio de fornecer alternativas, o dinheiro frequentemente vai para o estrangeiro, não vai para o próprio brasileiro. Acha que o brasileiro fala muito em confiança, mas o brasileiro não confiar no brasileiro. Prefere-se comprar coisa do estrangeiro, citou como exemplo o lançamento de um celular brasileiro, em que as pessoas diriam: “ah, não, mas eu prefiro o iPhone da Apple”. Apostou que uma parte faria isso.

Portanto, em sua visão, é um fator cultural profundamente arraigado e que acha que coloca em detrimento a segurança no nível mais profundo. Arriscou, mesmo que tivesse o risco de parecer polêmico, a dizer que isso afeta até a soberania. Acha que, sem medo de exagerar, o Brasil não tem essa soberania que acha que tem, porque não tem o domínio tecnológico das coisas.

Disse que adoraria ver os produtos gerados pela academia, pela inteligência brasileira virarem produtos usados no mercado nacional, que fomentassem a economia nacional para se ter uma soberania de verdade baseada no domínio tecnológico, na sabedoria. Os americanos dominam o mundo economicamente, mas eles são os líderes, eles tem esse domínio econômico porque eles são os líderes em pesquisa, tecnologia e na aplicação da tecnologia deles. Eles dominam o mundo porque eles exportam os roteadores Cisco, *juniper* etc., porque muitos deles, por exemplo, foi recentemente revelado, já saem com o *backdoor* da NSA. A confiança tem esse viés, por isso conclui ser difícil falar em confiança, porque é um assunto psicológico e ele desperta paixões, um assunto que não é terrivelmente ameno numa abordagem fria e racional, mas sem dúvida alguma, esses vieses culturais afetam na prática, conforme os exemplos que citou.

Silvio Rhatto (Coletivo Saravá): **também respondeu aos apontamentos feitos por Lisandro Granville** dizendo estar de acordo com a dificuldade de definir o que é confiança. Entende que, ao confiar sem definir, e também confiar definindo sempre corre um risco, entretanto, tentou se arriscar e definir um pouco segurança.

Para ele a confiança é como costura do tecido social, colocou que viver em sociedade, querendo ou não, se faz necessário confiar; uma confiança no outro, então, sem essa possibilidade, a vida comum seria impossível. Agora, a confiança é mais do que isso

porque, colocar a confiança de se conviver com alguém, é diferente da confiança em uma pessoa para realizar uma neurocirurgia, por exemplo. A confiança precisa ser qualificada, se está falando em comunicação mediada por sistemas digitais, têm que ter, de repente, um recorte maior sobre o que seria confiar em um sistema, quais seriam os parâmetros, e nesse sentido, talvez, conseguisse ter um pouco mais de objetividade nisso ainda sendo uma tarefa muito difícil.

Pontuou que o que se sabe é que, intuitivamente, a confiança é mais difícil de conseguir do que é fácil perdê-la. Uma vez que a confiança é perdida, a sua retomada é muito complicada, isso se realmente ela ocorre. Colocou que existem também aspectos não só sociais, mas, sobretudo, aspectos políticos que vão influenciar na questão da confiança. Pode-se pensar sobre a questão da cultura brasileira, e fez uma pequena comparação, em que principalmente no meio ativista, se percebe que, por exemplo, os norte-americanos, os estadunidenses, principalmente, têm uma confiança; a noção de confiança deles é muito baseada na Constituição americana. Eles acreditam, confiam nos direitos que eles têm, principalmente na liberdade de expressão deles e, no entanto, eles sabem que o modelo de vigilância de massa estadunidense é baseado realmente na liberdade de expressão. A NSA quer que se comunique porque ela vai grampear tudo. Quer que as pessoas falem, por outro lado, na Alemanha, a comunidade viveu a experiência da êxtase. Essa noção da liberdade de expressão é um pouco mais relativizada, tanto é que, em alguns aspectos, a comunidade *hacker* alemã esteve muito a frente da estadunidense e isso de adotar padrões e, eventualmente, fazer com que a comunicação aparentemente não exista, então, percebeu um fechamento de grupos falando entre si – seria aquela espécie de *cripto* sindicato.

Citando outro exemplo extremo, falou que hoje em um lugar que acha talvez muito interessante de observar, é Cuba, uma nação que está entrando aos poucos na Internet e curiosamente a noção de privacidade é muito difusa, como se não existisse. As pessoas perguntam da vida umas das outras: nos padrões brasileiros, um se mete na vida do outro, mas essa é uma coisa vista com naturalidade; e o Brasil tem certa semelhança cultural – tem certa semelhança na composição étnica etc. – e a entrada para os brasileiros na Internet foi muito abrupta, não teve uma construção de privacidade que os estadunidenses tiveram ou uma perda de privacidade dos alemães. Acredita que é um momento muito novo para ver o que vai acontecer. Na visão dele, desde os escândalos do Snowden e até muito antes de coisas do *Wikileaks* que a sociedade começou, o público brasileiro começou a se interessar muito por essa questão; porém, existe uma dificuldade de perceber o impacto na vida, da perda de privacidade.

Disse que é possível falar que o brasileiro é cordial e que em 5 minutos já se torna amigo, mas vê que por outro lado, que o brasileiro também é malicioso. Então ele acha que o brasileiro também tem ferramentas de defesa, sendo necessário saber como é que se pode articular essas coisas sem ser muito enganado; porque a confiança é necessária e importante: precisa-se confiar um nos outros, acha que pode usar esse aspecto cultural e para além dele.

No aspecto político, Silvio acredita que uma questão básica é: tende-se a confiar nos pares, portanto, confia-se em quem está na mesma situação. Então é muito mais fácil, por

exemplo, quem está na mesma área empresarial, estabelecer um vínculo de confiança por enfrentar um concorrente em comum que vai quebrar o mercado ou ativistas políticos que tem um mesmo oponente em comum. É muito mais fácil estabelecer esses elos com o comum. Porém, estabelecer um elo com os rivais é uma coisa muito complicada, e então acaba-se criando protocolos; em que tenta fazer a confiança no protocolo assume que o rival vai, de qualquer maneira, tentar burlar o protocolo e passa à história da criptografia.

Assumiu que o canal de computação e de comunicação, estão completamente grampeados, com grampo ativo e grampo passivo, portanto ele é comprometido, um canal hostil de transmissão. Colocou que é necessário entender que nós não vivemos em sociedades de consenso e nem sempre de resolução de consenso. O conflito vai existir; entre os pares, é muito mais fácil estabelecer vínculos de confiança pela condição. Agora, as pessoas se relacionam, também, com rivais componentes, sendo necessário tentar chegar em acordo e para isso, ao seu ver, é necessário criar protocolos. Acha que o fórum é um lugar ideal, pois é multissetorial, então entende que nem sempre vai ter consenso; vão se formar naturalmente núcleos de interesse, mas a questão é que existem as condição de criar esses protocolos de confiança.

Paulo Sérgio Licciardi Messeder Barreto (Universidade de São Paulo - USP, São Paulo, São Paulo) fez uma breve observação em relação à questão cultural em que por um lado é necessário saber exatamente quem é o adversário contra quem se está querendo se proteger, e por outro lado, quem é o que pode ajudar nessa tarefa, nesse processo de estabelecer as proteções de acordo com aquilo que se está precisando. Pontuou que existe uma cultura de que no Brasil não se vai encontrar soluções, disse que que ouve isso de colegas pesquisadores, de ex-alunos. Exemplificou que durante a sua pós-graduação, ouviu que: “brasileiro não cria tecnologia”. E atualmente usa essa frase com os seus alunos como um contraexemplo: que quando alguém falar uma coisa dessas, é possível apontar diversos casos de tecnologia que são criadas no Brasil e adotadas no exterior.
Disse que há muitos casos em que quando uma tecnologia brasileira é adotada dentro do país é porque passou primeiro no exterior. Ele vê isso como uma questão cultural e sabe que não tem como se justificar tecnicamente, mesmo expondo todos os motivos. Perguntou, então, o porque dessa cultura brasileira? Acredita que é difícil de mudar, anos e anos, décadas e décadas, sem saber se essa cultura vai mudar, mas sabe que é necessário começar uma mudança.

Fez um complemento referente à fala do representante do terceiro setor, em especial uma frase que e já ouviu muitas vezes que é um fator cultural, e que gostaria de compartilhar isso com os participantes para que não caiam nessa armadilha. Entre os vieses culturais interessantes dos brasileiros, que conhece, escuta muito essa frase: nada é 100% seguro; não tem como resolver totalmente um problema. Do ponto de vista estritamente lógico, está na grande maioria dos exemplos, em 99,99% dos exemplos, acha que isso é verdade. Não se consegue ter segurança absoluta com qualquer coisa. Tem alguns indícios de que algumas coisas podem ser 100% seguras, por exemplo, acha que dá para afirmar, com 99,99% de chance, que algum dia irá morrer. Mas pode ser que mudem isso amanhã, pois para ele a tecnologia evolui. A segunda lei da termodinâmica não está muita

a favor, mas pode ser que achem alguma solução.

Citou que no Brasil se escuta muito essa frase de que nada é 100% seguro como uma justificativa para nem começar a tentar. Ressaltou que os participantes não devem cair nessa falácia, e que toda vez em que ouvirem: “ah, não vamos trabalhar nisso porque não dá para tornar tudo 100% seguro”, não aceitem essa posição, esse viés cultural.

Acredita ser possível, ter soluções de segurança extremamente eficientes, com custos e com razões de custo x benefício extremamente atraentes, em qualquer área da computação. Ainda não viu nenhuma área e nenhuma subárea de segurança em que não tenha sido possível chegar a esse ponto. Então sugere que não aceitem essa filosofia derrotista, de que isso é fator cultural terrível e que tem ouvido muito falar em diversas áreas de discussões na área de segurança e alertando a todos para não caírem nesta falácia.

Antônio Rodrigo *(Portal R, Bahia)* começou sua fala inteirando as questões de tecnologias de segurança nacionais, e afirmou que existem tecnologias nacionais extremamente eficazes, exemplificando que em Brasília tem planos-piloto excelentes e que podia até compartilhar com o representante do governo, quais códigos que podem ser implementados para dar a possibilidade de implementar o algoritmo, no código deles e, assim, montar uma estrutura mais concreta. Depois expôs que em relação a questão social; é a da imagética com relação à segurança: qual imagem representa a segurança? Para os diversos nichos que a segurança possa ter, como o representante do setor empresarial falou, a segurança hoje pode ser classificada em diversos fatores, diversos requisitos, ou diversas coisas e motivos.

O participante atualmente vislumbra nas redes sociais, pessoas extremamente voláteis, culturalmente, informações confusas e informações que não vem de fontes seguras. Para ele as pessoas assumem aquela posição referente a essas informações e posteriormente, mudam de opinião conforme a mídia vai sendo atualizada. Culturalmente, esse indivíduo não tem aquele senso de pesquisa, de busca de fonte segura para se atualizar. e em relação ao fator humano, dentro da empresa; o participante acredita que quando se fala de segurança, tratando todo o perímetro, porém com o fator humano, ele utiliza uma metáfora, se constrói um edifício, colocando moradores, agente de portaria, segurança, câmeras de segurança, sensores de presença, e no final das contas, o morador libera o acesso de uma pessoa e ele acaba fazendo a bagunça no condomínio.

Para Antônio o princípio da segurança é o esclarecimento da política interna da empresa ou da organização, para os colaboradores; o esclarecimento da política, treinamentos contínuos referentes à política de segurança, ao que está acontecendo hoje na Internet; as vulnerabilidades; como eles devem agir. Porque a partir do momento em que cercam-se os perímetros e não educam os colaboradores e os participantes daquela cultura, a acaba se deixando o fator essencial da segurança à parte. E tudo isso reflete na imagética, naquilo que se vê, naquilo que se ouve, no que se traz.

