Relatório de Missão Oficial

7 de agosto de 2024 – Pittsburgh, PA, EUA.
8 e 9 de agosto de 2024 o corrente ano, Washington, D.C., EUA.

Composição da Delegação

Senador Esperidião Amin – Presidente da Subcomissão Permanente de Defesa Cibernética
Senador Sergio Moro – Membro da Subcomissão
Senador Chico Rodrigues – Membro da Subcomissão
Senador Astronauta Marcos Pontes – Membro da Subcomissão
Senador Jorge Seilf – Convidado dos organizadores

I - Introdução

As ameaças cibernéticas vêm aumentando à medida que o mundo se torna, cada vez mais, conectado e as principais estruturas dos países passam a depender fortemente do espaço cibernético. A transformação digital, acelerada pela pandemia da Covid-19, trouxe, à tona, a realidade de um mundo digital bastante desigual e exposto aos mais diversos tipos de conflitos cibernéticos. No que tange à economia mundial, os prejuízos financeiros, relacionados aos cibercrimes, estão estimados na casa dos trilhões de dólares.

Segundo o Fórum Econômico Mundial, se o crime cibernético fosse um país, ele seria a terceira maior economia mundial, perdendo apenas para os EUA e China.

No campo das Relações Internacionais, a cibersegurança já se incorporou à agenda de segurança dos Estados e, devido a sua abrangência e transversalidade, deve ser abordada sob uma perspectiva ampla e multissetorial.

No dia 18 de julho o mundo foi pego de surpresa. Uma atualização do software ‘Falcon’ da CrowdStrike, derrubou de uma só vez milhões de computadores em todo o mundo, atingindo serviços que vão desde a aviação, bancários além de saúde, revelou como a conectividade pode afetar vários serviços em escala global, bastando a falha de um software de uma única empresa. O caso reforçou os desafios da transversalidade do campo cibernético.

Neste Sentido agora teremos o desafio de nos preparamos não apenas para os “ataques-cibernéticos”, mas também para os incidentes cibernéticos causados por falhas de sistema ou mesmo humana.

Assim, considerando esse cenário extremamente grave e de preocupação geopolítica onde se situa a cibersegurança, motivou-se a Comitiva formada por membros da Subcomissão de Defesa Cibernética do Senado Federal e do Senador Jorge Seilf, a fazerem um intercâmbio com setores de defesa e tecnologia dos EUA, que envolveu também outras instituições brasileiras como ANATEL, GSI Ministério da Tecnologia e Inovação.

II – DA VISITA AO NCFTA EM PITTSBURG (07 DE AGOSTO)

Atualmente não se pode negar que um dos temas mais importantes discutidos no Brasil em sede de Cibersegurança, é o da necessidade da criação de uma agência brasileira de cibersegurança.

Foram várias as Audiências Públicas realizadas pela Subcomissão, com setores tanto do poder público como da área privada, que nos levaram para este caminho.

Neste sentido, era imprescindível para nossos representantes conhecerem, a convite o NCFTA dos EUA, com sede em Pittsburg.

A National Cyber-Forensics & Training Alliance (NCFTA) é uma organização sem fins lucrativos sediada em Pittsburgh, Pensilvânia,

que se dedica à luta contra o cibercrime. Fundada em 2002, a NCFTA promove uma colaboração entre a indústria privada, a academia e o governo para identificar, mitigar e neutralizar ameaças cibernéticas. A seguir, uma resenha detalhada sobre a NCFTA:

A missão da NCFTA é desenvolver e disseminar informações sobre ameaças cibernéticas, facilitando a colaboração entre os setores público e privado. Seus principais objetivos incluem:

Identificação e Análise de Ameaças: Detectar e analisar atividades criminosas cibernéticas emergentes.
Disseminação de Informações: Compartilhar informações de maneira segura entre seus parceiros para mitigar riscos.
Educação e Treinamento: Fornecer treinamento em cibersegurança e forense digital para profissionais da área.

