ICANN76 | Fórum da Comunidade – Debate do GAC: Abusos no DNS
Terça-feira, 14 de março de 2023 – 10h30 às 12h CUN

JULIA CHARVOLEN: Bom dia, bem-vindos à discussão do GAC sobre o uso indevido de DNS, 10:30, hora local, essa sessão está sendo gravado e se rege pelos padrões de comportamento da ICANN. Nesta sessão, as perguntas e comentários apresentados no chat vão ser lidos em voz alta se estiverem no formato certo. Se estiverem no Zoom, levantem a mão, e lembrem de dizer em que idioma vão falar, caso não seja inglês. Falem num ritmo razoável, para permitir uma interpretação certa. Silenciem os outros dispositivos ao falar, todas as funções disponíveis estarão na barra de ferramenta do Zoom, e passo a palavra agora à presidente do GAC, Manal Ismail.

MANAL ISMAIL: Obrigada, Júlia. Bom dia, boa tarde e boa noite a todos. Bem-vindos novamente, vamos conversar no GAC sobre mitigação de uso indevido de DNS, temos uma sessão de uma hora, e vamos continuar falando das iniciativas da comunidade da ICANN e da organização da ICANN para prevenir e mitigar o uso indevido do DNS. Também vamos passar as novidades sobre os últimos acontecimentos e esforços realizados pelos membros do GAC junto com a comunidade no seu conjunto para apoiar a ampliação de disposições contratuais e possíveis processos de políticas para melhor abordar o tema do uso indevido do DNS. Passo a

palavra para os responsáveis do tema, nesse caso temos Gabriel Andrews, do FBI dos Estados Unidos, e também Laureen Kapin, que é da comissão de comércio federal dos Estados Unidos, e copresidente do PSWG. E também, Chris Lewis-Evans, da National Crime Agency do Reino Unido, e também copresidente do PSWG.

CHRIS LEWIS-EVANS: Bom dia a todos, vamos passar direto para o slide. Vamos ter uma sessão sobre uso indevido de DNS e temos uma apresentação externa. Posso ver o líder da rede de política de jurisdição e Internet no canto, espero resolver alguns slides com nosso suporte do GAC. Então, antes disso, farei uma introdução rápida para nos dar uma ideia de por que é importante combater o uso indevido de DNS. Em seguida, teremos uma apresentação sobre estatísticas de crimes cibernéticos e como elas se relacionam com o uso indevido de DNS. E então dê uma olhada nas outras atividades acontecendo dentro da comunidade. Em seguida, faça um resumo e considerações para conselhos de comunicado ou assuntos importantes para nós. Passe para o próximo slide, por favor. Obrigado. Quase sinto que não preciso fazer este slide. Parece que falamos bastante sobre uso indevido de DNS. Já houve algumas sessões realmente boas durante esta reunião. Farei outra menção ao workshop de capacitação no sábado. Houve uma boa sessão para uso indevido de DNS, que você pode revisar sobre isso. Aqui, temos uma série de links que você pode acessar. Como sempre, você pode fazer uma pesquisa no site do GAC sobre uso indevido de DNS e isso trará itens no comunicado, que são da equipe de suporte. Benedetta e a outra equipe de suporte realmente mantêm isso atualizado. Eles fazem

um trabalho muito bom em ter recursos que podemos pesquisar lá. Portanto, temos vários itens que sinalizamos. É uma parte muito importante do trabalho do PSWG também. Está dentro do nosso plano de trabalho, que ratificamos e endossamos nesta reunião, o que foi muito bom, para apoiarmos as habilidades das autoridades policiais e de segurança pública para proteger o público, que é realmente o que eles fazem nisso. Como eu disse, há muita coisa acontecendo dentro da comunidade, então é importante para outras partes interessadas dentro da comunidade. Há muitas discussões acontecendo, consultas à diretoria e correspondência. E a comunidade empresarial tem falado bastante sobre como isso é importante para eles. Também houve equipes de revisão, a equipe de revisão de CCT, RDS-WHOIS2, SSR2, para citar alguns, e também PDPs da GNSO sobre procedimentos subsequentes que abordam o uso indevido de DNS. Depois a outra, que vamos abordar mais adiante na apresentação, é o esforço das Contratadas. Eles enviaram uma carta ao Conselho para abrir as negociações do contrato para ajudar a combater o uso indevido de DNS. Esse é um passo muito bom. Isso apenas mostra que todos na comunidade querem agir e é muito importante para todos, e é certamente por isso que consideramos isso por algum tempo. Atenção, Gabi. Você é o próximo. Assim, prosseguiremos com nossa apresentação sobre as tendências do cibercrime. Então podemos ir em dois slides, acho que é, no pacote? Obrigado. Gabe, para você. Obrigado.

GABRIEL ANDREWS: Obrigado. Oi. Meu nome é Gabriel, estou falando aqui como membro do Grupo de Trabalho de Segurança Pública. O que esperamos fazer aqui é algo que talvez estejamos otimistas de que possamos fazer anualmente mais tarde. Mas a razão para isso é quando se trata de entender o escopo e a escala do uso indevido de DNS, assim como tentar entender o escopo e a escala do crime na Internet, é importante reconhecer que não temos fatos perfeitos. O que temos são muitas perspectivas diferentes.

Então, como o cego nesta foto que você pode reconhecer do workshop de capacitação, eu também usei isso, temos muitas pessoas que estão fazendo o possível para observar o que está na frente delas, para falar sobre o que elas estão percebendo, na esperança de que, colaborando, possamos ter uma ideia melhor do que realmente está por aí. Então, é aqui que reconheço que há muitos grandes esforços da comunidade que visam fornecer dados, métricas, medições e observações sobre o uso indevido de DNS. E estou pensando em coisas como os relatórios Compass do DNS Abuse Institute, que começaram no outono do ano passado. Como o OCTO da ICANN e seus relatórios de atividades de abuso de domínio. Ouvi dizer que apenas na conversa de dois dias atrás, talvez, com a equipe executiva, John Crain mencionou que, além do que já esperávamos com relatórios de abuso no nível do registrador, ele tem ideias sobre análise preditiva e aprendizado de máquina que deseja incorporar. Estou muito animado para ver o que sai desses esforços. Mas, para complementar esses esforços da comunidade, esperamos fornecer perspectivas adicionais que somente a aplicação da lei pode trazer para a mesa e que só vêm da segurança pública. Estou pensando nas denúncias de vítimas que chegam até nós. Para ser claro,

não estamos sugerindo que todo crime na Internet seja uso indevido de DNS. Em vez disso, entendemos que o escopo e a escala do dano à vítima que nos é relatado pode ser uma daquelas perspectivas que você pode achar importante considerar em suas deliberações, especialmente se pudermos ser úteis de alguma maneira para ajudar para traduzir esse relatório para como e onde ele tem conexão com o uso indevido de DNS. E com isso, eu acho, Chris, você tem a primeira parte disso.

CHRIS LEWIS-EVANS: Sim. Apenas muito brevemente, antes de passarmos para o próximo slide. Desculpe. Podemos voltar um slide? Obrigado. Em nossa última reunião do PSWG, pedimos a todos os membros que nos forneçam algumas estatísticas sobre crimes cibernéticos e como isso pode estar relacionado ao uso indevido de DNS. No momento, não recebemos nenhum outro além dos EUA e do Reino Unido. Portanto, se você estiver envolvido com suas próprias agências de aplicação da lei ou agências de proteção ao consumidor, sinta-se à vontade para orientá-las em nossa direção. Gostaríamos muito de ver o que outros países estão vendo e poder fazer uma revisão um pouco mais ampla dessas estatísticas. E procuramos fazer isso, provavelmente uma vez por ano, para dar uma ideia da paisagem. Passando para os slides do Reino Unido, no Reino Unido temos um único órgão de denúncia chamado Action Fraud, que não apenas comete fraudes. Eles praticam crimes cibernéticos também. Mas o nome estava lá primeiro e depois eles adicionaram essa missão. Suas quatro principais estatísticas de coleta realmente não acompanham o uso indevido de DNS. Eles têm hacking,

mídia social e e-mail. Vírus e malware, então o lado do malware, mais ou menos, mas os vírus também estão lá, então não se alinha com o que entenderíamos como uso indevido de DNS. E então hackear, seja pessoal ou extorsão, que tende a ser o material mais focado em ransomware.