Exemplificou casos da pessoa trazer procedimentos para dentro da empresa porque um professor da faculdade ou um colega da faculdade falou que aquilo era o correto, sendo que a empresa já tinha as suas políticas aplicadas e todos os procedimentos eram documentados. Então não tinha o por quê da pessoa trazer aquilo. Disse que essa questão da imagética, da questão da imagem em si, uma frase, uma letra, uma imagem, o que a mídia passa para as redes sociais, a cultura, em geral, do Brasil – falando em especial do Nordeste porque há povoados bem remotos, em que a cultura não está, ainda, tão acessível, a cultura da tecnologia e do uso adequado da tecnologia e como se pode difundir isso no fator humano: cria-se o perímetro e deve proteger todo perímetro, mas diversas oportunidades e ele disse que já teve que ver as falhas vieram de dentro, e não de fora; e o que saiu, saiu de dentro pra fora e não de fora pra dentro.

Quase nunca de fora pra dentro, sempre de dentro pra fora. Então, pediu que os painelistas que fizessem uma abordagem geral dessa questão, se foi bem compreendida e agradeceu a oportunidade.

Daniel Araújo *(Serviços Geológicos do Brasil, Natal, Rio Grande do Norte)* iniciou comentando que os brasileiros confiam muito mal e que se parar para analisar a quantidade de sites, *websites*, relativamente grandes, fóruns ou mesmo serviços no Brasil, que usam senha em *play test*, é muito grande a quantidade. Isso é parte da cultura porque, a pessoa leva isso para as empresas e as implanta.

Em relação a questão da tecnologia disse que é possível criar tecnologia aqui no Brasil; só que isso se passa principalmente pelo governo. Enquanto brasileiro, existe muita dependência das políticas governamentais. E apontou como maior prova disso a banca da trilha 3, que entre quatro pessoas, pelo menos três delas fazem parte de universidades. Questionou se isso é muito ruim, pois ao começar a analisar os institutos de pesquisa no Brasil, qual é o maior? Petrobras, que pertence ao governo; segundo maior: as universidades como um todo – USP, UFRJ, UFRN e a UFBA; a quarta maior: IBM, que é privada, já não é do Brasil. E isso é extremamente complicado no Brasil porque a formação da mão de obra também se passa pelo governo; o governo tem que sentar e dizer: “olha, a gente está preocupado com defesa cibernética e tem que formar mão de obra”.

Disse que há pessoas que prestam serviços ao Exército; um deles é o tio do participante que é da Universidade de Brasília, inclusive, e veem pouquíssimas pessoas como ele atuando diretamente na área de cibersegurança, que fica restrita ao governo; para ele as empresas não estão muito preocupadas, não se importam muito com isso.

Falou que na questão de fomento, que também vem do governo: criar *hardware*, *software*, demanda dinheiro. E se fosse *open source*, por mais bonita que seja a ideia, não consegue viver isso, pois tem contas para pagar e tudo o mais, então caso alguém vá no Banco Nacional de Desenvolvimento (BNDES) e diz que pretende criar uma fábrica de roteadores para concorrer com a Cisco, não vão dar o dinheiro, porque se trata de um zé ninguém, porém se fosse o Eike Batista, com a ideia do OGX, iria mudar. Mas um zé ninguém o governo não vai querer incentivar.

E na questão de mão de obra, fez a seguinte pergunta: se houvesse uma guerra cibernética, o Brasil estaria preparado? Utilizou como exemplo a Coréia do Norte que é um país extremamente fechado, mas ocasionalmente, vasam algumas informações de lá. E as informações que visam de lá, os *hackers* de lá vivem como funcionários públicos de alto nível; eles são extremamente bem pagos –não sabe como é o sistema no país – mas eles são privilegiados. Aqui no Brasil não se vê nada disso. Por fim, perguntou se o Brasil tem mão de obra e como pode reverter esse cenário?

Coronel Ricardo Camelo (CDCiber – Centro de Defesa Cibernética – Exército Brasileiro): **iniciou sua resposta para o Daniel** explicando que se todos olharem para trás 100% do histórico conhecido e que poderia ser relacionado a atos e guerra cibernética, nenhum deles foi assumido. Sabe-se da capacidade dos demais países, que podem paralisar um país inteiro paralisação de radares para que a defesa do país levantasse voo enquanto a outra força aérea entrava e destruía instalações que supostamente estavam sendo construídas base nuclear, apagões de áreas enormes dentro da maior potência mundial, projetos roubados dessa mesma potência, entre outros.

Para ele é complicado conceituar a questão de guerra. Ao mesmo tempo, a questão é tão grave que até esses grandes *players* reconhecem que não podem deixar a coisa solta e acabam todos indo para a mesma mesa e discutindo "como é que vai disciplinar isso". Então para ele é muito relativa à questão de guerra.

Acredita que o Brasil é um país que reflete isso, pois há muitas redes com graus de maturidade muito diferenciados – e provavelmente a maioria, não tão maduros – então é muito fácil provocar efeitos que o militar chama de cinéticos, com pouco esforço. Isso é terrível para o país. Mas parece que não é também tão interessante provocar colapsos uns nos outros – até porque estão todos ligados, portanto se um cai todos vão.

Acha uma ótima pergunta que não tem uma ótima resposta, a não ser que a seja bem acadêmico e delimite bem o escopo de como se abordaria caso atacassem as infraestruturas críticas, se fizesse tal coisa; poderia ter várias possíveis respostas, mas até o próprio pressuposto fica comprometido.

Manoelito C. Neves Filho *(Raul Hacker Club, Salvador, Bahia):* discordou que é possível viver de *software* livre sim e focou sua pergunta na área de segurança. Citou a fala do Silvio Rhatto, em relação ao aclamado Marco Civil e o polêmico artigo 13 e 15, que é um tanto quanto anticonstitucional quando ele fere a presunção à inocência; ele obriga que os provedores guardem registros dos usuários – o que não acontece quando se faz uma ligação: a voz não está gravada pela operadora porque, teoricamente, o individuo é inocente, a não ser que tenha um indício de que esteja cometendo algum ato ilícito, e aquilo vai começar a ser grampeado.

Disse que quando se trata da segurança da informação como um todo, sabe-se que esses dados podem não estar seguros e essas informações podem estar vazando de forma não oficial. Perguntou aos painelistas como veem essa relação? Exemplificou com a Alemanha que partiu desse pressuposto e quis fazer um encaminhamento para o CGI.br, pois falaram que há um setor de estatística, no CGI.br, portanto quer fazer um

encaminhamento para que os dados de crimes cibernéticos – deixando claro ser contra crimes cibernéticos – mas que os dados de crimes cibernéticos sejam cruzados com as informações que estão sendo estocadas, porque é perigosíssimo estar gravando dados, ferindo a presunção da inocência, indo contra a Constituição, sem a devida segurança de que estes dados estão realmente resguardados.

Perguntou, por fim, se os painelistas poderiam explicar como lidam com isso, uma vez que a Alemanha voltou atrás, após entrar com esse tipo de modelo, viu, estatisticamente – são realidades diferentes, óbvio, pois não sabe se o criminoso de lá tem o mesmo conhecimento de *Virtual Private Network* (VPN) em criptografia e questionou como lidam com isso.

Marco Carnut (*Tempest Security Intelligence)* **respondeu ao Manoelito C. Neves Filho** que acha interessante inicialmente fazer alguns esclarecimentos, dando sua opinião pessoal de que não curte a história de retenção de dados. Tendo dito isso, disse que é preciso entender que vive-se em sociedade, inevitavelmente vivendo essas coisas.

Falou que não é advogado, sugerindo que o participante fale diretamente com um, mas citou como exemplo, a presunção da inocência só existe no Direito Criminal, não existe no Direito Civil, no Direito Administrativo. Portanto, quando se está gravando, quando está colocando esses registros do que fez no provedor, não necessariamente conflita com esse conceito de que está violando a presunção de inocência, porque a pessoa não foi acusada de um crime.

Disse estar ecoando o que os profissionais de direito lhe ensinaram. Contou que uma vez chegou para alguns profissionais de Direito e levou duas ou três bordoadas justamente por causa disso, então, está falando da possibilidade de que, quando for conversar com eles, pode levar uma bordoada também, porque o pessoal de Direito não entende desse jeito que o participante está entendendo. Eles entendem que a presunção de inocência –é circunscrita a um processo criminal, então, essa é uma questão.

Seu segundo esclarecimento foi sobre a coleta que tem no Marco Civil, que já existe por razões de *Billing* nos provedores. Os provedores já registram o endereço de IP, quem ligou ou quem efetuou *login*, na hora em que conectou, que hora desconectou e, por razões de *Billing*, tem que ter. Concorda com o participante que é extremamente frágil. Os provedores são *hackeados* como qual, e eles não entendem tanto assim de segurança como quase qualquer outra empresa; eles estão preocupados com outras coisas.

Já ouviu de vários provedores que "segurança não é o *business*, *business* é conectividade". Perguntou se é um problema sério? E respondeu que sim!

Citou que as autoridades investigativas precisam ser capazes de rastrear pessoas que cometem crimes. Disse ter um conjunto de opiniões políticas que se alinham mais com a questão libertária; e também que gostaria de viver num mundo onde fosse viável não ter a necessidade de ter esse tipo de registro registrado, gravado e mantido, disse que gostaria de viver nesse mundo, mas esse mundo está longe de acontecer e existem outras forças na sociedade, igualmente legítimas, das autoridades investigativas, que precisam ser

capazes de correlacionar, precisam saber quem foi que fez a pedofilia infantil de determinada criança e pra ele isso é tão legítimo quanto qualquer uma.

Então, acha que o Marco Civil não é perfeito e gostaria que ele fosse diferente, mas pelo menos foi o consenso até agora que a sociedade conseguiu chegar em relação a essa questão, portanto apesar de não ser perfeito, acredita foi o melhor que conseguiu ser feito.

Pontuou que não existem mecanismos na sociedade para mudá-lo se necessário. Por outro lado, todos vivem em uma época extraordinária. Citou, como exemplo, a criptografia, que permite comunicar com alguma garantia de segurança em alguns canais inseguros. Sugeriu ao participante que caso ele esteja chateado com esse negócio instale o TOR, para que aprenda sobre criptografia e inutilize essa infraestrutura que está dentro do poder do usuário e da usuária.

Disse que isso vai dar outra briga: tentar criminalizar a criptografia como David Cameron está tentando fazer no Reino Unido; e todos enquanto sociedade, precisam dar um basta nesse negócio. Não se pode deixar que a criptografia seja criminaliza.

Finalizou dizendo que gostou da abordagem do participante, que aparenta tão jovem estar antenado nessas coisas e acha isso absolutamente sensacional, mas o que pode dizer a ele é: a vida política na sociedade é um pouco mais complicada, um pouco mais cheia de usuários e usuárias como ele, e que existem outros segmentos tão legítimos quanto. O que pode fazer é lançar mão dessas tecnologias pra tentar contra balancear o que se percebe como sendo uma desvantagem.

Manoelito C. Neves Filho *(Raul Hacker Club, Salvador, Bahia):* disse que a respeito da questão que ele comentou da guarda que a companhia telefônica não guarda voz. Pontuou que o Marco Civil também não está pedindo para guardar a navegação que a pessoa está fazendo, só a informação de que horas a que horas se conectou e qual era o usuário dela, da mesma forma que as companhias telefônicas também guardam o horário que ligou e em qual número.