Estrutura e Operação
A NCFTA opera através de um modelo de colaboração único que reúne especialistas de várias áreas, incluindo:
Setor Privado: Empresas de diversas indústrias (tecnologia, finanças, saúde, etc.) que fornecem dados e recursos para a análise de ameaças.
Academia: Instituições de ensino superior que contribuem com pesquisas e desenvolvimento de novas tecnologias de cibersegurança.
Agências Governamentais: Órgãos de aplicação da lei e outras entidades governamentais que se beneficiam das análises e informações fornecidas pela NCFTA.

Principais Iniciativas e Programas:
A NCFTA é conhecida por várias iniciativas e programas que ajudam a fortalecer a segurança cibernética, tais como:

- Intelligence Sharing: Um dos pilares da NCFTA é a troca de inteligência cibernética. A organização facilita o compartilhamento de informações sobre ameaças entre os membros, permitindo uma resposta mais rápida e eficaz aos incidentes cibernéticos.
- Analytical Capabilities: A NCFTA possui capacidades analíticas avançadas, utilizando uma variedade de ferramentas e técnicas para investigar e analisar ameaças cibernéticas. Isso inclui a análise de malware, rastreamento de atividades criminosas online e investigação

- de fraudes cibernéticas.

- Prevenção de Fraudes: Através da colaboração e análise de dados, a NCFTA ajudou a prevenir inúmeras fraudes cibernéticas, protegendo tanto empresas quanto consumidores.
- Aprimoramento de Políticas: As descobertas e análises da NCFTA influenciam políticas de cibersegurança em várias organizações e agências governamentais.
- Desenvolvimento de Talentos: Através de seus programas de treinamento, a NCFTA ajuda a formar a próxima geração de profissionais de cibersegurança, equipando-os com habilidades essenciais para enfrentar ameaças cibernéticas modernas.

Conclusão
A National Cyber-Forensics & Training Alliance desempenha um papel crucial na proteção contra cibercrimes. Sua abordagem colaborativa, que reúne setores diversos para compartilhar inteligência e desenvolver estratégias de defesa, tem se mostrado eficaz na identificação e mitigação de ameaças cibernéticas. Através de suas iniciativas de treinamento e educação, a NCFTA também contribui para a capacitação de profissionais na área, reforçando a segurança cibernética global.

Assim, a troca de experiências serviu para a comitiva conhecer um novo modelo de parceria entre os setores público e privado, no combate aos crimes cibernéticos até então inédito no país.

III – Do intercâmbio de melhores práticas de cibersegurança entre Brasil-EUA, Washington D. C. (8 e 9 de agosto)

Representantes do Brasil e dos Estados Unidos concluíram um intercâmbio de dois dias sobre as melhores práticas de segurança cibernética, promovido pelo Banco Interamericano de Desenvolvimento - BID, em parceria com a Digi Américas, nos dias 8 e 9 de agosto em Washington, DC.
Autoridades governamentais de alto escalão e principais partes interessadas de ambos os países se reuniram para compartilhar

conhecimento, estratégias e inovações no campo da segurança cibernética.

Os eventos do primeiro dia começaram com comentários de Paula Acosta, Chefe de Divisão de Inovação em Serviços ao Cidadão do Banco Interamericano de Desenvolvimento (BID), e Santiago Paz, Especialista Sênior em Segurança Cibernética do BID. Acosta destacou o papel crítico das parcerias público-privadas no enfrentamento dos desafios em constante evolução da segurança cibernética.

Ela enfatizou que o BID está promovendo a transformação digital dentro dos governos e reconheceu a importância da expertise diversificada. De acordo com Acosta, a colaboração entre as partes interessadas é essencial para fazer progressos significativos na luta contra ameaças cibernéticas, que têm consequências sociais e econômicas de longo alcance. Ela também destacou que, embora o Brasil esteja liderando na transformação digital, essa posição de liderança também aumenta sua exposição a riscos cibernéticos.

Paz seguiu ressaltando os impactos sociais mais amplos de incidentes de segurança cibernética, observando que tais eventos podem interromper o acesso dos cidadãos a serviços essenciais, afetando assim sua qualidade de vida. Ele enfatizou a necessidade de implementar projetos maduros de segurança cibernética, particularmente aqueles que alavancam a automação para aumentar a eficiência e a eficácia. Paz também expressou o comprometimento do BID em continuar sua colaboração com o Brasil, visando avançar ainda mais as iniciativas de segurança cibernética e fortalecer a resiliência contra ameaças cibernéticas.