Então, como vocês podem ver neste slide, dados de 2014 e uma tendência geral de aumento na denúncia desses crimes. Passe para o próximo slide, por favor. Uma das coisas que eles também fazem é enviar pesquisas para empresas e instituições de caridade para entender como foram afetados, o que estão vendo e como estão lidando. Esta parte da análise é sobre quantas organizações identificaram violações ou ataques em seus sistemas. Então, bastante estático, talvez uma tendência de queda no lado dos negócios. Mas muito interessante, nas instituições de caridade, um aumento definido. Alguns dos pensamentos por trás disso são as instituições de caridade, antes do GDPR, talvez não estivessem bem configuradas para olhar para suas próprias redes e fazer análises. Uma vez que você começa a procurar algo, você tende a encontrá-lo. Portanto, se essa é uma das razões para esse aumento, é que eles estão procurando e encontraram, ou se é um aumento nos ataques direcionados, é muito difícil dizer. Pode ser muito difícil dizer. Mas apenas um pouco de tendência lá. E para o próximo slide, por favor. Nesse slide, obviamente, daqueles que sofreram uma violação, foi perguntado como eles identificam essa violação e como foi o vetor de ataque inicial. Ao longo dos anos, a resposta para isso, 80% das vezes, foi o phishing. Phishing está definitivamente no espaço de uso indevido de DNS. Então você pode ver, de todos os outros crimes que cometi no primeiro lote, 80% ou mais

estão relacionados a phishing, ou o vetor de ataque inicial foi phishing. Assim, ao reduzir o phishing, podemos ter um impacto real nos danos causados por outros crimes com os quais lidamos no dia a dia. Em seguida, o segundo superior parece um pouco com phishing. Mas isso é mais focado em domínios semelhantes, e-mails falsificados e esse lado das coisas. Isso representou apenas sob o resto disso. Obviamente, alguns desses, pode haver um pouco de sobreposição também. Próximo slide, por favor. Mesma pergunta para instituições de caridade e uma resposta muito semelhante. Mais uma vez, 80% de phishing. Uma análise tão forte que, se pudermos ajudar no uso indevido de DNS e combater o phishing, isso terá um impacto muito bom na redução da quantidade de crimes que essas empresas e instituições de caridade estão sofrendo. Próximo slide, por favor.

No Reino Unido, temos um serviço chamado Suspicious Email Reporting Service. Não é só a ICANN que gosta de siglas. Foi criado em 2020 e é um serviço onde indivíduos ou empresas podem denunciar e-mails suspeitos ao governo. Tem os detalhes aí. Eles aceitam encaminhamentos de e-mail e também enviam SMS porque essa é outra grande fonte de relatórios de phishing. Durante 2022, recebemos 6,4 milhões de denúncias nesse serviço. Então, realmente em grande escala. Muitas vítimas no Reino Unido e pessoas relatando isso. Como disse, só lançado em 2020, obviamente como resposta a alguma atividade que se desenrolou durante a pandemia. Mas desde aquele lançamento, tivemos 15,8 milhões de relatórios nesse serviço. E é uma tendência ascendente, mas não há dados suficientes no momento para mostrar isso. Certamente, nos próximos anos, provavelmente colocarei isso em um pequeno gráfico, sem dúvida. Então, relacionando isso ao

governo, o que eles podem ver nessa reportagem, obviamente, é que eles estão tentando fingir ser uma entidade governamental. Então, dentro desses ataques de phishing, eles tiveram representações sobre nosso serviço de saúde, nosso licenciamento de TV, nossas receitas e costumes e, em seguida, o gov.uk. Portanto, há um site onde divulgamos todas as nossas informações públicas, sejam conselhos sobre o que fazer em relação ao COVID, conselhos sobre viagens. Tudo está lá. E então o outro é a agência de licenciamento de motoristas e veículos também. Definitivamente, muitos ataques governamentais e este serviço foram úteis para derrubar alguns deles. Próximo slide, por favor.

Eu falei sobre negócios, mas obviamente, indivíduos e usuários da Internet também serão afetados por isso e nos denunciarão o crime. Houve uma revisão por telefone de várias vítimas que nos relataram para entender qual foi o impacto sobre elas do ponto de vista financeiro. Você pode ver aqui. É um gráfico horrível. Desculpe. Isto é o que me foi dado. Mas você pode ver aqui que uma faixa entre 20 e 250 libras é provavelmente a grande perda das pessoas. Mas quando você pensa sobre isso, não é muito dinheiro. Mas então, tivemos 6,4 milhões, este ano, as pessoas denunciaram um crime. E se você disser que cada um deles perdeu até 20 libras, 20 vezes 6,4 milhões é um bom dia de trabalho ou um bom ano de trabalho. Então, realmente em grande escala quando você olha para isso. Pode parecer um pouco. No entanto, obviamente, especialmente no momento, com a crise do custo de vida que temos em vários países, é realmente impactante para as pessoas perderem esse dinheiro. Próximo slide, por favor. Falamos muito sobre dinheiro em crimes cibernéticos. E não é só o dinheiro que

afeta as pessoas, especialmente os indivíduos aqui. As empresas sofrem perda de dados e isso é impactante para elas. Mas em um nível individual, pode ser realmente impactante e realmente perturbador para eles. Vou apenas fazer um rápido estudo de caso sobre isso. Recebemos algumas informações em nosso sistema policial sobre um jovem de 17 anos que relatou que um hacker estava pedindo mais senhas e tinha acesso a várias de suas contas de mídia social. Conseguimos fazer algum trabalho por trás disso. Conseguimos identificar o suspeito, descobrimos que ele tinha um histórico de invasão de contas de mídia social de vários indivíduos. Então, obtivemos um mandado para visitar seu endereço residencial e encontramos vários telefones ativos que ele usava para cometer alguns desses crimes. Nesses telefones, havia evidências de phishing em massa. Passe para o próximo slide, por favor. Este é um exemplo de uma das comunicações. Você verá aqui que ele representa alguém que encontrou alguma informação sobre um indivíduo e diz: “Encontrei algumas imagens suas em um site. Você pode querer fazer algo a respeito. A pessoa volta e diz: “Qual é o link?” E então esse indivíduo publica um link para eles acessarem. Ao revisar os telefones, encontramos centenas de mensagens enviadas para meninas, em geral, tentando obter acesso às suas contas. Então você vê aqui, de um domínio ou um indivíduo, ele pode ter centenas de vítimas. Não é uma coisa análoga, um domínio, uma vítima. Pode ser um domínio, centenas de vítimas. E tudo depende do tipo de ataque e da maneira como está sendo usado para funcionar. Também examinamos esse site, obviamente, para ver como esse indivíduo o estava usando para extorquir outras pessoas. Passe para o próximo slide, por favor. Este

slide vai ser um pouco ocupado, então peço desculpas antecipadamente, e um pouco pequeno, mas é pequeno por um motivo. No canto superior direito da tela está um serviço de phishing hospedado na Internet que oferece aos usuários registrados a capacidade de comprar páginas de phishing e de tê-las na Internet. Então você clica em um deles, seja Netflix, Facebook, Snapchat ou qualquer outra coisa. Você pode até selecionar o idioma em que deseja. Muito pequeno aqui, mas há inglês, espanhol, francês e russo, acho, tudo lá. Assim, você pode selecionar os idiomas em que deseja aparecer. Você paga por esse serviço.

E então, no canto inferior esquerdo, há um exemplo de Snapchat. Ele criará um domínio malicioso que você poderá anexar à sua mensagem. Isso colherá os detalhes para você. A imagem inferior é um exemplo do painel que eles criam, onde você pode acessar e ver todas as suas credenciais coletadas. Obviamente, uma vez que colhem essas credenciais, é aí que começam a fazer a extorsão. Eles pegam as imagens que estão lá armazenadas, sejam elas particulares, se foi um Google Drive, se não é nem compartilhada nas redes sociais. Portanto, isso tem um grande impacto nas pessoas. Conseguimos tirar este site do ar com o apoio dos registradores. Obrigado por isso. O indivíduo envolvido vai a tribunal no próximo mês, mas neste momento encontra-se em prisão preventiva devido à ameaça que representa para o número de vítimas. Nisso, é muito importante. Obviamente, tentamos entrar em contato com todas as vítimas que conseguimos identificar e dizer a elas que protegemos seus dados, removemos e sugerimos que atualizem suas senhas e tudo mais. É muito importante entender esse impacto para eles. Nós tivemos tanto, “Oh, obrigado por

fazer isso. Eu não sabia como lidar com isso.” E é realmente importante saber como lidar com isso e como remover alguns dos danos causados. Então, para o próximo slide. Acho que vou passar para Gabe.

LAUREEN KAPIN: Estou me perguntando onde estamos em relação à apresentação de nosso colega Bertrand. Você está pronto para ir? Você prefere ir agora? O que você acha?

CHRIS LEWIS-EVANS: Acho que faremos o de Gabe porque segue bem. Então vamos parar de volta. Desculpe. Eu tenho mais um slide. Este é apenas um resumo dos dados corporativos e individuais juntos. O relatório mais recente foi de 2020 a 2021. No Reino Unido, eles receberam 875.000 denúncias de fraude e crime cibernético. Desculpe. Isso deve ser ambos combinados. Isso representa 2,35 bilhões de perdas nesse relatório. Então, 80% dessa fraude também foi habilitada para o ciberespaço, seja de um e-mail de phishing ou de outra forma. Portanto, uma grande quantidade dessa perda se deve a alguma forma de atividade cibernética. E, como dissemos antes, e-mails de phishing, 80% provavelmente, um grande facilitador para os criminosos usarem para iniciar seus ataques cibernéticos. E esse definitivamente é o último slide antes de eu passar para Gabe.