Marco Carnut (*Tempest Security Intelligence):* disse *a*o **Paulo Sérgio**, que ele pode e consegue ver que tem uma tremenda discussão e muita pesquisa mostrando que somente os dados de quem fala com quem, de criptografia, chama-se análise tráfego, e só de análise tráfego dá para saber muito a respeito dos hábitos de uma pessoa, que aliás, já é sobre uma certa métrica, uma invasão de privacidade.

Silvio Rhatto *(Coletivo Saravá):* **respondeu ao Manoelito C. Neves Filho** que a análise de tráfego ganhou muito destaque nos últimos anos, especialmente porque ela é barata. Analisar conteúdo é muito difícil, requer algoritmos muito sofisticados e muito processamento, de modo que se tem hoje uma tendência a observar uma preferência pela investigação baseada em metadados.

Exemplificou que se alguém quer saber em uma investigação quais os números de telefone que gostaria de grampear para fechar uma rede social e estabelecer o

organograma de uma organização.

Disse ser contra os artigos 3 e 15, do Marco Civil da Internet, e que durante toda a evolução do Marco Civil e nas legislações anteriores sempre foi contra. Acha que, primeiro tem essa lição da escalada: quem realmente for praticar um crime, provavelmente vai se proteger, já sabe usar o TOR, ou acredita-se que o terrorista vai usar um e-mail comercial qualquer para se comunicar ou se preparar?

Disse que seu ponto é que quem vai se dar mal é quem não tem acesso às tecnologias de criptografia, roteamento e anonimato. Acha que uma das grandes ligações que se tem que fazer agora, que é aonde pode, um dos caminhos pro Marco Civil é tentar fazer alguma coisa na regulação dele, uma outra ligação que pode estabelecer com projetos de lei de proteção de dados pessoais, a que vai lidar justamente com a segurança dessa informação coletada.

Citou que apenas o artigo 13 fala sobre o acesso à Internet, mas os provedores de conteúdo com fins lucrativos, são obrigados a registrar o horário e os metadados de acesso. Disse que há um recurso na *web*, que pode ser um blog, pode ser uma rede social ou outras coisas. Apenas os provedores sem fins lucrativos estão isentos desse registro, ou seja, a *priori* deve-se registrar os metadados de acesso.

Disse fazer parte de um grupo sem fins lucrativos que tem operação no Brasil, provedores de conteúdo e que estão isentos, desde que começou a existir o Saravá, há dez anos, nunca registrou número *IP* – só em pequenos momentos para fazer alguma coisa, algum tipo de teste, para consertar seus sistemas.

Falou que é uma regra pétrea interna do Saravá, que sempre esteve disposto a lutar até o fim para garantir isso, pois eles não tem interesse em saber quem acessa ou quem usa o sistema. Disse que esse tipo de vínculo de confiança se obtém de outra forma e acha que essas duas provisões do Marco Civil escondem às vezes uma incapacidade das organizações de lidarem com sua própria segurança interna e isso acaba gerando uma necessidade de um remendo jurídico que acaba servindo para se isentar da sua responsabilidade de consertar seus sistemas.

Por fim, declarou achar que esses artigos a longo prazo são inócuos e se a tendência continuar, os próximos sistemas a serem criminalizados são os de comunicação anônima.

Marco Carnut *(Tempest Security Intelligence):* **perguntou ao Silvio Rhatto** se o Marco Civil diz que não precisa registrar os metadados se for uma "coisa" sem fins lucrativos?

Silvio Rhatto *(Coletivo Saravá):* **respondeu ao Marco Carnut** que a *priori* sim ou seja, havendo indício de um crime, um dano até no Código Civil, a autoridade policial ou investigadora pode solicitar que o provedor, mesmo sem fins lucrativos, inicie o processo de registro, apenas para normalizar.

Disse que a saída da rede Tor é um ponto de contato entre uma rede que implementa um pseudo anonimato, um anonimato com a Internet do lado de fora. Logar todos os *IP's* de

saída da rede Tor, efetivamente é inócuo porque assume-se que, ao sair da rede Tor, a origem daquela comunicação já está 'anonimizada'. Então isso não seria realmente um perigo, nesse sentido. Acha que seria muito mais fácil acontecer de esse nó da rede Tor não ser bem configurado, acabar sendo mau usado e um provedor, ou então alguém, resolver processar a organização que roda o modo de saída.

Citou que o modo de saída da rede Tor realmente não é uma coisa fácil, existem muitos desafios jurídicos e operacionais, mas acha que, por exemplo, se o computador tem um problema – ele é invadido – e ele começa a ser usado a partir da rede doméstica para fazer todo o tipo de besteira. O IP já está registrado em tudo quanto é provedor; imagina o tipo de problema que será enfrentado pelo usuário e pela usuária que escolheu um fabricante que não se preocupa com isso, confia em uma legislação que vai proteger, em termos de uso que vai proteger, portanto, disse ver nesse sentido a ineficácia e o quanto é prejudicial para todos.

Pontuou também outro aspecto que não se sabe o que se pode ser feito com esse tipo de informação, se no futuro tiver algum regime de governo mais draconiano, o que ele pode fazer desse tipo de tecnologia para rastrear as pessoas e para, não exatamente ir atrás de todo mundo. Citou que vigilância de massa ela é automática, a guarda dos registros é automática, agora, o monopólio da violência é limitado, porém, se consegue criar um clima de terror e medo – que foi justamente esse clima da guerra ao terror – e esse clima mina a confiança que se tem nos sistemas, a confiança que se tem na liberdade de expressão, e isso vai minando o tecido social, ou seja, às vezes é uma consequência direta dessas medidas todos se comunicam menos, tendo muito receio do que quer e do que pode falar.

Sugeriu que é necessário verificar outras formas de combater crimes como pedofilia, por exemplo, e que acha que vai ser inócuo o Marco Civil nesse sentido que só tem como prejudicar. Pensa que o que se pode fazer hoje, como redução de danos, se no futuro a não conseguir revogar esses dois artigos, pelo menos, prestar muita atenção na regulação, na regulamentação do Marco Civil para especificar exatamente o que são esses metadados. Do que se está falando? Está falando de data, número IP e recurso? Ou de outras coisas? Essa definição de metadados também é muito complexa.

Ao mesmo tempo, disse que é preciso prestar atenção no anteprojeto de lei de proteção de dados pessoais que isso é uma coisa que acha muito mais bombástica porque vai em um restaurante, registrasse dados pessoais, vai em um evento e registrasse dados pessoas que ficam armazenados e não se sabe que tipo de base de dados, se ficam, se vazam ou não vazam. Pensar que privacidade não é uma construção individual, não protege a privacidade de ninguém, porque seria viver em um mundo fechado, sendo que todos vivem em um mundo aberto, onde as pessoas fornecem informações pessoais.

Exemplificou, que alguém pode revelar seu endereço, seu número de telefone, e ainda mais isso vai ficando mais perigoso com a interoperabilidade das bases de dados. Se no Marco Civil teve um *lobby* muito forte ao lado da privacidade que contou, inclusive, com grandes empresas de Internet estrangeiras que queriam menos problemas jurídicos para elas, o cenário fica muito pior na questão da proteção de dados pessoais porque não vai

conseguir ter grandes atores do lado da sociedade, já que as empresas de Internet hoje vivem dos dados pessoais de usuárias e usuários, bem como monetizam esses dados. Vai ser um desafio muito mais complicado. Então tem que prestar atenção não só no Artigo 13 e 15, mas também em alguma legislação à proteção de dados pessoais.

Coronel Ricardo Camelo *(CDCiber - Centro de Defesa Cibernética - Exército Brasileiro):* **comentou a fala do Manoelito C. Neves Filho** com relação à aplicação do Marco Civil, relembrando que fez o comentário fórum passado e que uma das coisas que tem feito área militar em relação a defesa cibernética, segurança cibernética etc., estabeleceram uma política própria de defesa, dentro da Estratégia Nacional de Defesa, e foram descendo as normas até a parte que chamam de Tática Último Estágio, que ainda está em andamento, para terem referências.

Citou que aquele ensinamento básico da administração: quem não consegue medir, não consegue gerenciar. Isso não significa controlar; controlar no sentido pejorativo da palavra. Exemplificou que em outros países tem a Política Nacional de Segurança Cibernética, que é o grande chapéu em que vai desdobrando para baixo tudo o que é necessário. Disse, ainda que em relação Marco Civil, é uma lei, que recebe como missão, independente da opinião específica a respeito, e que teve pelo menos uma satisfação inicial com relação a estar fazendo alguma coisa, começando a rodar o ciclo de evolução, porque antes era terra de ninguém, era nada.

Disse que o surgimento de polêmica em especial desses artigos, que os usuários e usuárias devem gritar se está errado, está certo, quais são os argumentos, pois não é uma questão trivial. Se for pensar apenas no sentido técnico, como por exemplo, a parte de forense, a parte investigativa. Confessou que há situações que "até Deus duvida" quando se trabalha na defesa e trabalha-se com computação e que se não houver capacidade de processamento ou de armazenamento de dados, não se conseguirá responsabilizar, atribuir responsabilidade e terá problemas insolúveis.

Ele acredita que o profissional não vai deixar rastros e colocaria a culpa em outro indivíduo que não tem nada a ver com a história. E disso não há como a polícia fazer uma investigação forense para avaliar. Disse que quando há 200 problemas ao mesmo tempo não se sabe por onde começar e faz o que é possível. **Concordou com Vitor** que não há cabimento por diversos motivos e isso faz parte da evolução como sociedade brasileira. **Respondendo ao Silvio**, acredita que é importante a princípio que seja equilibrada em todos os sentidos. Por isso, há de se ouvir a área policial, militar, sociedade civil, comercial e "ficar de olho" nos estrangeiros sem necessariamente vê-los como inimigos, mas tentar descobrir a melhor maneira.

Disse acreditar que não existe melhor maneira, questionou o motivo de existir diversos “se não” na área. Explicou que acredita existirem melhorias sucessivas no modelo e para os técnicos existe ansiedade para encontrar uma solução que as vezes estava "na frente dos olhos". Ressaltou que também é problemático quando tem que ter uma solução que se aplica a um país inteiro, de tamanho continental. Aí então a característica de caminhar um pouco mais lentamente que outros países. Acredita que estão todos de parabéns e há de ser ativo e gritar, para que fique claro. Finalizou apontando que é necessário resolver,

mas é importante ter cuidado para encontrar um meio termo.

Everton (*Universidade Federal do Alagoas*): iniciou sua fala esclarecendo que algum painelista citou que com o *software* livre não era possível ser vivido, pela questão de ter que pagar as contas. Disse que ao referenciar o *free* do software é livre como em liberdade, e não que seja gratuito. Porque a palavra "*free*", traduzida para o português ou em outros idiomas, também, pode ter dois significados: 1. livre, ou a questão 2. do gratuito, e gera essa confusão. Além disso, perguntou ao representante do terceiro setor se tem trabalhado com soluções de *software* livre e se as soluções tem atendido às necessidades dos seus clientes.

Silvio Rhatto (*Coletivo Saravá):* **respondeu ao Everton** que só usa *software* livre e que *software* livre é um pressuposto, não só pela liberdade de executá-lo, de estudá-lo, de modificá-lo e distribuí-lo, mas acha que com a questão da segurança se usa essas liberdades do *software* para também poder verificar se tem problema de segurança e sabe que o *software* livre não é necessariamente invulnerável por ser livre, porém a dinâmica de correção de vulnerabilidades é muito mais saudável no *software* livre.

Everton disse que quis falar de *software* livre, em uma questão da confiança, pois consegue revisar o código, sabendo das vulnerabilidades existentes a partir de uma visão simples. Logicamente que uma pessoa técnica faça isso.