Diretor do BID Santiago Paz em palestra para os membros da comitiva brasileira em Washington D.C.

Comitiva do Senado Federal participa de intercâmbio na sede do BID, dia 08 de agosto

Jennifer Bachus, Secretária Assistente Adjunta Principal do Bureau of Cyberspace and Digital Policy do Departamento de Estado dos EUA, forneceu uma visão geral da Estratégia Internacional de Política Digital e Ciberespaço dos EUA, que estabelece uma visão de futuro para o papel da tecnologia na sociedade. Ela enfatizou que a colaboração internacional e a colaboração com parceiros globais são cruciais para aproveitar o potencial positivo da tecnologia ao mesmo tempo em que aborda seus desafios.

Seguindo Bachus, Patricia Soler, Chefe de Seção do Joint Cyber Defense Collaborative (JCDC) na Cybersecurity and Infrastructure Security Agency (CISA), forneceu uma visão geral aprofundada do JCDC e seu papel crítico dentro do CISA. Ela destacou a importância

da colaboração entre o setor privado e o CISA, dado que a maior parte da infraestrutura crítica (CI) é de propriedade privada.

Soler discutiu o desenvolvimento contínuo do Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), enfatizando que o objetivo é coletar dados essenciais sem sobrecarregar os parceiros de CI. Ela também detalhou a estrutura da força de trabalho da CISA, o alcance regional e as colaborações internacionais, particularmente por meio do JCDC, que une os esforços globais de defesa cibernética. Soler abordou o equilíbrio entre o compartilhamento voluntário de informações e o relatório obrigatório, observando que a CISA está se expandindo para atender às novas demandas e prioridades de segurança cibernética, ao mesmo tempo em que mantém seu foco na melhoria da segurança nacional por meio da colaboração e de sistemas de dados avançados.

O próximo foi um painel sobre inteligência artificial (IA) com palestrantes do Instituto Nacional de Padrões e Tecnologia (NIST) e do Departamento de Comércio dos EUA.

Jesse Dunietz apresentou o AI Risk Management Framework (RMF) do NIST, projetado para promover sistemas de IA confiáveis por meio de quatro funções principais e destacou o manual do RMF, que fornece orientação detalhada para organizações implementarem o framework de forma eficaz. Ordens executivas recentes atribuíram ao NIST várias responsabilidades, incluindo a criação de ambientes de teste, red teaming de IA e avaliação de capacidades de IA.

Amy Mahn discutiu atualizações do NIST Cybersecurity Framework (CSF), agora na versão 2.0. Ela elaborou sobre o processo de atualização envolvendo ampla colaboração internacional, incluindo workshops públicos e solicitação de feedback. Mahn observou que a versão 2.0 foi traduzida para o português, expandindo sua acessibilidade.

Adam Sedgewick explorou a intersecção entre segurança cibernética e privacidade, enfatizando que precisamos ir além de olhar para a privacidade somente no contexto de conformidade e entender como a tecnologia pode aprimorar a proteção da privacidade. Sedgewick deu uma visão geral do NIST Privacy Framework e destacou os recursos disponíveis para organizações, incluindo traduções, vídeos e guias de início rápido.

Em relação à adoção dessas estruturas no Brasil, tanto Mahn quanto Sedgewick afirmaram a disposição do NIST em auxiliar tanto formal quanto informalmente. Eles observaram que o NIST colabora com países e organizações globalmente, inclusive por meio de padrões ISO, para ajudar os países a adaptar essas estruturas às suas necessidades específicas.

Os Senadores participaram ativamente com várias intervenções durante as explanações e principalmente no final das apresentações, quando foi realizada uma roda de debates e discutidos os principais entraves e soluções para a segurança cibernética do Brasil.