GABRIEL ANDREWS: Podemos ver o próximo slide? Obrigado. Do ponto de vista dos EUA. E, novamente, como Chris disse, realmente esperamos que haja outras

pessoas por aí que possam encorajar suas agências de aplicação da lei a compartilhar perspectivas de todo o mundo. O FBI acaba de lançar, na semana passada, seu Relatório de Crimes na Internet para o ano civil de 2022, então isso está no ar. É também por isso que acho que poder falar sobre isso anualmente é uma coisa boa, porque gostamos de poder compartilhar essas informações quando elas são lançadas e enquanto são recentes. Esses dados são um resumo de todas as reclamações de vítimas que chegam ao nosso Centro de reclamações sobre crimes na Internet. É o portal centralizado pelo qual recebemos e agregamos todos esses números. Então eles se viram e publicam relatórios baseados nisso. Mas observe que esta não é uma imagem de todos os crimes na Internet que existem. É apenas isso que nos é relatado. Próximo slide, por favor. Nos últimos cinco anos, o IC3, novamente, abreviação de Internet Crime Complaint Center, recebeu uma média de cerca de 650.000 reclamações por ano. Isso dá uma média de pouco mais de 2.000 reclamações por dia, então é um número justo. Mas ainda sub-representa grosseiramente a verdadeira quantidade de crime que existe por aí. Sabemos que não recebemos todas as reclamações o tempo todo. Uma coisa que é interessante notar aqui é que quando você olha para o número de reclamações reais, essas são as pessoas que nos procuram, ele ficou relativamente estável nos últimos três anos, o que é interessante. Mas o volume das perdas aumentou constantemente. Eu gostaria de ter uma boa explicação para você sobre o porquê disso. Não temos uma explicação muito boa sobre isso no momento, mas é definitivamente algo interessante de se notar. Isso mostra que o dano continua, mesmo que o número relativo de denúncias permaneça estável. Continue no próximo slide. Como Chris

mencionou em suas categorias de crime e como elas as agregam, também não rastreamos o uso indevido de DNS como uma categoria. Mas há categorias de uso indevido de DNS que são rastreadas em nossos relatórios IC3.

E noto aqui em particular, na parte inferior, phishing. Quando examinamos as cinco principais categorias de crimes na Internet relatados a nós, vemos que o phishing é a principal categoria. Além do mais, como isso mostra nos últimos cinco anos, você pode ver que, por algum motivo ou outro, o phishing aumentou tremendamente de cinco anos atrás para onde está hoje, pelo menos em termos de reclamações que recebemos. Próximo. Novamente, isso mostra apenas todas as categorias de crime, não apenas as cinco principais, e mostra como o phishing se relaciona com elas. Algo a destacar aqui, como Chris já mencionou, é que o phishing, embora seja rastreado como uma categoria própria, geralmente é o método inicial que os bandidos usam para comprometer as vítimas de uma série de outras categorias de crimes que existem aqui como bem. Apenas como exemplo, você pode perguntar: “O ransomware é um uso indevido de DNS?” Não, não é. Ransomware é quando um bandido leva seus dados em sua máquina, eles os criptografam e não permitem que você os obtenha, a menos que você pague um resgate. Mas se você fizer a pergunta: “O ransomware é espalhado por phishing?” a resposta para isso é sim. Há um relatório que acabou de sair na semana passada sobre uma nova variante de ransomware chamada Royal ransomware da CISA, uma das minhas agências irmãs. Neste relatório, eles estimaram que 67% das infecções de ransomware Royal vieram de phishing. Novamente, estamos rastreando a categoria inicial lá, mas ela tem um impacto a jusante.

Assim, só para reforçar o ponto, quando nossos amigos, colaboradores e colegas da comunidade da ICANN que existem no nível de registrador ou registro tomam medidas antiabuso responsáveis para lidar com domínios registrados maliciosamente que são usados em phishing, eles estão ajudando para abordar não apenas o tipo de crime na Internet mais comumente relatado que chega até nós, mas também todas as outras categorias que são possibilitadas por ele. Próximo slide. Além de compartilhar essas estatísticas do relatório anual, também perguntei a alguns de meus colegas: “Ei, qual é a novidade? O que há de novo, futuro e definição de tendências? O que é notável nos últimos meses?” O que eles voltaram para mim foi algo que eles chamam de “ malvertising ”. Para benefício dos tradutores, trata-se de uma combinação de malware e publicidade. Ele recebeu muita atenção, começando em dezembro do ano passado e bem nos primeiros meses deste ano. Como no phishing, o bandido aqui obtém um nome de domínio parecido que é registrado para fins abusivos.

Às vezes, eles recebem um nome de domínio que pode parecer um pacote de software, alguma outra marca confiável ou algum serviço. Mas, em vez de usar isso no e-mail, eles vão aos provedores de mecanismos de pesquisa e compram anúncios. Nesse caso que você vê na tela aqui, isso vem do Abuse CH. Peguei no feed do Twitter deles. O bandido neste caso está fingindo ter um site associado ao cliente de e-mail Thunderbird legítimo. É um tipo de software que muita gente gosta. Mas, obviamente, eles não estão compartilhando apenas pela bondade de seu coração. Se você fosse ao site de publicidade dele lá no topo, você obteria esse software mais malware em sua máquina, neste caso, IcedID. É uma forma de Trojan bancário. Se estivesse instalado em

sua máquina, eventualmente capturaria quando você fizesse login em seu banco, roubaria essas credenciais de login e tentaria drenar as contas. Portanto, essa nova tendência é interessante porque ainda depende desses domínios registrados com códigos maliciosos. É phishing, por si só? Provavelmente não porque não há nenhuma conexão de e-mail lá. Mas ainda tem o mesmo resultado final. Eu digo isso porque: um, é novo; dois, porque tem ligação direta com o DNS; mas três, também porque acho importante reconhecer que temos que ser um pouco ágeis e ágeis em responder às verdadeiras situações do mundo e estar dispostos a incorporar essas novas tendências em nossas ideias sobre o que podemos abordar. Mas, como antes, os registradores responsáveis que agem contra domínios registrados com códigos maliciosos também estão lidando com isso, e isso é bom. Próximo slide. E este será meu último slide. Eu só quero realmente enfatizar o ponto. Em inglês, diríamos “batendo um cavalo morto” aqui. Mas o phishing é comumente aceito entre todos os membros da nossa comunidade aqui na ICANN como uso indevido de DNS. É também, como acabei de saber em nosso relatório mais recente, atualmente o tipo de crime na Internet mais relatado. E o phishing permite muitos outros crimes. A ação rápida contra domínios registrados com códigos maliciosos e o incentivo que podemos fornecer por meio de nossas políticas aqui para isso é importante. Afeta o que vemos. Essa é a minha principal conclusão e agradeço sua atenção. Acho que agora que Bertrand está aqui ao meu lado e pronto, podemos fazer a transição para ele.

MANAL ISMAIL: Sim, por favor, Bertrand. Vá em frente. E muito obrigado à Internet e Jurisdição por sempre entrar em contato com o GAC e nos manter informados sobre o trabalho que vocês fazem em relação ao uso indevido de DNS, que obviamente é um tópico de grande interesse para o GAC. Obrigado.

BERTRAND DE LA CHAPELLE: Muito obrigado, Manal. É um prazer estar de volta ao GAC porque estive lá como representante da França muitos anos atrás, inclusive como vice-presidente do GAC. Vejo alguns rostos familiares daquela época. É um prazer ter a oportunidade de apresentar aqui. Sou o diretor executivo da Internet and Jurisdiction Policy Network, uma organização que fundei há 10 anos. E estou muito feliz em vir aqui falar sobre esse debate que anima a comunidade da ICANN há vários anos e mostrar um pouco no que estamos trabalhando para ajudar o debate a avançar e buscar soluções. Internet and Jurisdiction Policy Network, e Ajith Francis, que está aqui atrás, é o diretor de programas lá. Somos uma iniciativa de múltiplas partes interessadas, reunindo governos, empresas, operadores técnicos, academia, sociedade civil e organizações internacionais para lidar com os desafios jurisdicionais na Internet. Temos, em particular, três programas que não vou me alongar sobre os dois primeiros. Mas um deles é dedicado sob o rótulo de domínios e jurisdição, à questão de exatamente quando é apropriado atuar no nível do DNS para lidar com abusos? E há um grupo de contato que já funciona há mais de cinco anos com cerca de 40 pessoas de diferentes comunidades. Fico muito feliz em dizer que o Manal tem sido muito gentil, e outras pessoas aqui, inclusive a Susan, têm participado