Silvio Rhatto *(Coletivo Saravá):* respondeu ao **Everton** que para mexer nos códigos requer conhecimento. E disse que existem percalços – mesmo no *software* livre – e acha que não deve-se por conta disso desacreditar o *software* livre; para ele é um pressuposto.

Disse que é muito difícil construir segurança e confiança sem *software* livre, porque vai estar lidando com coisas que não tem como, de alguma forma, testar essa confiança. Exemplificou com o caso do *Open SSL*, que é uma suíte de criptografia mais usada. Falou que é um código muito velho, desenvolvido por pouca gente com pouco financiamento e assim, praticamente é a base da criptografia cotidiana. Acha super curioso que *bugs* de vulnerabilidade de segurança como *heartbleed* foram quase que por acaso descobertos – e vulnerabilidades que estavam ali há muito tempo - acha que o *heartbleed* estava ali desde 2009.

Portanto, entende que não é uma garantia de segurança, mas é um caminho. Falou que é necessário se preocupar especialmente com os *softwares* críticos de segurança que sejam livres ou abertos, que eles tenham uma equipe de desenvolvimento saudável, com uma certa sustentabilidade, que haja algum tipo de auditoria. Tem que garantir que não é o que acontece em todas as situações. Citou como exemplo um outro *software* que é crucial para segurança, um navegador que de mês em mês se vê alertas de segurança escabrosos nos navegadores.

Acredita que fazer uma auditoria de segurança não é fácil porque uma vulnerabilidade às vezes é expressa por um caractere no código. Para ele é um trabalho ingrato, mas precisa ser feito; com a quantidade de códigos existentes hoje é impossível fazer uma varredura atípica, existem várias técnicas de teste automatizados de *softwares*, portanto,

acredita que é necessário garantir que as comunidades tenham essa saúde mínima, uma questão de sustentabilidade, etc.

Citou que que no caso no *SSL*, é muito curioso porque todos usam; não apenas o terceiro setor, como o participante expôs. Acha que o espectro aqui e que todos usam, e curiosamente, o modelo do *Open SSL* é insustentável. Acha isso um problema bizarro, um absurdo se vive e é *software* livre aberto. Entretanto, colocou que um mundo proprietário é muito pior, porque eles não vão revelar, não se tem a possibilidade de procurar esses *bugs*.

Concluiu que no *software* livre/aberto o usuário e a usuária é mais soberano (a) porque consegue controlar. Pontuou que ainda há um problema de organização, mas que se pode melhorar porque tem esse poder no *software* livre. E acha que é por esse caminho que se consegue as implementações de referência, acha que tudo deveria ser baseado em *software* livre e acredita plenamente nisso por questões ideais, políticas, mas também por questões práticas de segurança. Para ele o pilar do que chama de soberania computacional é baseado, basicamente, em *software* livre com segurança e resiliência.

Marco Carnut (*Tempest Security Intelligence)* **respondeu ao Everton** que para ele o buraco é bem mais embaixo. Por exemplo, diz ter certeza absoluta que o representante do terceiro setor faz uma força para usar principalmente *software* livre no sistema dele, mas ele não usa só *software* livre; ele usa força proprietária. Provavelmente a BIOS (basic input/output system) dele é proprietária.

Disse que não se tem acesso ao *software*, mas que há um projeto que está tentando fazer uma BIOS não proprietária, mas ainda não está suficientemente funcional. Agora inventaram as BIOS UEFI (Unified Extensible Firmware Interface), que é outro sistema operacional dentro da máquina e tem toda uma área dentro de pesquisa e segurança de troianos e *backdoors* para BIOS UEFI, que é um *software* proprietário, que também no notebook Linux roda uma versão especial do Linux, que tem uma série de containers de alta segurança etc., mas prossegue vulnerável pela BIOS UEFI.

Falou que tentou desabilitar, mas que é bem complexo e exemplificou que se tem no seu computador uma placa de rede *gigabyte* de Internet, um fato pouco conhecido é que as placas de rede *gigabyte* de internet são um computador completo. Para fazer o processamento em velocidade *gigabyte*, rodar com a arquitetura normal do computador, eles colocaram essas funcionalidades num processador separado da placa de *gigabyte*. Ele tem um processador com *RAM* própria, com sistema operacional próprio, proprietário, que não se sabe qual é. Então existe, por exemplo, onde as pessoas aprenderam a "desassemelhar" esses *softwares* proprietário e colocaram *backdoors* dentro da sua placa de rede *gigabyte*. Portanto, pode-se ter o Linux mais seguro do universo, e ainda assim a máquina pode estar sendo rastreada sem saber. Dá para deletar pelos *logfiles* de perímetros, tem como saber, mas considera complicado.

Vislumbrou que um outro problema quando as pessoas dizem: "ah não, a gente está fazendo uma força danada para fazer *software* livre", não está fazendo nem metade do que deveria. Há toda uma fronteira inexplorada e o *software* proprietário muito à frente da

em termos de *know-how*, em termos de poder econômico. Outra coisa que também quis deixar claro é que o *software* livre não é só sobre copiar e fazer as coisas funcionares, etc. e poder compartilhar o *software* a um custo baixo e disponibilizar o código, é sobre ter *know-how*, entender o código.

Concluiu que se tem um *software* livre, não é capaz de alterá-lo para fazer o que ele quer ou tirar as vulnerabilidades que lhe incomodam, está apenas sendo vítima da mão de outra pessoa. Para ele o *software* livre é uma coisa cultural e que o entristece profundamente, disse que corre risco de talvez gerar uma inimizade com a academia, e adoraria que, uma das coisas que acha que o Brasil precisa é fazer com que aquele trabalhinho de faculdade de Ciências da Computação que faz de lista ligada ao invés dele só servir para satisfazer o professor e dar uma nota, que fosse publicado no Github, para outras gerações de pessoas se aproveitarem daquele código que foi feito.

Gostaria de ver *softwares* livres sendo praticados desde o ensino universitário. E acha que exceções são necessárias, porque ás vezes tem algumas coisas que tem interesse comercial e tudo mais. Mas se fizesse isso seria criada uma cultura do *software* livre. O *know-how*, de publicar o código, de compartilhar o código, de ter o ciclo de vida do *software* livre, acha que está faltando no Brasil.

E outra coisa que gostaria de ver e que colide com isto que está falando é se já não tem muito *know-how* de escrever o código e entender as vulnerabilidades, e aproveitou para fazer uma pergunta ao representante da academia, se há cursos universitários, em que segurança seja uma disciplina do currículo? Pois disse que conhece muito poucos cursos universitários em que a programação segura ou histórico das vulnerabilidades, caem em provas. Disse que não se vê *heartbleed* numa prova de Redes, de curso de Redes.

Citou Stallman e que uma de suas frases mais legais é: “você tem que controlar o computador, e não o contrário.” Hoje, a informática está sendo usada como outra maneira de manipular as pessoas, outra forma de poder, outras pessoas chamam de quinto ou sexto poder; tem os três poderes convencionais, o quarto poder é o de imprensa, o quinto tem vários *contenders* e o sexto poder é o poder da informática como meio de dominação da massa.

Coronel Ricardo Camelo *(CDCiber - Centro de Defesa Cibernética - Exército Brasileiro):* **comentou que** o aproveitamento de soluções brasileiras, bem como as possibilidades de sistema de como isso é, acredita ser uma questão complicada por depender de burocracias infinitas do governo. Acha muito difícil um empresário brasileiro ter a solução e citou que o Centro de Defesa Cibernética, embora não seja a solução disso, tem trabalhado muito forte nessa área também, fomentando e em alguns casos até financiando trabalhos científicos a respeito ou gerando parcerias por conta da burocracia complicadíssima.

Pontuou que o Brasil tem uma das principais soluções do mundo em infraestrutura de equipamentos de inter-redes, justamente soluções do país e do irmão do norte que muito provavelmente vem abençoadas, inclusive por lei deles, disse que há uma empresa no Brasil que faz esse tipo de ativo, que é estratégico e precisa ser apoiada e outras

precisam surgir.

Citou que acompanhou uma empresa em Brasília com um tipo de solução que tecnicamente é muito complexa: o *firon*. Mas muitas vezes muitas vezes uma escolhem-se soluções estrangeiras por ser mais madura.

Disse que sozinho, apenas com o CDCiber não se consegue melhorar, mas que com conversas e discussões possa despertar interesses. Afirmou que existem muita coisa no Brasil e que muitas vezes estão isoladas e que está tentando descobrir para quem pedir ajuda, portanto fez um convite a todos que se conhecerem alguém que tenha um projeto, procurar o CDCiber, para que vá para frente.

Ricardo *(Faculdade Estácio - Rio de Janeiro):* iniciou falando que em muitos países, como os EUA, quando um *hacker* consegue invadir um sistema do governo, o *Federal Bureau of Investigation* (FBI) é acionado e quando a pessoa for descoberta, ela é punida, mas procura-se aproveitá-la. E preguntou ao representante do setor governamental como são aproveitados esses jovens *hackers* no Brasil? São simplesmente punidos ou se também procuram aproveitá-los e fazer com que o mal que ele fez seja aproveitado para o bem da sociedade?

Coronel Ricardo Camelo *(CDCiber - Centro de Defesa Cibernética - Exército Brasileiro):* **respondeu ao Ricardo** que iniciou sua resposta com um exemplo clássico, o Kevin Mitnick, um dos mais antigos *hackers* que fez, para o painelista sucesso e lembra de seu julgamento dele e da frase do repórter quando ele saiu condenado e passa pelo técnico da IBM que ajudou o FBI a cassá-lo: o gênio do mal nesse momento passa pelo gênio do bem.

Acha que apesar de questionável, uma série de possibilidades que tem de enxergar esse tipo de aproveitamento, porque tem um lado do terreno afetivo que é totalmente incontrolável. Como que são as referências morais dessa pessoa? Isso não significa que qualquer *hacker* tem referências morais deterioradas; mas quer dizer que alguém que já tem um histórico criminal passa a “ser do bem”. Por que o pragmatismo? O cara tem uma competência: precisa-se disso e ele diz: “escuta, você trabalha pra mim e eu te atenuo a pena, fico te monitorando e você faz o que eu quero com essa competência”. Acha muito prático, mas necessária uma legislação para apoiar isso e a questão cultural. Acredita que nesse aspecto, culturalmente não se tem isso muito claro; não se vê aquele que cometeu um delito como alguém que não serve mais para nada.

Citou que ocorreu no Exército algo semelhante, só que não foi um crime. Um Tenente no início da carreira, de curioso, derrubou uma rede de um dos principais centros de comando e controle. Esse ato era suficiente para puni-lo porque ele inviabilizou grande parte do serviço do quartel. O Comandante averiguou e viu que tinha sido, como ele era reconhecidamente um *nerd* e apaixonado por essa área, viu que foi um incidente, não foi uma atitude proposital, colocou ele na pós-graduação imediatamente, nessa área. E ele foi por um bom tempo, infelizmente ele tomou um outro rumo na vida, mas enquanto ele era das forças armadas, foi um elemento que fez muita diferença nessa área.

Acredita ser uma questão complexa o como controlar essas pessoas que denominou monstrinhos, no sentido de terem um capacidade gigantescas de fazerem coisas para que ele fique polarizado e produzindo para a empresa, para a instituição, para o país; isso é uma questão complexa, não é uma solução simples.

Acha que em todos os níveis decisórios, não necessariamente nas forças armadas, parte-se de uma premissa mais relativa à área policial, e não à área de defesa, que se pode fazer uma analogia com relativa facilidade, acha que há como se aproveitar sim, se os decisores tiverem atenção para a questão. Não deixar o fruto apodrecer para ver se dá, se não dá, se confia. Mas se houver o reconhecimento do talento, ainda que aconteça um efeito colateral, como se chama nas forças armadas, de uma experiência ou de um ato qualquer cibernético, que acabe num primeiro momento gerando prejuízos, como exemplificou desse tenente, aproveitá-lo sim.

Pensa que esses talentos tem que ser cultivados e tem que ser potencializados e são movidos a desafios, tem que motivá-los. É uma gerência de recursos humanos e vai muito ao encontro disso, a questão de gerir os talentos humanos. Isso é complexo, mas é necessário; na segurança da informação, tem um bloco que é só de recursos humanos, que é lidar com a pessoa, conscientizá-la para ela ter atitude favorável para atenuar os riscos.

Marco Carnut (*Tempest Security Intelligence)* **comentou a fala do Ricardo** e do **Coronel Ricardo Camelo** em que acha que o Brasil não sabe criar *hackers*, não tem um curso e ele acredita que precisa-se mais deles. Se tivesse mais deles, poderia colocar um no CDCiber a mais para a ciberguerra, mas não se sabe formar essa gente, não tem um curso universitário para isso.

Quanto a eles terem cometido delitos, acha se alinha um pouco com a visão do representante do setor governamental: cada caso é um caso e há delitos perdoáveis; quando se é jovem, pode fazer muita besteira, até porque faz parte da juventude fazer besteiras e quando se é mais velho, não, tem a gravidade e uma série de coisas.

Citou o Mitnik que fez um monte de besteiras, e que a história é bem mais dramática do que o que o representante do governo citou, o Mitnick passou um tempão isolado, sem ser acusado de nada e detido, e finalmente ele cumpriu pena. E teoricamente, pelo menos a ideia era essa, quando serve a sua pena na prisão, pode-se voltar à sociedade.

Não sabe como isso funciona, mas a ideia básica é que deixe de ser um criminoso. Cada caso é um caso, mas o que acha profundamente interessante é que hoje não se sabe cultivar o talento *hacker*. Tem que descobri-lo como uma caça ao talento, para de repente achar alguém brilhante.

Citou que sua empresa recruta esse tipo de gente e que gostaria muito de conseguir empregar mais gente assim. Disse que descobrir esses talentos é uma arte e 90% dela é sorte, em sua opinião e gostaria de acrescentar.

Alfredo *(Procurador da República do Ministério Público Federal em Pernambuco):* explicou que trabalha em uma área que envolve crimes na Internet e que está aprendendo muito com a discussão. Perguntou ao Coronel Ricardo Camelo, representante do governo, se no dia a dia do Centro de Defesa existe uma política clara de delimitação entre as infrações que afetam a soberania e aquelas que são mais afeitas á segurança pública e assim seria mais a área da polícia federal, se existem mecanismos de cooperação e quais seriam os assuntos que seriam objetos dessa cooperação.

E sua segunda pergunta é sobre essa polêmica a respeito do Marco Civil da Internet. Existe, claro, uma primeira questão abstrata, que é o papel do Estado que se quer na sociedade, sob uma perspectiva de, por exemplo, da biopolítica, o limite de violência potencial que se admite do Estado.

Citou que leu uma reportagem que dizia que o Parlamento Chinês está para aprovar uma lei que permite, inclusive, o corte de acesso à Internet quando ele verificar questões que afetam a soberania, soluções que acredita serem drásticas possíveis nesses limites, e o outro, que é um papel, de certa forma, mais simples que é: se o Estado tem o papel de investigar e de punir, ele tem que ter, como foi falado pelo Coronel, mecanismos para que possa chegar aos autores dos crimes.

Citou o crime de pedofilia, por exemplo, é um crime onde, pelo menos no Brasil, a maior parte deles foi cometido por amadores; e se não houver a possibilidade de acessar dados de conexão ou dados de aplicação, é impossível identificar a autoria desses crimes. O registro de dados não se discute, por exemplo, nos EUA e na Europa, que são os centros de segurança pública que mais se dialogam frequentemente, e na Europa, por exemplo, em 2008 foi aprovada uma lei de registro de dados, mas essa lei foi considerada inconstitucional porque ela permitiu o registro de dados, mas não dizia como esse registro era acessado e como eram administrados esses dados. Mas eles não discutem a necessidade de incorrer no registro, porque sem o registro é impossível a investigação.

Nesse contexto, acredita que o Marco Civil é pioneiro porque delimita não só o tempo, 1 ano de registro de conexão e 6 meses para registro de aplicação, mas ele diz como esses dados devem ser acessados. Certamente se escorou nessa polêmica que houve na Europa para dizer que esses dados só podem ser acessados por ordem judicial. E pontuou um problema muito prático: a questão de vanguarda, de falar de 1 ano e de 06 meses, por mais que sejam afinados os órgãos de segurança civil – a polícia e o MP, especialmente – é um prazo muito curto.

Disse que a Polícia Federal recebe centenas – não há registro oficial sobre isso – pode chegar a milhares de notícias sobre crimes cibernéticos, inclusive informados a maior parte deles por órgãos internacionais, como a Interpol, e esses dados precisam ser repassados ao Ministério Público (MP) para que o MP por sua vez pedir autorização ao juiz para saber, por exemplo, de onde partiu o IP e outras informações decorrentes. Essas comunicações – polícia federal, MP e judiciário – por mais que o lapso seja curto, é no mínimo 06 meses. Então certamente esse prazo de 06 meses e de 01 ano da lei vai gerar uma polêmica decorrente da aplicação da lei recentemente aprovada, e talvez haja uma pressão no Congresso para que seja alterado, inclusive o tempo de guarda dos dados.

Finalizou, dizendo que a questão não é o registro dos dados, mas o tempo que ele é guardado e como ele é acessado.

Paulo Sérgio Licciardi Messeder Barreto (Escola Politécnica da USP): fez um comentário sobre a fala do **Alfredo** acredita que uma das grandes discussões é o tempo de armazenamento desses dados e citou que viu nas redes sociais o slide de uma apresentação – ele não sabe exatamente a referência – sobre o que significa exatamente armazenar metadados.

No slide em que viu, foram colocados vários exemplos, todos eles caricatos; e explica que armazenar metadados significa que é possível saber que uma pessoa anteontem, entre as 02hs e as 04hs da manhã, acessou um site de bate-papo erótico. Só que ninguém vai saber exatamente o que conversou. Esses dados não são armazenados. Essa é a diferença entre armazenar metadados de dados e a quantidade de informação que se consegue extrair, só de armazenar metadados.

Acha que a maioria já deve ter visto, pelo teor mais ou menos divertido que o autor procurou dar, mas tem outro lado da moeda que ele foi falando depois disso. Só acha divertido quando ele fala assim: “tal pessoa teve seus metadados gravados e, portanto, agora está todo mundo sabendo que tal pessoa acessou aquele site”, conforme havia exemplificado.

Questionou o que aconteceria para determinada pessoa se aparecesse que foi ela que acessou um site em que nunca viu na vida? Então, aparece a polícia, bate na porta, fala: “olha, você está sendo preso porque acessou um site aqui de tráfico de armas. Você está sendo acusado disso.” Afinal de contas, como o Silvio mencionou aqui, é problemático proteger a máquina; quando é uma dificuldade ou facilidade que tem de invadir a máquina, colocar um agente lá e o agente começa a tomar conta da máquina, mesmo que nem perceba que tem um agente rodando ali, e começa a acessar esses sites, sem se saber.

E acessou o site, fez a operação e mais ainda, qual é a dificuldade ou facilidade de fazer isso sem deixar rastros? Então, como falou, não tem uma resposta, só está provocando os participantes, porque é muito difícil dar uma reposta para isso e a problemática: “são apenas metadados”, sendo que os metadados revelam muito, sendo que é tão fácil assim de colocar a culpa em outros que invadem a máquina. Acha que, infelizmente, vai demorar muito até fechar completamente essa questão aqui.

Marco Carnut (*Tempest Security Intelligence)* respondeu ao **Alfredo** e ao **Paulo Sérgio** que não concorda com essa visão de que é “impossível determinar quem foi o pedófilo se os metadados não forem retidos”; não é impossível, é mais difícil. Diz ser super desconfortável com essa história dos metadados serem coletados de todo o mundo, sem suspeita provável, de todo o tipo e de todo o tempo. Para ele a polícia poderia perfeitamente, tendo a suspeita de pedofilia, aquela situação específica, para aquele IP, para o prumo daquela investigação, ele monitora, grampeia, faz o que quiser.

Para todas as pessoas, acha complicado. Complementou um pouco a brilhante colocação do Professor Paulo, e disse que recentemente saiu o caso de uma empresa italiana chamada Hacking Team, que vazou várias ferramentas dele. Uma das ferramentas que eles faziam – eles faziam ferramentas de invasão e vasou, inclusive, que o governo brasileiro estava negociando com eles – mas uma das ferramentas que eles tem é uma ferramenta especificamente projetada para invadir a máquina e colocar pedofilia infantil na máquina para incriminar a pessoa. Então acha que coordenar as pessoas por metadados é uma coisa muito complicada.

Coronel Ricardo Camelo *(CDCiber - Centro de Defesa Cibernética - Exército Brasileiro):* respondeu a pergunta do **Alfredo**, com relação à pergunta da parceria com a polícia, disse que uma das brincadeiras que costuma fazer no Centro é que sem ação colaborativa, a vida não é possível em cibernética. São frases de efeito que usa tentando conscientizar os colegas e até os próprios chefes, e tem funcionado bem, tem sido respaldo prático isso.

Falou que a Polícia Federal tem sido um parceiro muito importante, de grande relevância para lidar com essas ameaças cibernéticas, de um modo geral, ainda que o escopo das duas organizações sejam claramente diferentes. A polícia está lidando com questões criminais, que não são coisas da defesa. Eventualmente há crimes no âmbito da defesa, mas que vão ser tratados pela polícia, ou às vezes, na pior das hipóteses, pela polícia interna, mas que vai redundar num processo cujo rito vai, provavelmente, ou quase que necessariamente, passar pela autoridade policial que tenha a prerrogativa para fazer determinadas ações.

Citou como exemplo, se alguém precisa chegar até um eventual criminoso cibernético porque ele está com algum tipo de ação, quem tem a prerrogativa para fazer toda a escuta, por exemplo, fazendo analogia com a escuta de ligações telefônicas, devidamente autorizadas por um juiz, dentro de um rito administrativo, é a polícia. Então se tenta alimentar um ao outro com a informação e já tem um caso bastante significativo de sucesso nesse respeito.

Falou que está sendo consolidado a questão de confiança que citou em sua fala mais cedo, que começa pelas pessoas, mas que não pode se limitar à elas, porque se um se aposenta, é transferido e tudo mais, cai tudo por terra, e começa a criar métodos administrativos para forçar, no bom sentido, uma espécie de cultura inter organizacional, em que já é normal que um confie no outro dentro de determinados protocolos pré-estabelecidos. Um instrumento de convênio ou algo desse tipo.

Exemplificou com o Serviço Federal de Processamento de Dados (SERPRO); que foi o primeiro que o CDCiber assinou. Disse que há um convênio maior com a Itaipu, que é uma das principais infraestruturas críticas. E dentro de poucos dias, o General estará com o chefe da Unidade de Repressão de Crimes Cibernéticos, já esboçando algo nesse sentido, para transformar ou formalizar o que na prática vem construindo.