ativamente do trabalho. Estou particularmente grato a ela, dada a grande carga que ela carrega, por ter dedicado seu tempo para participar. Era importante. Basicamente, o que importa é o que estamos falando aqui, como combatemos os abusos que existem online? Esses abusos são extremamente diversos. A apresentação diante de mim mostra que a engenhosidade humana é absolutamente ilimitada. Qualquer forma de usarmos mal alguma coisa será mal utilizada. Nós todos sabemos isso. Portanto, o principal desafio é que, na maioria dos casos, e esse é o segundo ponto, esse é um problema transnacional. É particularmente interessante falar sobre isso no GAC porque vocês são representantes governamentais. Eu fui um representante governamental. E todos nós sabemos que a razão pela qual temos problemas para lidar com os abusos online é porque não temos as ferramentas de cooperação entre os governos para agir transnacionalmente. Temos uma arquitetura internacional baseada na separação de soberanias e a cooperação é extremamente difícil. Um dos programas que temos trata do acesso transfronteiriço a evidências eletrônicas. É uma questão extremamente problemática e leva anos para organizar o devido processo entre os países para conduzir investigações usando evidências eletrônicas. Portanto, o problema que enfrentamos é que não apenas a rede é global, não apenas os atores trabalham livremente além das fronteiras, mas as ferramentas que temos para lidar com isso não são eficientes e não estão aqui para facilitar a cooperação intergovernamental. A próxima coisa é que, para resolver esses problemas, é necessário entender melhor como a própria Internet funciona. Quando falamos sobre o sistema DNS, há uma falta de compreensão em muitos círculos, com os quais você

provavelmente está familiarizado quando fala com colegas, sobre como essa arquitetura funciona. Se você quiser entender como entrar em contato com um registrante, saber como funciona o WHOIS, que você encontrará o registrador e assim por diante. Isso não é algo muito fácil. A próxima coisa, ainda mais importante, é que eu estava falando da falta de ferramentas, mas também há uma questão de competências. Os operadores de DNS são apenas aliados básicos, disponibilizando nomes de domínio. Eles não têm nenhuma competência para examinar, fundamentalmente, se algo é phishing, se é malware, então eles dependem de notificadores. É ainda pior quando falamos de abusos relacionados a conteúdo. Como você consegue avaliar a legalidade do conteúdo de uma colcha de retalhos de jurisdições. Estou mencionando recursos porque investigar qualquer caso único leva tempo. Esta é uma indústria relativamente lenta e com margens pequenas. O ponto principal é que este é um problema para todos. É um problema para os governos porque vocês estão preocupados, legitimamente, que os abusos não sejam combatidos. É um problema para as empresas porque elas também são vítimas ou têm um fardo em lidar com essas coisas. E é um problema para os usuários. Então, a próxima coisa é que precisamos entender algo que é básico.

Todos vocês estão familiarizados com isso, mas quero compartilhar isso que compartilho frequentemente com pessoas fora de nosso próprio ambiente, porque elas não necessariamente sabem exatamente como o sistema funciona. Portanto, a relação entre o registrante, os registradores, os registros e os usuários; as consultas que vão de um para o outro; e os papéis que os diferentes atores

desempenham para fazer com que a Internet funcione da maneira que queremos. Esta é uma arquitetura na qual não vou me alongar. O ponto que quero enfatizar é que existem apenas quatro ações que os operadores de DNS podem realizar em relação aos nomes de domínio. A primeira é que você pode bloquear o domínio. Basicamente, você não pode alterar as informações fornecidas pelo registrante. Você não pode ter transferência, exclusão, modificação. E você não pode alterar o servidor ou o endereço IP mencionado. É importante ressaltar que essa ação não torna o conteúdo inacessível. Particularmente, você pode bloqueá-lo. É bom para a investigação depois. Mas não muda nada em relação ao funcionamento. O segundo elemento é que você pode segurar. A esse respeito, você pega o nome de domínio, remove do arquivo de zona TLD pública e o domínio não resolve. Você também não pode alterar as informações sobre o servidor. Mas aqui, novamente, o sistema ainda funciona. Se você usar o endereço IP, ainda poderá ter acesso ao elemento.

O terceiro elemento é o redirecionamento. Isso geralmente é usado para identificar um determinado nome de domínio quando você deseja conduzir uma investigação. É basicamente editar o arquivo de zona para redirecionar para outro servidor para observar o comportamento, identificar as vítimas e coisas assim. O quarto elemento é a transferência, quando você coloca isso em outro registrador. Isso pode acontecer quando o registro foi feito de maneira errada em um determinado registrador. Mas, seja qual for o motivo, há interesse em colocá-lo, por exemplo, em um registrador de última instância, algo em que Benedict Addis está muito envolvido. O próximo slide é importante porque essas são as quatro coisas. Você pode excluir, mas não insisto

em excluir porque não é uma ação recomendada por vários motivos. A questão-chave é: atuar no nível do DNS, com apenas essas quatro coisas, é o instrumento certo para lidar com os abusos? A resposta é sim, em alguns casos, e não em outros. Não é a panaceia perfeita. Não é basicamente o que algumas pessoas fora de nossas comunidades tendem a considerar como uma espécie de grande painel de controle. Como se você tivesse um problema em um nome de domínio ou anexado a um nome de domínio, basta ligar o botão e o problema desaparece. Este não é o caso, mas ainda assim é útil ter ações em certos casos. Portanto, os problemas-chave, ou as questões-chave, são os seguintes. Em primeiro lugar, é um instrumento que abrange não só o serviço de acesso a um site de nomes de domínio, mas também uma série de serviços auxiliares. Isso pode ser e-mails, transferência de arquivos e outras coisas. Portanto, é um instrumento muito contundente.

A segunda coisa é que tem um impacto global. Está cobrindo o mundo inteiro. Você não finge. Você não bloqueia geograficamente a suspensão do nome de domínio. Aqui, é interessante porque você pode ver isso como um recurso ou um bug. Como um bug, tem um impacto global, portanto não é granular. Mas quando conectado ao que eu estava dizendo antes, faltam-nos as ferramentas para a cooperação internacional. Ter algo que tenha um efeito global é benéfico em certos casos. A próxima coisa é, como eu disse, você ainda pode acessar a maioria dos serviços por meio do endereço IP. Em seguida, você está em uma situação em que os operadores de DNS fazem parte de um ecossistema maior. Precisamos levar em consideração a arquitetura geral, incluindo provedores de hospedagem, ISPs e outros atores que

também podem ter ações. Agir no nível certo é o mais importante. O próximo ponto é que, atualmente, nos Contratos de Credenciamento de Registradores e Registros com a ICANN, há uma obrigação de haver pontos de abuso e de investigação, mas há um número limitado de obrigações que esclarecem o que é realmente exigido e o que é realmente necessário. Isso leva à situação que testemunhamos por um longo período de tempo, que houve e tem sido um debate prolongado dentro da ICANN, por muitos anos, principalmente em torno da própria palavra "uso indevido de DNS" e a definição do que significa. As pessoas estavam tendo posições muito diferentes a esse respeito. Tantas sessões por vários anos em torno disso. Crítica entre os diferentes constituintes sobre se a definição é esta ou aquela. E até mesmo tensões dentro dos diferentes constituintes sobre quanta ação deve ser tomada ou não.

Não é para dizer que eles são maus atores. Sabemos que existem maus atores. Há atores que são mais responsáveis do que outros. Mas, claramente, não havia como avançar para um consenso lá. O resultado foi esse sentimento de frustração. O ponto principal é que, se você fizer a pergunta errada, é improvável que tenha a resposta certa, o que exige reformular o problema. Reformulando, para o próximo slide, a verdadeira questão é quando é apropriado agir no nível do DNS para lidar com abusos online? Acho que esta é uma formulação que pode ser aceita por todos como uma formulação válida que leva em conta os diferentes elementos. Como parte dessa reformulação, trabalhamos com o grupo de contato que mencionei anteriormente por um longo período e reduzimos a compreensão do uso indevido de DNS, que chamamos de abuso técnico em determinado momento. Mas, com a

ajuda de alguns dos atores, reduzimos a noção de que o uso indevido de DNS deve ser considerado como essas cinco coisas: circulação de malware, botnets, phishing, pharming e spam na medida em que é usado como um mecanismo de entrega para os itens acima. Você pode encontrar mais detalhes sobre as definições dessas cinco coisas, primeiro nas abordagens operacionais que I&JPN produziu em abril de 2019. Isso levou à incorporação dessas definições de uso indevido de DNS na Estrutura para abordar o abuso que foi produzida por um certo número dos atores da comunidade em dezembro de 2019 e, posteriormente, o relatório SSAC 115 em 2021 que incorporou essa definição de uso indevido de DNS. Pode não ser a definição perfeita, mas é um elemento muito importante fazer uma distinção entre isso, que podemos chamar de uso indevido de DNS, que todo ator está entendendo tem um motivo para ser investigado e é da competência dos operadores, desde conteúdo - abuso relacionado que abordarei mais tarde. Nesse contexto, produzimos, e não vou entrar em todos os detalhes, mas um kit de ferramentas em 2021 que encorajo você a ir e ver online para ajudar os operadores de DNS, os notificadores e os legisladores ou as autoridades policiais a entender os diferentes parâmetros e tendo elementos de orientação para convergência e trabalho em conjunto. O próximo slide menciona um elemento importante que é o fluxo de trabalho em torno de quatro elementos para lidar com qualquer tipo de abuso. A primeira é basicamente a identificação do abuso em si. Pode ser de notificadores ou das próprias operadoras. A segunda é a avaliação desse abuso. Está de fato justificando uma ação no nível do DNS? A terceira é qual é a ação que deve ser tomada entre as quatro que mencionei? E o quinto é algo que

ainda não discutimos, mas faz parte do cenário, que são as vias de recurso quando há uma decisão tomada e que deve ser alterada, por qualquer motivo. Erros podem acontecer. Sem nos alongarmos muito, para cada uma dessas etapas, produzimos um certo número de coisas, como definir mais claramente os tipos de abusos. Mencionar elementos sobre o que os notificadores devem fazer, em termos de devida diligência, para documentar esses elementos. Não basta lançar um aviso sem nenhuma evidência sustentável. Quais são as condições para notificar o registrante, principalmente quando os sites estão sendo comprometidos?