Falou que o caso de sucesso aconteceu entre a Rio+20 e a Copa das Confederações. Na Rio+20, sofreram ataques do mundo todo; era um evento cercado com muita ideologia,

muitos antagonismos, e na área cibernética não era diferente. E o Brasil sofreu ataques do planeta inteiro, independente da questão da clonagem dos IPs, das suas origens etc., mas oque foi possível levantar é que eles vinham de tudo quanto era lado. E por muito pouco a imagem do Brasil, não foi manchada. Quem foi ator principal não foi o CDCiber, foi um dos parceiros, o SERPRO, onde os ativos estavam fisicamente instalados, na página ativa do evento e mais propriamente, na página do evento que chegou a balançar ali.

Disse que não tinha saído a lei da Caroline Dieckmann, portanto não estavam criminalizadas as tentativas de pichação de site, a subtração de informações, de permissões de computadores etc. Só que a parceria, já estava ocorrendo na Rio+20 em conjunto, a troca de informações entre o Centro e a Unidade de Repressão de Crimes Cibernéticos, a complementariedade das ações pôde chegar à identificação de pessoas físicas.

Citou que o que aconteceu na preparação para a Copa das Confederações, na reunião de coordenação, com todos os parceiros, o Delegado da Polícia Federal responsável falou que não queria repetir as mesmas coisas do Centro, cada um no seu quadrado e a até pela parceria anterior, e aproveitando que a lei foi aprovada, fazer visitas e ações educativas.

Então tinham-se algumas lideranças que puxaram ações de vários *hackers*, e esses líderes puxavam fortemente o trabalho deles; e o que aconteceu é que na Copa das Confederações, essas curvas de acompanhamento desceram, caíram tremendamente. Houve um apoio, principalmente, do *Anonymous*, um dos movimentos de rua, foram coisas realmente assustadoras que foram implementadas nas redes sociais, com apoio às manifestações de rua, coisas assim, muito incríveis, desde exposição de informações de pessoais de policias para que fossem perseguidos, a organização de vaquinhas para tirar gente da cadeia, receitas para fazer artefatos caseiros para combater a polícia – armas, bombas ou como filtrar gases lacrimais – teve de tudo, mas ataque propriamente cibernético sumiu.

Entre a Copa das Confederações e Jornada Mundial da Juventude, apareceu um vídeo do *Anonymous*, aquela voz distorcida falando: “alguns dos nossos irmãos foram visitados, mas nós não vamos recuar”, ou seja, aquilo que estava constatando por gráficos veio até explicitamente se não uma prova, mas uma demonstração que realmente o que a polícia chamou de “efeito educativo” funcionou, ou o que o militar chama de dissuasão, que é o que os países tentam fazer.

Disse também que teve um efeito muito significativo; então, embora as áreas sejam diferentes, o problema é que o espaço cibernético é um só, no planeta. Então uma instituição ajuda a outra porque geralmente está tropeçando em coisas que interessam ao outro, que se complementam.

Exemplificou com o terrorismo, que interessa aos dois. E isso pode ajudar a falta de comunicação, como o Marco lembrou muito bem, o 11 de setembro é o exemplo clássico, pode gerar tragédias. Então se está consciente disso e não tem ainda um instrumento

formalizado com a Polícia Federal, mas se está neste caminho, tentando instituir isso. Às vezes é uma complicação, a burocracia, as decisões envolvidas no momento às vezes aceleram ou deixam a coisa mais devagar, mas se está tentando manter a impulsão para fechar esse processo formalmente também aquilo que já é prático.

Igor Dias *(Companhia de Tecnologia da Informação do Estado de Minas Gerais e Partido Pirata):* Solicitou ao Comitê Gestor da Internet no Brasil, ao Fórum que fizessem no relatório final uma orientação quanto a precarização que existe dentro das teles no Brasil. Por que isso? Porque, com esse conhecimento desse projeto de lei que aconteceu agora, o 4330, hoje PLC 30, ocorreu que no primeiro texto dele existia a possibilidade de terceirização das empresas estatais. Ou seja, todos os dados dos cidadãos do Brasil inteiro poderiam cair em mãos de pessoas que não se sabe o que fariam com eles. Para que saísse no relatório final do evento uma preocupação com isso. E perguntou para a mesa é qual o posicionamento em relação à computação na nuvem, porque sabe-se onde estão sendo armazenados, onde estão estes servidores e a qual legislação de qual país eles têm que respeitar.

Marco Carnut (*Tempest Security Intelligence)* respondeu ao **Igor Dias** quanto a história da computação das nuvens é uma oportunidade muito grande de poder voltar àquele tema que havia falado anteriormente: computação em nuvem pode fazer sentido ou não dependendo do que entende por segurança e qual o modelo legal da instituição. Citou como exemplo que acha que computação em nuvem é ótimo para empresas do tipo Groupon, Peixe Urbano etc., e citou que eles até usam, inclusive o modelo como eles colocam a política de privacidade dele que isso não parece, numa olhada rasteira, muito problemática.

Disse que ao mesmo tempo, computação em nuvem pode ser extremamente problemática. Exemplificou, quando estava em uma reunião com um órgão judiciário onde uma pessoa disse: “esses data centers custam muito caro e vamos colocar todos os processos jurídicos da gente na nuvem da Amazon, do Google etc.”. Marco disse que ficou estarrecido, porque isso basicamente significa que se a nuvem da Amazon ou do Google, ou sei lá de quem sair do ar, para todo o judiciário daquele estado e achou um absurdo.

Concluiu que não se pode ter uma resposta simples e curta; a resposta, acredita que depende das particularidades definir o que é o seguro contra o quê e das particularidades individuais daquele tipo de negócio, daquela instituição, daquela coisa. Existem várias coisas em que a nuvem funciona muito bem; existem várias de coisas não funcionam muito bem. Mas é contra a colocar na nuvem só pela moda; devia colocar porque sabe o que está se fazendo.

Silvio Rhatto *(Coletivo Saravá):* comentou a fala do **Igor** em relação ao Projeto de Lei Complementar 30 disse não ter conhecimento ainda, porém relativo à possibilidade de terceirização da coleta ou do armazenamento de dados e metadados de acesso, o Marco Civil proíbe; até onde sabe uma organização não poder fazer isso; ela deve manter esses dados em ambiente seguro e protegido.

Disse que não tem uma definição do que isso significa, se haverá uma norma e o que essa norma significa, mas terceirização, acha que não, porém não se tem uma posição relativa aos dados pessoais. Sabe-se que já houve convênios da Serasa com a Receita Federal para o armazenamento de informações e isso já gerou duas Comissões Parlamentares de Inquérito (CPI) e até onde sabe não deu em nada. Então acha que isso é um assunto perigosíssimo porque terceirizar às vezes é compartilhar, também.

Com relação à nuvem, acredita ser um tema super delicado, com relação ao âmbito do *software* livre, o Stallman elegeu isso como um dos próximos perigos da computação. Disse que há um problema porque não está se falando só de armazenamento, mas de processamento, de computação, de dados em nuvem. Disse que existe uma fala muito interessante e convidou a todos procurarem, que é sobre a guerra que está por vir contra a computação geral. Então acha que nesse caso será um pouco mais pessimista agora e dizer que o buraco também é mais embaixo porque se está vulnerável à terceirização da própria computação.

Perder o controle, não só dos dados pessoais, mas também do processamento desses dados. E isso evoca questões nos diversos níveis inclusive da manipulação da própria informação e do resultado dela. Se está perdendo poder computacional porque agora se elege que é melhor para criar grandes silos de processamento e ter pequenos aparelhos de acesso, pequenos terminais de acesso.

Acha que é muito perigoso e particularmente evita ao máximo colocar coisas na nuvem; e sabe que isso é impossível, mas essa palestra provavelmente estará numa nuvem, então são coisas que estão além do controle. Porém prefere manter os seus próprios serviços; e acha que é um papel da comunidade, principalmente *hacker*, de fomentar possibilidades de outras nuvens. Nuvens que se tenha controle. Nuvens que de fato entreguem apenas armazenamento e banda, e no futuro, talvez, até um processamento que se possa confiar.

Acha que a pesquisa de ponto o professor deve saber muito melhor do que ele sobre processamento criptografado, em que se tem algumas propriedades em que se consegue operar no dado cifrado e o dado também é cifrado, então pode-se vislumbrar, mas se elas se revelarem inviáveis talvez tenha a possibilidade de contar com a nuvem apenas para armazenar informações que já estejam cifradas.

Um dos projetos que acredita bastante e que está numa etapa experimental, é chamado *Lip*, ele partilha de conceitos comuns com outros projetos, de que a criptografia deve ser realizada nas pontas e a função da rede é armazenar e repassar, é endereçamento e armazenamento da informação. Então, uma perspectiva de nuvem que acha possível seria essa. Nuvens em que eventualmente pague a conta ou um modelo de negócios em que o provedor gratuito não consiga minerar a informação, então provavelmente seria uma nuvem que pagaria, mas seria um preço bem barato, porque essas coisas estão se barateando.

Então acha que talvez essa seja uma possibilidade, ou então ter a sua própria nuvem, uma nuvem comunitária ou da organização, interna. Mas disse que vê uma possibilidade que não seja a nociva numa nuvem de terceiros, que seria justamente usá-la apenas para

armazenar, repassar e eventualmente fazer isso de forma anônima, enfim. Acredita que são possibilidades que ainda não tem hoje e por isso acha que é preciso ter muito cuidado se for armazenar ou usar uma nuvem que não seja sua ou que não esteja sob o seu controle.

Marco Carnut (*Tempest Security Intelligence)* comentou a fala **Silvio Rhatto** e do participante **Igor,** apresentou um contraexemplo, em que se tem uma nuvem a rede *bitcoin*, desde que não desabilitem aquela linha de código que mostrou. Mas a grande sacada dela é que é uma tecnologia que dá o que se chama de consenso distributivo global, que está sendo usado para criar uma moeda digital e essa moeda é distribuída sem uma instituição central.

Disse que os bancos estão com medo, porque o *bitcoin* pode e acha que vai mudar o mundo e a natureza dos bancos e o relacionamento com o dinheiro, num modo geral, e ele é uma nuvem que tem essa característica: é uma nuvem em que a criptografia é feita nas pontas, que o meio da rede realiza diversos tipos de computação, tem uma série de regras. Disse que quis colocar isso mais como um contraponto.

Citou que o representante do terceiro setor está certo em falar que em certos aspectos o buraco é muito mais embaixo, também é verdade afirmar que existe um admirável mundo novo de soluções impactantes e seguras. A rede *bitcoin*, em que pese, essas soluções precisam melhorar e isso é um fato, como tudo na Internet porque nada disso nasceu pronto, mas a rede *bitcoin* é uma das coisas mais transformadoras, seguras e que mudam muitos paradigmas. Disse que já viu muitos exemplos clássicos de nuvem de maneira mais nuvem que a nuvem pode ser.

Paulo Sérgio Licciardi Messeder Barreto *(Escola Politécnica da USP):* respondeu ao **Igor**, bem como disse estar de acordo com a tecnologia do *bitcoin*, apontada pelo **Marco Carnut** e especificamente com a questão do DHT, acha que até um pouco mais atrás, uma coisa um pouco mais anos 90, a própria história de servidores de chave, partiram dessa ideia porém as implementações de mensageria estão engatinhando.

Acha que um dos caminhos, em que ainda não há uma solução massiva, mas que os DHTs também tem seus problemas e que é uma grande discussão e rica devendo todos ficarem de olho nisso e em outras abordagens que às vezes são até mais clássicas de se obterem resultados semelhantes. A ideia do DHT é que se pode também ter cópias e eventualmente até dividir a rede, então concluiu que ela também opera uma resiliência, nuvens de nuvens.

Silvio Rhatto *(Coletivo Saravá):* fez observações em relação a perspectiva do CDCiber, lidar com as empresas de Telecomunicações o que acredita ser fundamental. Disse que antes que alguém fale que ele quer que os militares controle os *backboards* pra ver tudo o que está passando. Explicou que sim, é claro que é um ponto chave da governança e passa pela questão dos *backboards* e como eles saem do Brasil.

E citou que atualmente tem os portos que saem do Brasil, pouquíssimos cabos que tornam bastante dependentes inclusive, de estruturas internacionais nada convenientes, no mínimo, teoricamente, sendo bonzinho, podem apagar de uma hora pra outra. Então esse aprofundamento em relação a questão de como as Telecomunicações tratam os dados, se julga muito importante.

Disse que percebeu que os grandes eventos estão servindo como um laboratório maravilhoso e eventos que servem como verdadeiros catalizadores de maturidade para o país nessa área de cibernética. Disse também que observa, uma constatação não muito boa, que as Telecomunicações ainda lidam com bastante deficiência em relação a comunicação de dados no país, e muitas vezes fica surpreendido com a capacidade gerencial disso, pois muitas vezes já com um orçamento na ponta diziam: 'não, isso aí eu não forneço porque não está no contrato', não tem nem como trocar informações a respeito de negação de serviço que está entrando no país e que se pode detectar facilmente e pelo menos deveria poder, ou seja, é uma visão muito comercial da necessidade de gerir os dados, que complica muito e talvez tenha a ver com a própria história curta da estruturação das Telecomunicações no país, e como se observa em muitos exemplos, muitas vezes em nossos próprios telefones, parece que a expansão das Telecomunicações é maior do que elas podem dar conta em determinados momentos.

Falou que está tentando ser diplomático, mas é como alguns apagões e algumas indisponibilidades que se observa que as vezes chegam a picos bastante intensos. O que o Ministério da Defesa por meio do Centro, vem tentando influenciar nessa área, é se aproximar da Agência Nacional de Telecomunicações de tal maneira que se possa identificar pela perspectiva comum (Agência e o Ministério da Defesa), mecanismo que discipline ou potencialize como lidar com essa questão, até pra proteger melhor as instituições. Disse que aconteceu dentro dos grandes eventos mesmo, com instituições brasileiras, em que ataques de negação de serviços eram maciçamente encaminhados para determinadas instituições que tinham contratos específicos com Telecom e foi da surpresa que conversar com esse provedores, e que não tinha previsto isso no contrato, não tem conversa, ou seja, nem mesmo para manter um cliente mais significativo foi demostrado essa maturidade em relação atenuar a questão do risco e lidar com a segurança.

Disse que pode ser que as coisas tenham evoluído, pois tudo está mudando constantemente. Mas, chegou também à conclusão de que, considerando o país como um continente, várias telecoms, várias concessionárias de telecomunicações, negociar uma a uma é inviável. Não tem como, então ir na agência ver que dispositivos legais, que é possível fazer, que é possível daqui pra frente e acertar pra que se possa ter uma gerência de dados dentro das comunicações de longa distância no país, que apontem mais no que diz respeito a segurança.

Pontuou que uma questão de alteração de dados, quando tem ataques maciços, que é quando acabam invadindo o país, e entram nos ponteiros dessas Telecoms e tem que detectar, tem que detectar, portanto não vê outra possibilidade.

Comentou a pergunta de Igor em relação as nuvens, dizendo ser uma nuvem ''tenebrosa' porque realmente, quando se fala em nuvem, a não ser que faça as coisas todas, que crie uma própria nuvem e faça chover, ou seja, gerencie o sistema, não tem governança, então novamente se tem a questão de ter que confiar. Ao mesmo tempo, não sabe se está errado, mas já viu essa história acontecer algumas vezes, diz que não pode, é perigoso e tudo mais, mas sente meio que tentando mandar de volta um tsunami com uma raquete de tênis.

Citou que quando surgiu a Internet, se dizia: 'não, é perigoso, não podia colocar dados sensíveis', isso vai, o usuário se encantou pelo canto da sereia e em pouquíssimo tempo a coisa se disseminou de uma maneira totalmente incontrolável, o que veio depois, qual foi o próximo tsunami que foi um monte de pessoas para praia com raquete de tênis pra mandar de volta: rede sem fio.

Então citou outro tsunami, um outro grupo querendo mandar de volta a tecnologia móvel, como *tablets*. A nuvem para ele é outro tsunami que está chegando. Acha tecnicamente viável, mas em termos práticos, difícil de colocar em prática, deter essa onda.

Então, acha que todos têm que se voltar para uma possível abordagem e voltar para as boas práticas de segurança da informação, capítulo, gestão de risco e avaliar como tratar isso pra atenuar os riscos relacionados, como por exemplo, a questão da clássica solução desde o tempo dos 'Césares', e até antes, meio inseguro, o que colocar? Cripto. Acha necessário fazer a gerência disso pra fazer da maneira correta. Quando o PGP apareceu, conta o mito que o governo do irmão do Norte quase foi a loucura, porque conseguia controlar antes quando chegou aos dois lá que fizeram a cifra e mandaram pra rede e saiu do controle e, agora, então existem possibilidades de lidar com a coisa, precisando tomar cuidado.

Acha complicado porque o cidadão quer viver em paz com a benesse da tecnologia servindo sem precisar achar que tem uma assombração dentro que vai matá-lo a qualquer momento. Isso é terrível. Então cabe as suas áreas tecnológicas e gerenciais, atenuar o risco. Obviamente a área legislativa e política tem que disciplinar. Concluiu que não é um problema trivial, mas é um problema que existe.

Manoelito *(Raul Hacker Club):* perguntou em relação ao Ministério da Defesa como está a questão da segurança em nível de *hardware* e *firmware*, porque recentemente saiu uma página em que todos os dispositivos que tenham USB na face da terra podem se contaminar. E sendo impossível de detectar, se está acima de qualquer permissão que o maior usuário da máquina possa ter.

Disse que isso é em relação aos *hardwares* também do Exército, as informações. E fez um adendo em relação a nuvem, que salvo engano tem uma lei federal que proíbe que dados federais sejam hospedados e, o Rafael que faz parte do Raul Hacker Club e trabalha na Universidade Federal de Lavras (UFLA), já colocou que professores não podem armazenar nenhum tipo de dado federal no Dropbox, por exemplo, é proibido.

Acredita que a UFLA tem que criar um serviço de nuvem próprio, com uma certa diretriz de segurança. Citou que a Universidade de Tel Aviv em Israel, conseguiu quebrar a criptografia ouvindo o barulho do processador, portanto, concluiu que existe uma série de técnicas e fontes. Perguntou como o Ministério da Defesa se prepara para esse tipo de coisa? Disse que faz Engenharia Elétrica na UFLA também, e tem interesse por esta área, principalmente, pelo Programa CI Brasil, que é muito pouco disseminado pra que capacitem os estudantes na área de *hardware*, pra que esse tipo de autonomia Nacional realmente se concretize.

Disse não ver muito esforço para que isso realmente seja disseminado. Contou que na universidade há pouquíssimos estudantes sabendo do programa, **respondendo a Paulo Barreto** que há um pequeno número de pessoas. Questionou Ricardo Camelo como o Ministério da Defesa lida com essas informações. Exemplificou com a piada dizendo que Dilma envia e-mail para Obama enviando para ela mesma.

Coronel Ricardo Camelo *(CDCiber - Centro de Defesa Cibernética - Exército Brasileiro):* Iniciou sua fala explicando que o Ministério da Defesa é uma instituição como outra qualquer, refletindo as evoluções e as dificuldades brasileiras, apesar do foco do militar ser o planejamento da guerra. Pelo motivo do medo, o Exército possui um desenvolvimento um pouco mais rápido que o da sociedade. **Respondeu a Vitor** que isso foge da governabilidade do Ministério da Defesa. Exemplificou que o Exército não foge da lei de licitação, comprando pelo menor preço e com problemas de mercado do próprio país, ou de especificação. Com isso, acaba-se adquirindo equipamentos que tenham comprometimento de segurança. Destacou que se trabalha desde 2000 em uma área que é a mãe da área de segurança, a chamada "*contra inteligência*".

Assim, disse ele, o Exército já trabalha nesse ritmo de atenuação, adotando as boas práticas e tentando implementar regras, as famosas políticas de segurança, disciplinando desde a área de recursos humanos, até a área de equipamentos. Então áreas sensíveis, o Exército procura filtrar e atenuar o risco. Também relembrou que o Exército possui um legado que não se pode simplesmente jogar fora, porque não se tem recursos financeiros para, de uma hora para outra, mudar todo o parque. Assim, atenua-se isso com criptografia de Estado e com processos de sensibilização. Então, de acordo com Camelo, dentro do governo e do próprio ministério existem áreas bem mais adiantadas por força da necessidade, áreas de Inteligência, como por exemplo, o próprio Centro, que é uma unidade muito jovem e tem tido bastante trabalho nessa área de tentar nascer o melhor possível, ainda que tenha coisas em que se viram obrigados a arcar com o risco.

Disse que não vê boas opções, mas a metodologia escolhida, se bem executada em passos e procedimentos poderá ter um menor risco. Apesar disso, apontou que infelizmente não existe muitas opções na área de *hardware* e disso se vai convivendo. mas por exemplo não adotam *software* fechado, famoso, que virou cocaína do mundo. Destacou ser preciso sensibilizar as autoridades, algo que não é simples, pois são profissionais de outras épocas, não sensibilizados pela temática. Também há o atenuante da contra inteligência, tema que eles entendem melhor e são mais sensíveis, sendo um processo sucessivo de substituição paulatina do que é mais crítico em termos de *software* e *hardware*.

Para ele, há poucos *hardwares* criptografados, mas já existe parceria com a Agência Brasileira de Inteligência (ABIN). Sua opinião é de que a fórmula mundial não é copiar e colar o modelo lá de fora aqui dentro. Reclamou do setor privado que está absorvendo os vários profissionais de excelência dentro do Exército, pois não se fica rico sendo militar. Explicou que motivos que fazem estar no Exército é poder ver que engenheiros eletrônicos estão construindo coisas, além da tradicional tarefa de integração de objetos. Criticou apontando que não é no ritmo que se quer, mas está se caminhando para frente.

Finalizou destacando o rico painel realizado, mas não esgotou pois é um assunto muito vasto, mas disse acreditar que há subsídio para saírem do evento e refletirem sobre a área. Agradeceu a oportunidade e desejou boa noite a todas e todos.

Marco Carnut (*Tempest Security Inteligence*): Iniciou sua fala apontando ser um sujeito pragmático, adorando discussões filosóficas mas sempre tem frustações com a filosofia, pois ela não gera produtos práticos para melhorar o mundo e sair do ponto que está sendo discutido. Encerrando sua fala apontando alguns pontos para as pessoas adotarem: 1- Se forem desenvolvedores, escreverem códigos que evitem vulnerabilidades. 2- Pediu mais funcionalidades que *bugs* (defeitos no código de programação) do *software*, sendo mais esmeros, cuidadosos com segurança, sendo ela uma prioridade. Isso faria com que existisse uma quantidade menor de vírus e *malwares*, destacando que a indústria de vírus não precisa existir. Cada *Firewall* é um bloqueio que melhora toda a Internet, os IPs ficando mais seguros.

Explicou que cada *Buffer Overflow* em um *software* permite que seja invadido e-mail e outras aplicações. Sua opinião é de que as vulnerabilidades estão matando a Internet, e deste modo fazer um *software* se conectar à Internet é um pesadelo devido a uma série de problemas de conexão e de segurança. **Questionou Paulo Barreto** sobre criação de cursos acadêmicos que ensinem a programar sem vulnerabilidade. Exemplificou que bons engenheiros civis aprendem sobre a história de edifícios e pontes que caíram por erros em seus projetos. Criticou a ciência da computação por não ter uma disciplina como essa, contando a história de *bugs*. Sua opinião é de que antivírus e *firewall* são remendos mal feitos, e se deve matar a raiz do programa. Exemplificou também o uso do Tor e anonimização, não precisando ser gênio em criptografia para usar o *software*. Defendeu que essas são pequenas grandes coisas que possam ser feitas.