Na avaliação, há uma questão-chave de quais são os limites, os critérios de ação? Quando é necessário atingir um limite? E escolha de ação. Existem diferentes tipos de ação, como mencionei. E há um documento que explica com precisão os desenhos que mostrei antes. Por último, sobre o recurso, coloca-se a questão dos canais de recurso e elementos relativos à transparência. Este é um processo. Tudo o que está ligado às investigações para tentar remediar o abuso passa por diferentes etapas que envolvem a cooperação entre os diferentes atores. Se eu for para o próximo slide, nesse contexto, o grupo de contato produziu uma série de documentos que espero que sejam úteis para vocês como comunidade, mas que sejam úteis para o debate geral. A primeira é sobre o que os avisos devem conter? Quais são os componentes para avisos que suportam evidências? A segunda é quais são os tipos de notificadores? É o mesmo ser um notificador de imagens de abuso sexual infantil ou de violação de marca comercial, por exemplo? A próxima coisa é, como eu disse, qual é a devida diligência que os notificadores devem realizar para garantir que o ônus da validação não

seja inteiramente dos operadores? Qual é o tipo de acordo que pode ser feito entre os notificadores confiáveis? Quais são os arranjos dos notificadores confiáveis? Quero fazer um esclarecimento aqui. Ninguém pode dizer, por conta própria, “Sou um notificador confiável”. Na melhor das hipóteses, você pode dizer: “Tenho experiência nesse campo específico que me torna um notificador especialista”. Uma relação de notificador confiável é um reconhecimento bilateral. Você pode ser um notificador confiável para um operador, mas não para outros. É uma distinção importante e precisamos trabalhar mais a noção dos notificadores.

Um documento dedicado está abordando a questão das botnets. Não tenho tempo para entrar em detalhes. Mas há uma questão muito importante que é chamada de domínios gerados por algoritmos. Encontrar uma melhor cooperação entre a aplicação da lei, ICANN e os operadores de DNS em torno de domínios gerados por algoritmos é um elemento muito importante. Acho que esse documento ajudou a levar a discussão um pouco adiante. Por fim, em relação a phishing e malware, trabalhamos com o grupo de contato para criar um fluxo de trabalho gráfico claro sobre qual é a distribuição de funções nas diferentes etapas entre registros e registradores. Quais são os canais de informação e assim por diante? Estou extremamente feliz em mencionar isso aqui porque Graeme Bunton está aqui no canto e alguns de vocês já o viram antes. Deu origem a duas grandes iniciativas que estou extremamente feliz por terem sido construídas a partir do trabalho desenvolvido no I&JPN, a criação do DNS Abuse Institute, graças à ajuda do PIR, e a produção neste contexto de algo que nós havíamos discutido dentro do grupo de contato, que é uma interface

para denunciar abusos, agora chamado NetBeacon. Jeff Bedser tem sido fundamental para que isso aconteça. Brian Cimbolic está perto dele para o PIR. Brian é, na verdade, o coordenador do grupo de contato que temos em I&J. Este trabalho é surpreendente para mim porque é o resultado de cinco anos de trabalho que conduzem a um elemento muito concreto, algo que é operacional, que não é apenas discussão ou papel. É realmente algo operacional. Grande gorjeta de chapéu para aqueles que estão levando a tocha adiante.

Isso é importante porque, além disso, também levou às discussões que estão ocorrendo aqui durante este ICANN76 sobre a melhoria do Contrato de Credenciamento. Então eu encerro essa parte e tenho uma bem curtinha depois. Trata-se de uso indevido de DNS, entendido como os cinco elementos sobre os quais estávamos falando. Próximo slide, por favor. Acho que, em resumo, há um acordo entre os atores responsáveis de que o uso indevido de DNS, entendido dessa forma, é algo que é de fato algo que geralmente se justifica agir no nível do DNS quando há evidências substanciais, a menos que o site tenha sido comprometido ou há outras coisas. Mas, de um modo geral, estamos vendo o movimento em uma direção positiva em direção à cooperação implementável. A última parte que quero abordar, que está mais em andamento no momento, é a questão do abuso relacionado ao conteúdo, que é muito mais complexo porque aqui a imagem é um pouco espelhada. De um modo geral, o nível do DNS não é o lugar certo para lidar com o abuso relacionado ao conteúdo por vários motivos, incluindo o fato de não ser granular o suficiente. É difícil ter algo que esteja de acordo com as ilegalidades de uma região ou de outra. A competência para avaliar se há abuso é muito diferente. Não é uma

coisa técnica que os operadores saibam. E de um modo geral, não é uma ferramenta eficiente porque o conteúdo permanece disponível na maioria dos casos. Mas há, no entanto, um certo número de situações que são suficientemente excepcionais para justificar uma ação no nível do DNS quando são atendidas. E nas abordagens operacionais que produzimos em 2019, antes da conferência global que organizamos em Berlim, existem quatro elementos, muito provisoriamente, que podem ser levados em conta para adivinhar ou avaliar quando é apropriado atuar no nível do DNS para conteúdo relacionado Abuso. É o quão globalmente aceito é que o conteúdo em questão é ilegal? Aqui você tem uma graduação completa entre coisas que são, CSAM, por exemplo, em um extremo de uma certa forma e coisas que são extremamente diversas em termos de legislações ao redor do mundo. Grande variedade sobre o que é ilegal e o que não é. A proporção do site dedicada ao conteúdo infrator. A intenção ou má-fé do registrante ou do operador do site.

E também, se os outros níveis foram esgotados ao ir para o operador do site, o registrante ou o provedor de hospedagem. Eu não me alongo sobre isso, mas é importante realmente fazer uma distinção entre essas duas categorias de coisas. Ambos são importantes, mas não devem ser tratados exatamente da mesma maneira. Um dos grandes desafios é que não temos espaço para discutir esse segundo problema. A ICANN é o lugar certo para discutir a questão do uso indevido de DNS da maneira como descrevemos antes. Mas ficou muito claro que, de acordo com o mandato, e a comunidade está totalmente de acordo com isso, não é o lugar para discutir abuso relacionado a conteúdo. Tem havido postagens consistentes em blogs sobre “a ICANN não é a polícia de

conteúdo" etc. E isso é totalmente compreensível. O problema é que não há muito mais onde isso possa ser discutido. É por isso que, no último mês de maio de 2022, uma parte significativa das pessoas que participaram do grupo de contato do I&J nos pediu para ser basicamente o local onde a discussão sobre abuso de conteúdo do site poderia ser explorada para essas circunstâncias excepcionais, encontrando os limites, critérios e mecanismos. É nisso que embarcamos este ano. É preliminar. Está apenas começando. Mas acho importante para esta comunidade do GAC ter uma visão geral e entender que a ICANN está realmente avançando com base no trabalho que realizamos coletivamente sobre a questão do uso indevido de DNS. Não é perfeito e tem que ser implementado e tem que ser fortalecido. Mas está realmente avançando nesse sentido, melhor clareza, melhores mecanismos e melhor cooperação. Sobre abuso relacionado a conteúdo, embora não seja dentro da ICANN, nós, como I&JPN, continuamos essa atividade em torno dos seguintes elementos que são o próximo slide. Primeiro, a camada DNS para abuso relacionado ao conteúdo é acionada porque há um motivo absoluto para ir diretamente para lá ou porque é o último recurso depois de esgotar outros níveis na pilha. E a questão de como entrar em contato com o operador do site, o registrante, o provedor de hospedagem? Qual é o caminho de escalonamento é a primeira discussão. O segundo elemento é como formular os critérios de limite.

Para dar um exemplo, você pode dizer: "Todo o site deve ser dedicado ou é dedicado ao conteúdo ou atividade infratora". Ou você pode dizer: "Não há outro conteúdo legítimo no site além deste". Ou você pode dizer: "A intenção do operador do site é fazer x, y e z". As formulações

são importantes e estamos facilitando essas discussões. Finalmente, a noção de acessibilidade é interessante. No momento em que dizemos que há um caminho de escalonamento, como você envia um aviso e como entra em contato com o registrante, ou o operador do site, ou o provedor de hospedagem para esse assunto? Isso é algo que vamos explorar com mais detalhes porque não há um equivalente claro do WHOIS para provedores de hospedagem. Descobrir onde um determinado site está realmente hospedado é um pouco mais complicado do que apenas descobrir quem é o registrador. Finalmente, mencionei a noção de acordos de notificação confiável. É um ponto extremamente importante porque especialmente para o abuso relacionado ao conteúdo, ainda mais do que para o phishing, mas para o abuso relacionado ao conteúdo, não haverá solução para isso sem a cooperação entre as três categorias de atores, a aplicação da lei, os notificadores de vários tipos que devem aumentar sua capacidade e credibilidade, e os operadores de DNS em acordos existentes. Como um trocadilho para aqueles de vocês que se lembram da formulação da afirmação de compromissos entre a NTIA e a ICANN antigamente, acredito que existe um conceito de estrutura que é a afirmação mútua de compromissos. Precisamos ter mecanismos que reúnam notificadores com competência e procedimentos de devido processo legal, agentes da lei que facilitem a cooperação e operadores para lidar com os casos em que é apropriado atuar no nível do DNS. Quero destacar que não estamos falando aqui de regulamentação de grandes plataformas. Não é Facebook. Não é o Twitter deste mundo. Você não vai pedir para derrubar o Facebook.com porque há algum conteúdo em um dos subgrupos que estão lá. Mas quando alguém cria um site por

trás de um nome de domínio para ter uma intenção maliciosa, encontra essas pessoas e basicamente interrompe o exercício maluco de apenas pará-lo aqui e pará-lo ali, e seguir em frente para capturar as pessoas que estão realmente fazer essas coisas é a importante cooperação necessária. Portanto, minha conclusão é que essa é uma responsabilidade compartilhada. Isso é algo que requer a cooperação entre os diferentes atores. O lema da Internet and Jurisdiction é "permitir a cooperação de várias partes interessadas".

Fazemos isso facilitando a formação de um certo número de acordos. Estamos muito felizes com o progresso no ambiente da ICANN. E é a única maneira de abordar essas questões. Você tem, nos slides, deveria ter um slide antes. Desapareceu. Eu vou reintegrá-lo. Há um slide com todas as conexões e links para os documentos que apresentei. No último slide, aqui estão meus dados de contato e os contatos de Ajith Francis, caso você queira conversar conosco sobre isso depois. Muito obrigado pela oportunidade de apresentar.

MANAL ISMAIL: Muito obrigado, Bertrand, pela apresentação tão completa, bem estruturada e informativa. Antes de passar isso para os líderes de tópicos do GAC, quero apenas reconhecer uma mão muito paciente no Zoom do Irã. Você quer ir primeiro? OK. Kavouss, só um segundo. Chris e depois passo a palavra. Desculpe.

CHRIS LEWIS-EVANS: Obrigado, Manal. Eu só ia sugerir, na verdade. Recebemos muitas informações, muitos de nós conversando. Talvez, se você tiver alguma

reflexão ou alguma pergunta para nós sobre as últimas apresentações, seria bem-vinda agora. Em seguida, abordaremos as atividades em andamento na comunidade da ICANN e as considerações sobre a linguagem do comunicado de Cancun. Isso também terá perguntas. Mas talvez apenas nas duas últimas apresentações que fizemos, algumas perguntas e reflexões seriam boas agora. Obrigado.

MANAL ISMAIL: Muito obrigado, Chris. Kavouss, alguma coisa na primeira parte desta sessão, seja para tópicos ou para Bertrand? Por favor, vá em frente.

KAVOUSS ARASTEH: Muito obrigado, Manal. Deixe-me expressar meus sinceros agradecimentos às pessoas no pódio. Essa foi, na minha opinião, uma das discussões mais interessantes que tivemos sobre uso indevido de DNS. Embora eu não queira fazer uma comparação entre os diferentes, mas a última parte, para mim, foi muito interessante. Como mencionei ontem, temos problemas. E nós resolvemos os problemas. O que eu recomendo, primeiro, distinto presidente, você e Nicol, o presidente do GAC para o futuro, precisamos colocar na agenda do GAC da próxima reunião mais tempo para este assunto. Não é possível, superficialmente, vir alguma coisa e não ir ao cerne do problema como fizemos hoje para ver o que somos. Há muitas coisas para se ter. Não sei. Não temos tempo agora que eu explico. Eu tenho algumas sugestões. Não sei o que você me sugere. Mas há um caminho a seguir. Mas acho que quero abordar apenas um dos pontos. O distinto amigo à direita do pódio mencionou a cooperação intergovernamental. Isso foi

discutido muitos anos. Não é um problema da ICANN porque a ICANN não é intergovernamental e o GAC não é intergovernamental.

O GAC é o Comitê Consultivo Governamental. Os governos são intergovernamentais. Eles estão em outro lugar, mas não aqui. E eu sinto muito. Sou muito franco com todos. Muitas vezes, queríamos abordar essa questão, a cooperação intergovernamental. Alguns governos se opuseram a isso, dizendo que o cibercrime é um problema nacional e não deve ser tratado internacionalmente. E eles disseram que qualquer cooperação intergovernamental poderia ser útil se firmada em um tratado. E não é possível ter um tratado sobre isso. Então vamos ao fundo da situação, não nesta sessão porque estamos no final da reunião. Vamos, distinto presidente do GAC, se possível, discutiremos o assunto um pouco mais para ver o que podemos fazer. Muitos bons pontos foram levantados. O que, até agora, foi levantado é principalmente levantar os problemas. Mas ainda assim, soluções não são propostas. Aquilo é importante. Às vezes, eu diria, não é muito fácil, mas é fácil levantar o problema. Mas é mais difícil sugerir soluções. Onde estão as soluções? Temos que adotar uma abordagem mais pragmática, não para a parte legislativa para ver o que podemos fazer. Categorizá-los, no grau de prioridade, o que podemos fazer. A cooperação intergovernamental, por enquanto, não é tão fácil de abordar. Mas há muitas outras coisas para resolver e assim por diante. Recebemos relatórios do Reino Unido e dos EUA. Poderíamos perguntar a todos os membros do GAC: “Vocês têm a mesma experiência? Qual é o relatório? Já enfrentei, mas nunca denunciei. Eu pessoalmente, no meu e-mail muitas vezes, eu disse ontem. Teve outro dizendo que tinha carro diplomático com 10% do preço. Não abri

porque meu filho é muito esperto. Disse-me: “Papai, não abra nenhuma dessas coisas. Não abra. Se você recebeu um e-mail e não conhece o remetente, não o abra. Posso não ser bom, mas não abra isso”. E depois há outras abordagens. Alguns dos provedores de e-mail, eles têm a segurança dupla, que se sua senha e assim por diante forem pegas por alguém, além de sua área de trabalho ou equipamento, ninguém poderá usar isso porque eles pedem a segunda abordagem, a segunda segurança. Portanto, temos que fornecer alguns bons conselhos às pessoas como precaução preliminar. Quais são essas coisas que pelo menos reduzem quantidade disso? Então, isso é algo que temos que discutir. Há muitas outras coisas que eu tenho, mas não há tempo. Então me desculpe, isso é tudo. Obrigado.

MANAL ISMAIL: Muito obrigado, Irã. Se me permite, Chris, temos mais dois pedidos de palavra e talvez você possa reagir um pouco. Temos apenas 20 minutos restantes e eu tenho a República Democrática do Congo e depois os EUA. Por favor, vá em frente. República Democrática do Congo, por favor.

BLAISE AZITEMINA FUNDJI: Muito obrigado. Obrigado a todos os oradores presentes. Eu gostaria muito, como o Kavouss, de mencionar o quão importante é esta apresentação. Do ponto de vista do governo, para a maioria dos governos e principalmente da África, acho que as expectativas de nosso governo de ter um delegado no GAC é principalmente para lidar com esse tipo de abuso. Minha pergunta ou comentário será

principalmente, é claro, obviamente, o título ou o tópico aqui é abuso. Mas eu realmente gostaria de perguntar se há alguma ação que possa ser feita pelos governos para prevenir. Claro, estamos falando de cura, de cura. Mas como você sabe, em francês, dizemos: “Il vaut mieux prévenir que guérir.” Existem algumas ações em que a ICANN pode aconselhar? Claro, estamos falando de questões de segurança cibernética onde a soberania das nações está envolvida. Mas mesmo em termos de aconselhamento, principalmente para empresas e principalmente para governos, quais são os conselhos? Como podemos evitar que isso aconteça? Vimos algumas apresentações do FBI e principalmente também da experiência do Reino Unido. Eu entendo que existem alguns estudos. Existem algumas estatísticas que podem ajudar a entender por que temos esse tipo de abuso. Sabemos que, do lado dos usuários finais, é principalmente phishing. É e-mail, comprometimento de senha. Mas para empresas e principalmente governos, existem algumas ações que podem ser feitas para prevenir do que esperar que o abuso seja curado ou curado? Obrigado.

MANAL ISMAIL: Muito obrigado, Congo. Eu tenho EUA e França. Por favor, muito brevemente. Depois vou passar a palavra para Chris. Estados Unidos, por favor, vá em frente.