Outras ação defendida por ele é o uso de moedas digitais como a *bitcoin*, apontando ser uma das coisas mais inovadoras e um dos usos mais bonitos de criptografia e protocolos de consenso já visto há muito tempo. Finalizou apontando que nenhum da plateia precisa ser gênio em computação pra fazer isso. Agradeceu a oportunidade e desejou boa noite a todos.

Paulo Sérgio Licciardi Messeder Barreto (Universidade de São Paulo - USP, São Paulo, São Paulo): Finalizou dizendo que testemunhou sobre o ponto de vista acadêmico, apontando que a academia forma muito pouco recursos humanos que se tornam profissionais na área de segurança da informação e criptografia. chamou atenção também no baixo número de professores na área, sendo um ciclo vicioso: poucos professores formam poucos profissionais. Mas isso acontece porque poucos profissionais tem a

chance de se tornar professores. É preciso mudar esta cultura e incentivar mais. Disse que não se deve assustar com as fórmulas, acreditando que quando as pessoas começam vendo um monte de símbolos se desestimulam e partem para outros assuntos que gostem mais. Convidou os interessados na discussão a trabalharem na área e se capacitarem na área.

Falou que não conhece nenhum criptógrafo soteropolitano além dele mesmo e gostaria de ter um conterrâneo para poder conversar. Criticou os presentes pois apenas um ou outro veio falar com ele durante o *coffee break*. Explicou que gostaria de ver mais pessoas interessadas pois há mais problemas que solução na área. Agradeceu a presença de todos e oportunidade de participar do Fórum da Internet.

Silvio Rhatto (*Coletivo Saravá*): Seguindo a mesma linha, Rhatto acha que as notícias de vulnerabilidades e falta de segurança, a q as pessoas estão expostas diariamente podem gerar muita angústia, impotência e da impotência pra apatia. Ele acha que deveria ser feito um esforço pra gerar potência e entender exatamente onde que se pode ir. Silvio tem certeza que a construção da segurança e da privacidade não é individual, ela é coletiva, em todos os níveis e todo mundo pode colaborar. Seja digamos passando a palavra adiante, irmãos e irmãs, até trabalhando mais ativamente com a capacidade de cada pessoa, porque isso virou uma necessidade de alfabetização, não só digital, mas de segurança, uma espécie de capacidade de ser cidadão, ou ser um ator político ou ser uma pessoa, ela vai depender não só de cada um, todo mundo ter condição de melhorar a situação da segurança e da privacidade.

O painelista acredita que várias sugestões já foram dadas durante a trilha, no âmbito da academia, do desenvolvimento de *software*. Para ele, no Brasil, pelo menos antes de 2012, não havia tanto interesse nesse assunto porque era uma coisa assim, fora da realidade. No entanto, o assunto existe hoje, existe interesse, um interesse massivo das pessoas em discutir esse tipo de coisa, e não se dá conta. Então é necessário descobrir como fomentar esse debate, sem esperar que surjam “os iluminados” da criptografia e da segurança, pois, para Silvio, qualquer pessoa pode ter esse debate, pois é mais fácil falar sobre padrões e *softwares* já existentes, é questão de tomar esse poder, acreditar nisso e procurar opiniões para fomentar esse debate. Rhatto considera que não é necessário apenas pessoas na Academia produzindo *software*, mas sim de pessoas em todos os níveis e em todas as áreas levando essa discussão adiante, e conforme os problemas reais aparecerem, as pessoas vão levar isso mais a sério.

Silvio recomendou que se trate esse problema com relação à segurança e privacidade, como um problema de saúde pública, pois é um problema epidêmico, em que o mundo todo está sofrendo, não apenas uma ou outra pessoa. Reiterou que essa não é uma opinião somente dele, mas toda a comunidade de segurança também pensa assim, e se tem um arcabouço das ciências médicas para lidar com a epidemia. De acordo com ele, se tem um conhecimento desse tipo de epidemiologia que poderia ser adaptado para isso, sendo que, para ele, poder-se-ia ir até mais longe, herdando conceitos da redução de danos, pois é muito difícil reduzir completamente o uso dessas tecnologias; vive-se atualmente uma tensão entre não participar automaticamente dessas tecnologias e começar a se desligar socialmente ou profissionalmente de diversas atividades. Silvio

afirmou que todo mundo compartilha dessa angústia e que uma das saídas para essa epidemia seria trabalhar com a redução de danos.

No entanto, Rhatto ponderou que para se adotar uma abordagem de redução de danos, é preciso, primeiramente, ter um exercício de humildade em entender que isso é a vida, porém que isso não gere uma impotência ou uma apatia, mas sim que incentive a melhorar pouco a pouco a situação até um nível confortável de segurança e privacidade. Assim, recomendou que, quem esteja preocupado com isso, não decida simplesmente, da noite para o dia, adotar as melhores práticas e esquecer um pouco da vida para estudar isso. O ideal, de acordo com o painelista, é ir aos poucos, respeitando seus limites e suas capacidades. Também acordou que ao ir devagar, pode-se compartilhar esses avanços com outras pessoas, que talvez não sejam pessoas interessadas no tema, mas que, com alguma inércia, possam evoluir para um nível melhor de segurança e privacidade.

Ele destacou que não existe uma plataforma chamada *Test Security*, um *software* um pouco melhor, contudo, sem ser a solução para todos os problemas. Porém, sua opinião é de que seria factível migrar e aos poucos convencer as pessoas com quem se convive a migrarem para a plataforma e assim por diante. Resumiu para irem com calma, e não há tempo para se pensar se todos querem ou não essas tecnologias. Elas simplesmente aparecem, contou. Defendeu a capacidade das brasileiras e brasileiros de mudar a situação. Agradeceu a todos pela oportunidade.

Lisandro Granville *(Conselheiro CGI.br*): agradeceu a presença de todos, aos painelistas pelos temas abordados e encerrou as intervenções e debates, mesmo dizendo que tinha o interesse de debater a formação de recursos humanos. Disse que isso acontece pelo efeito colateral do intenso interesse no tema.

Marco Carnut (*Tempest Security Inteligence*): Sugeriu que ano que vem fosse setorializado ou até mesmo alocasse mais tempo para discussão. Para ele, a dinâmica demonstrou que há grande interesse e deveria ser viabilizado de alguma forma a discussão.

O coordenador finalizou a trilha explicando que todas as sugestões e intervenções estão sendo registradas e até o final do evento haveria um relatório sintético a ser conferendado com todos e depois de um mês o relatório completo. Apontou que esta é a matéria-prima para continuar a discussão, se atualizar sobre o que foi discutido. Agradeceu a presença de todos.

5. DEBATES DOS GRUPOS DE APROFUNDAMENTO

Não houve grupos de aprofundamento.

6. ANEXOS

6.1. Lista de Participantes

Nome	Instituição	Cidade	Estado
Adson Mota	Ruy Barbosa	Salvador	BA
Alderi Santos de Oliveira	AL	Natal	RN
Alex F. Pereira	Tec I 9	Salvador	BA
Alexandra	Ibliss	Salvador	BA
Alexil Ferreira		Salvador	BA
Ana Leticia da Silva	Ruy Barbosa	Salvador	BA
Analhan C.	Ruy Barbosa	Salvador	BA
André N.	Dom Pedro II	Salvador	BA
Antonio Rodrigo C. Macedo		Salvador	BA
Bruno F. Viana	SERPRO	Salvador	BA
Caio Tiago G. de Sousa	COLIVRE	Salvador	BA
Caio V.	FRB	Salvador	BA
Crislete O. Santos	Ruy Barbosa	Salvador	BA
Deusdedire C. P. Junior	IFBA	Salvador	BA
Djair F. Bastos	Estudante	Salvador	BA
Eber Santana	Fiat	Salvador	BA
Erik Costa	Tempest	Recife	PE
Everton de Lima	UFAL	Arapiraca	AL
Filipe de Cruz Ribeiro	IFBA	Salvador	BA
Francisco Chagas	IFBA	Salvador	BA
Gabriel Ferreira dos Santos	UFBA	Salvador	BA
Gabriel P. C.	Ruy Barbosa	Salvador	BA
Graziela de J. Santos	Ruy Barbosa	Salvador	BA
Guilherme A. C. C. Santos	MPF	Salvador	BA
Gustavo Diôgenes de Oliveira Paiva	UFRN	Natal	RN

Hugo Cláudio B.	UFMT	Barra Das Garças	MT
Hugo de Souza	IFBA	Salvador	BA
Ícaro Ariel Carneiro L.	UNEB	Salvador	BA
Idelma Bernardes	Mauricio Nassau	João Pessoa	PB
Igor T. Dias	Prodemge	Belo Horizonte	MG
Ingrid O. de Souza	Ruy Barbosa	Salvador	BA
Isis Natalie Torres Silva	Ruy Barbosa	Salvador	BA
Janderson Dias Trindade	Ruy Barbosa	Salvador	BA
Jeferson R. Lima	Ruy Barbosa	Salvador	BA
Jonathas Azevedo	Ruy Barbosa	Salvador	BA
Josângela Barbosa de J. Santos	OAB	Salvador	BA
José Aragão	Senai	Salvador	BA
Josemire Reis	UFBA	Salvador	BA
Kleber Oliveira	IFBA	Sfilho	BA
Laércio Sales de Jesus	Ruy Barbosa	Salvador	BA
Leilson L.	Ruy Barbosa	Salvador	BA
Leonel G. Lobo	PRF	Brasília	DF
Lisandro Granville	UFGRS	Porto Alegre	RS
Lucas Novais de Almeida	Ruy Barbosa	Salvador	BA
Luciano Lucas Silveira	SINPEF	Palmas	TO
Manoel da S. Souza	Ruy Barbosa	Salvador	BA
Manoelito C. Neves Filho	Raul Hacker Club	Salvador	BA
Marco C.	Tempest	Recife	PE
Mariana Ruivo	Unicamp	São Paulo	SP
Mariana N. M.	Unifacs	Salvador	BA
Marina A.	UFBA	Salvador	BA
Marlucio Costa Lopes	PMUC		PA
Mateus Sena		Salvador	BA

Matheus N. Santos	FRB	Salvador	BA
Maurita Gomes Costa		Salvador	BA
Maxlen P. D.	SERPRO	Salvador	BA
Michelle R Silva	LSE	Londres	
Murilo Sousa Frois	Ruy Barbosa	Salvador	BA
Neuma de S. Cordeiro		Salvador	BA
Paloma de Sena Santos	Ruy Barbosa	Salvador	BA
Paulo S. L. M. Barreto	USP	São Paulo	SP
Pedro R.	Câmara Federal	Rio De Janeiro	RJ
Rafael Gomes	Raul Hc	Salvador	BA
Ramon Mendes	Ruy Barbosa	Salvador	BA
Ricardo S.	Rui Barbosa	Salvador	BA
Rodrigo M. S.	COLIVRE	Salvador	BA
Rogerio F.	Petrobras	Salvador	BA
Rogério R.	FINEP	Rio De Janeiro	RJ
Romilda Santos	Ruy Barbosa	Salvador	BA
Tiago da S. Pereira	Comerciários	Salvador	BA
Vanessa Cruz Santos	Ruy Barbosa	Salvador	BA
Wesley Sampaio de Jesus	Ruy Barbosa	Salvador	BA