SUSAN CHALMERS: Muito obrigada, Manal. Na verdade, fico feliz em ceder a palavra para que a pergunta do nosso colega seja respondida. Obrigado.

MANAL ISMAIL: Muito obrigado, EUA. Eu tenho a França e depois vou entregá-la a você. Tudo bem, Chris? França, por favor, vá em frente.

JONAS ROULE: Em primeiro lugar, gostaria de agradecer a todos os palestrantes por suas apresentações. Estou honrado por estar aqui substituindo meu colega anterior. Eu só queria intervir, só contribuir com as discussões. Sou novo no GAC e tenho a impressão de que, antes de começar a trabalhar, devo aprender mais sobre alguns tópicos. Primeiro, como recém-chegado, gostaria de explorar algumas ajudas para ver se posso fazer algo para evitar ataques externos. Sinto que o preço vantajoso proposto por alguns atores leva a algum abuso no DNS. Então eu gostaria de saber como poderíamos trabalhar para ver a taxa de renovação dos nomes de domínio. Talvez isso possa ajudar a comunidade a fazer algo a respeito. Sabemos quais atores não estão atuando legalmente. Então talvez possamos descobrir alguns mecanismos que eles usam. Mas algumas das dificuldades que observamos precisam ser comprovadas com evidências. Acho que é algo que precisamos. Obrigado pela sua atenção.

MANAL ISMAIL: Muito obrigado, França. Vejo a mão de Ruanda levantada. Então, por favor, seja breve, porque estamos ficando sem tempo.

VINCENT MUSEMINALI: Muito obrigado. Só quero agradecer aos apresentadores, aos painelistas que fizeram a apresentação do relatório dos EUA e do

relatório do Reino Unido sobre crimes cibernéticos. Apenas para obter alguns esclarecimentos sobre criptomoedas. A maioria das pessoas agora enfrenta alguns desafios relacionados a domínios que usam crimes cibernéticos vinculados a criptomoedas. E esses domínios às vezes são fechados e as pessoas perdem seu dinheiro e investimento. E agora eles têm que fazer o acompanhamento desse investimento. Gostaria apenas de saber como eles cooperam com a Interpol. Obrigado.

MANAL ISMAIL: Muito obrigado, Ruanda. De volta para você, Chris. Desculpe apertar o prazo, mas é bom ouvir os colegas do GAC. Por favor, vá em frente.

CHRIS LEWIS-EVANS: Obrigado, Manal. Com certeza é e muito obrigado pela sua contribuição. Vou tentar resumir algumas das minhas contribuições rapidamente. Do lado do conselho, que ouvimos tanto do Congo quanto da França, não vamos cobrir isso aqui agora. Há muitos conselhos. Há muitas coisas que você pode fazer. Talvez isso seja algo para um workshop de capacitação em uma futura ICANN. Então, talvez um para o GAC considerar porque precisaria ser uma sessão um pouco mais longa. Então, isso pode ser algo que poderíamos considerar. Então, no ponto do Irã sobre o proativo, “O que podemos fazer?” Acho que Bertrand cobriu alguns deles. O NetBeacon, certamente mencionado como uma ferramenta de relatórios, é uma forma de ação e uma forma de combater um pouco disso. Isso leva muito bem às atividades em andamento, se pudermos passar para esses slides.

Abordaremos algumas das ações que estão acontecendo na comunidade que está apoiando parte desse uso indevido de DNS. Também no lado das criptomoedas, acho que isso vem um pouco do ponto de vista de Bertrand. Isso pode ser entregue a partir de um e-mail de phishing, onde cairia no uso indevido de DNS, ou pode ser um problema relacionado ao conteúdo, onde cairia em mecanismos lá. Em seguida, partindo para atividades comunitárias. Há muito trabalho acontecendo. Os registros estão trabalhando no compartilhamento voluntário de estatísticas. Como vimos do ponto de aplicação da lei, achamos que isso é muito importante. Isso nos dá uma visão geral. Da mesma forma para os registros que dariam suporte a isso. Só para mencionar o próximo, que é acidtool.com. Bertrand disse que não há ferramenta para identificar provedores de hospedagem e e-mail. Na verdade, os registradores criaram esta ferramenta para ajudar as pessoas a identificar o ponto certo e correto a ser abordado, para tomar medidas efetivas. Ouvimos na apresentação da I&J que tomar medidas efetivas é realmente importante. E identificar o ponto certo, seja um revendedor, um registrador, um registro ou um provedor de hospedagem é muito importante. Outro apelo ao NetBeacon, novamente, aqui, como um método de ação. Isso está muito alinhado com as recomendações do SSAC115. Tivemos uma boa apresentação do SSAC sobre isso e, novamente, mencionada no relatório I&J. Todas essas são atividades que estão ajudando a mitigar esse conselho que está acontecendo no momento. Além disso, o DNS Abuse Institute está compartilhando seu trabalho de análise dos dados coletados e vistos como parte desse relatório de uso indevido de DNS. Próximo slide, por favor.

Provavelmente estou falando muito rápido para os intérpretes, então vou me desculpar agora e diminuir um pouco o ritmo. A pequena equipe da GNSO sobre uso indevido de DNS também tem estado muito ativa. Eu só quero sinalizar aqui que suas descobertas refletem algumas de nossas questões importantes dentro do Comunicado de Haia de que qualquer trabalho futuro de PDP sobre uso indevido de DNS deve ser estritamente adaptado para produzir alguns resultados oportunos e viáveis. Para o ponto de vista do Irã, qualquer trabalho que fazemos na comunidade precisa ser direcionado para permitir que aconteça e aconteça rapidamente. Eu sei que às vezes há frustrações sobre as coisas não acontecerem rápido o suficiente. Então, próximo slide, por favor. Também dentro do mandato da ICANN, eles têm a equipe OCTO, têm o sistema DAAR. Isso também ouvimos no sábado, creio que foi, em torno deles analisando dados de 1.145 gTLDs, o que surpreendeu quantos havia nisso. Também há, eu acho, 21 ccTLDs. Novamente, é apenas uma imagem melhor para dar uma maior compreensão do que está acontecendo para poder tomar medidas eficazes. Próximo slide, por favor. Este é apenas um lembrete sobre esse caminho e quem contatar. É um espaço complicado. Este é um diagrama da ICANN, então muito obrigado. Eu não consigo nem chegar perto assim. Ouvimos falar de ir até a pessoa certa para poder tomar a atitude certa no momento apropriado.

Certamente, do meu ponto de vista, vemos onde podemos fazer isso, que também reduz o dano. Portanto, ser capaz de entender para onde ir e para onde ir rapidamente é muito importante. Portanto, ferramentas como NetBeacon e ACID Tool são realmente úteis. A imagem é na verdade um pouco mais complicada do que isso também.

No lado direito, você tem o registrante e, em seguida, um revendedor. Nem sempre há um revendedor ou às vezes há mais de um revendedor. Portanto, entender isso é realmente importante para poder encontrar o lugar certo para entrar. Próximo slide, por favor. Apenas para sinalizar na frente do revendedor, durante o trabalho da Fase 1 no EPDP, ele recomendou que os registradores gerassem um elemento de dados do revendedor para o revendedor com um relacionamento com o registrante. Isso é importante onde há vários. Portanto, na resposta WHOIS no momento, há um campo de revendedor, mas não necessariamente coletando todos eles. E como eu disse, é muito importante podermos ir diretamente à pessoa que pode receber a resposta mais eficaz. Isso também se refletiu na Revisão do CCT. Próximo slide, por favor. E entregue para Laureen. Peço desculpas por ir rápido, mas gostaria de chegar ao nosso segundo conjunto de perguntas, se possível.

MANAL ISMAIL: Laureen, já temos um pedido de palavra. Você gostaria que pegássemos primeiro? OK. Vejo a mão do Reino Unido levantada. Nigel, por favor, vá em frente.

NIGEL HICKSON: Muito obrigado, senhora presidente. Eu ficaria feliz se Laureen fosse primeiro e então nós entraremos mais tarde, talvez. Vá em frente, Laureen, por favor.

LAUREEN KAPIN: Obrigado, Nigel. Estou falando na qualidade de um dos copresidentes do Grupo de Trabalho de Segurança Pública e um dos especialistas nesse assunto tão importante. Podemos ir para o próximo slide?

Fico feliz que a sessão tenha sido interativa, mesmo antes deste momento. Muitas informações e perspectivas foram compartilhadas. Agora estamos no ponto em que podemos discutir o que o GAC gostaria de destacar no comunicado, portanto, possíveis problemas. Em primeiro lugar, e isso se enquadra na categoria "se vale a pena dizer, vale a pena dizer muitas vezes", temos as negociações contratuais em andamento entre Registros e Registradores e a ICANN. Mais uma vez, todo o objetivo desse processo é levantar o piso, para melhorar as obrigações contratuais com relação à tomada de medidas contra o uso indevido de DNS. Portanto, obrigações, não esforços voluntários. Essas obrigações, o objetivo seria refletir uma obrigação que vai abranger todos. Isso incluiria atores mal-intencionados e também daria à ICANN ainda mais ferramentas do que já tem para lidar com esses cenários relacionados ao uso indevido de DNS. Novamente, este é apenas o primeiro passo e pode haver etapas futuras. Mas este pode ser um momento importante para o GAC reconhecer e aplaudir que esse esforço está em andamento e que foi feito por iniciativa das partes contratantes. Este é um passo proativo e é sempre bem-vindo. Este é o primeiro de muitos passos para que o futuro trabalho político seja previsto. Quero repetir um dos comentários de meu colega do Irã de que é muito importante priorizar aqui e focar porque é assim que as coisas são feitas. E podemos aplicar esses dois princípios orientadores a quaisquer PDPs, que não são necessariamente conhecidos por sua ação rápida e focada, mas podem e devem ser neste contexto. Além

disso, pode haver oportunidades para mais negociações entre as Partes Contratadas e ICANN. Para sinalizar, haverá uma próxima oportunidade para comentários públicos assim que os Contratados liberarem os frutos de seus trabalhos, que aguardamos ansiosamente. Então haverá oportunidades para o GAC decidir que tipo de contribuição gostaria de transmitir. Próximo slide, por favor. Essa questão dos revendedores também foi identificada. A razão que se conecta ao uso indevido de DNS é porque é muito importante, como observou nosso colega da Internet and Jurisdiction Society, Bertrand. É muito importante poder contatar a entidade certa quando você está lidando com uso indevido de DNS. Este tópico foi objeto de contribuições do GAC de várias formas diferentes, relacionadas ao relatório final do CCT e também, mais recentemente, às recomendações de dados de registro de domínio da Fase 1. Próximo slide, por favor. Agora estou passando para meus colegas do GAC para suas opiniões sobre pensamentos e ideias sobre o que poderia ser incluído no comunicado do GAC. Também observo, sei porque o tempo é curto, que temos sessões de redação de comunicados. Mas este seria um ótimo momento para obter uma prévia do que as pessoas estão pensando.

MANAL ISMAIL: Muito obrigado, Laureen. Temos Reino Unido, Irã e Comissão Europeia. E nós temos três minutos, então, por favor, seja breve. Reino Unido, por favor, vá em frente.

NIGEL HICKSON: Sim. Muito obrigado Manal. Muito obrigado pelo pessoal da mesa principal por nos apresentar. Foi uma sessão excepcionalmente útil, como observaram outros membros do GAC. Apenas quatro pontos muito rápidos, se me permitem. Uma delas é reiterar nossa posição sobre as negociações contratuais que estão por vir. Estou incrivelmente positivo. A sessão que tivemos ontem com os representantes dos Registradores e Registros, achei excelente. Certamente estamos ansiosos pela consulta pública. Nenhuma intenção de interferir nessas negociações. Ansioso por atualizações, é claro. E como foi dito ontem pelos representantes, este é um primeiro passo. Pode haver outras iniciativas, mini PDPs ou qualquer outra coisa, para examinar o uso indevido de DNS. Em segundo lugar, em termos de comunicado, sem dúvida estaremos discutindo essas questões. Acho que é certo deixarmos bem claro no comunicado como recebemos essas iniciativas, mas também listar essas recomendações, o conselho do GAC sobre a recomendação 17 da revisão do CCT e outras questões em termos de revendedores que devemos sinalizar para que toda a comunidade entenda que há certas ações em vigor que precisam ser tomadas antes do próximo processo SubPro. Eu vou deixar lá. Muito obrigado.

MANAL ISMAIL: Muito obrigado, Reino Unido. Eu tenho o Irã a seguir e estou fechando a fila depois do Japão, por favor. Irã, vá em frente.

KAVOUSS ARASTEH: Muito obrigado, Manal. Discuti com alguns colegas ilustres, incluindo você, que a questão do uso indevido de DNS é a questão central do atual, futuro próximo e longo prazo da ICANN. Isso é algo importante. Mas todos, Diretoria, Organização da ICANN, membros e todos, estão estudando o assunto. Não há necessidade de nenhum parecer do GAC sobre isso. Deixe as pessoas respirarem, reflitam, digerirem o assunto, e não forcem mais do que precisamos. Eles sabem o que é um problema. Por outro lado, nas questões importantes para o GAC, a primeira coisa que precisamos mencionar é que reconhecer as negociações que estão sendo realizadas na Diretoria da ICANN ou ICANN e as Partes Contratadas, Registros e Registradores, isso é um bom passo, dizer isso. E então devemos mencionar que precisamos de um relatório de progresso sobre isso em nossa próxima reunião da ICANN, ICANN77 em Washington, DC, um relatório de progresso sobre o que está acontecendo. E esperamos que o relatório final seja 78, ou 79, ou 80, mas também com medidas suficientes, a fim de aconselhar o governo ou o pessoal do GAC sobre como combater, como lutar, como meu colega mencionou, ou como enfrentar essa situação, e ver muitos outros elementos que foram indicados no relatório de Chris, Laureen e Gabriel, colocando nele questões importantes para o GAC. E tente enfatizar a importância da coisa. Trabalhe o texto para ser mais claro, para ser mais preciso e conciso também, e tente colocar os pontos e fazer uma ação de acompanhamento. Mas sugiro que não incluamos nada sobre uso indevido de DNS no conselho do GAC neste estágio. Obrigado.

MANAL ISMAIL: Muito obrigado, Irã. Eu tenho a Comissão Europeia, depois o Japão. E um lembrete amigável para, por favor, seja breve. Comissão Europeia, por favor. Gema, vá em frente.

GEMMA CAROLILLO: Muito obrigada, Manal. Elogiei as apresentações no bate-papo, então não farei isso novamente por causa do tempo. Em relação muito brevemente aos pontos e considerações para o comunicado, conforme solicitado gentilmente por Laureen, certamente concordamos que esta é uma grande jogada. As negociações, a gente vem pedindo isso há muito tempo dentro do GAC. Portanto, isso é algo, com certeza, em que devemos apoiar. Em termos de substância adicional, podemos adicionar à seção de uso indevido de DNS nas questões de importância. Eles vão levá-lo, mas é claro, para uma discussão mais aprofundada. Em primeiro lugar, a importância de uma medida preventiva. Estamos um pouco preocupados com o que ouvimos até agora, é principalmente sobre medidas reativas. Mas a prevenção do uso indevido de DNS é realmente fundamental do nosso ponto de vista. Eu ouvi isso anteriormente, também, de um ou dois colegas. Em seguida, possivelmente explore a questão dos incentivos, que foi levantada nos conselhos muito bons dos colegas do PSWG, etc. E por último, mas não menos importante, ligando ao que Nigel disse sobre a próxima rodada de gTLDs, em geral, gostaríamos de garantir que o trabalho anterior não seja esquecido, em particular, em relação a medidas razoáveis para evitar o uso indevido de DNS. Mas o GAC tem sido muito forte em vincular a precisão dos dados, a precisão do registro de nomes de domínio e o uso indevido de DNS nos comunicados 71, 72 e 73, e tenho

certeza de que há mais. Portanto, não se trata de listar isso, mas apenas para deixar claro que gostaríamos que o trabalho feito em relação à precisão dos dados de registro e à importância de impedir o uso indevido de DNS não fosse perdido. Muito obrigado.

MANAL ISMAIL: Muito obrigado, Comissão Europeia. E por último, mas não menos importante, é claro, tenho o Japão.

NOBU NISHIGATA: Muito obrigado, Manal, e os co-presidentes do PSWG. Boa noite, na verdade. Já é noite no Japão. Bom dia, boa tarde a todos de Tóquio. Muito obrigado pela organização que fez esta sessão maravilhosa hoje. Apenas respondendo à apresentação de Laureen sobre a consideração do comunicado. O Japão gostaria de expressar o apoio à negociação do contrato em andamento, o que é muito bem-vindo, o progresso atual até agora. Mas, por outro lado, o Japão gostaria de levantar uma questão e problema no Contrato de Credenciamento de Registradores, o Artigo 3.18.1, que trata da ação exigida do registrador para denunciar atividades ilegais. O governo japonês informou e está ciente de que alguns registradores não tomam nenhuma ação ou mesmo não respondem ao relatório de atividades ilegais de partes japonesas. Portanto, é por isso que o governo japonês continua pedindo a melhoria do texto ou dos termos deste contrato. Houve alguma evidência do governo japonês. Ainda assim, há várias outras evidências semelhantes a esta, o relatório de auditoria da ICANN ou o relatório recente da ICANN, da GNSO. O Japão está à espera deste relatório

preliminar, e estamos ansiosos de poder falar entre sessões com relação a isso, e poder expressar nossas preocupações. Também queremos expressar nossa gratidão com relação à informação atualizada das negociações, e estamos ansiosos de poder continuar essa conversa com vocês.

MANAL ISMAIL: Obrigado, Japão, obrigado, Bertrand, Chris, Laureen, obrigado a todos. Vamos voltar a nos reunir às 3 da tarde, hora de Cancún, então por favor, estejam aqui em tempo para a sessão bilateral, muito obrigado.