Senador Esperidião Amin faz questionamentos sobre o modelo de Agência de Cibersegurança dos EUA - CISA

Senador Sergio Moro faz explanações sobre a visita da NCFTA, e a necessidade de se avançar em um modelo semelhante no Brasil

Senador Chico Rodrigues acompanha atentamente a palestra do Diretor do BID, Santiago Paz, sobre cooperação com o Brasil em matéria de Cibersegurança.

Já no segundo dia, a colaboração continuou com a participação de representantes do Fórum Econômico Mundial (WEF), do Financial Services Information Sharing and Analysis Center (FS-ISAC), do Health Information Sharing and Analysis Center (H-ISAC), do Institute for Security and Technology (IST) e da Câmara de Comércio dos EUA lideraram discussões adicionais. Essas sessões promoveram diálogos robustos, fornecendo insights acionáveis para aprimorar políticas e estruturas de segurança cibernética.

Comitiva de Senadores participa de Palestra do Fórum Econômico Mundial, sobre os riscos globais de Cibersegurança, no dia 09 de agosto

Joanna Bouckaert, líder do Center for Cybersecurity (C4C), destacou que a segurança cibernética continua sendo um dos principais riscos globais, exacerbando crises existentes e colocando em risco princípios democráticos. As principais preocupações para 2023 incluem desinformação e informações falsas, juntamente com uma crescente desigualdade global em segurança cibernética. Houve um declínio de 30% nas organizações que mantêm resiliência cibernética viável, afetando particularmente pequenas e médias empresas. A escassez de profissionais de segurança cibernética é grave, com uma lacuna de quatro milhões na força de trabalho global, e há otimismo limitado para melhorias nos próximos dois anos.

A percepção das regulamentações cibernéticas e de privacidade está mudando positivamente, com 60% dos executivos reconhecendo sua eficácia na redução de riscos, embora os desafios com regulamentações conflitantes persistam. Há uma abertura crescente para regulamentações e agências nacionais, impulsionada pelos riscos da cadeia de suprimentos e pela necessidade de melhor controle sobre a segurança de terceiros. Esforços estão em andamento para construir pipelines de talentos em segurança cibernética globalmente, e as discussões em andamento se concentram na adaptação de regulamentações para enfrentar novos desafios impostos pelas tecnologias de IA.

Brian Tishuk, Conselheiro Geral do Financial Services ISAC, explorou o papel crucial do FS-ISAC no aprimoramento da segurança cibernética financeira global e da resiliência. Como uma organização sem fins lucrativos, orientada por membros, o FS-ISAC fornece uma rede de compartilhamento de informações em tempo real que fortalece a defesa coletiva ao amplificar a inteligência e as práticas em todo o setor financeiro.

O FS-ISAC está expandindo sua presença na APAC e LATAM, com 95% das entidades financeiras sistemicamente importantes do Brasil sendo membros. A organização se envolve em várias iniciativas importantes, como colaborações em gerenciamento de risco de nuvem e parcerias globais público-privadas. Tishuk também abordou os desafios e benefícios de interagir com outros Information Sharing and Analysis Centers (ISACs), enfatizando as vantagens de um conselho nacional de ISACs para coordenação.

O FS-ISAC mantém relacionamentos fortes com agências de gerenciamento de risco do setor, incluindo o Departamento do Tesouro dos EUA, para aumentar a segurança e a resiliência de todo o setor. Tishuk também compartilhou que, em relação a um ISAC setorial vs. regional, é melhor começar onde há uma disposição para participar e construir a partir daí, reconhecendo que a separação setorial permite que você acesse o conhecimento personalizado de especialistas no assunto dentro desse setor.

Denise Anderson, Presidente do Health Information Sharing and Analysis Center (Health-ISAC) enfatizou o papel crítico que os ISACs têm no aprimoramento da segurança cibernética em todos os setores. O Health-ISAC, atendendo a uma comunidade de mais de

10.000 analistas de segurança globais, foca na confiança e no anonimato no compartilhamento de informações.

No primeiro trimestre de 2024, o Health-ISAC emitiu 289 alertas — um aumento de 175% em relação ao trimestre anterior. As principais estatísticas incluem o relatório da IBM de um custo médio global de violação de dados de US$ 4,88 milhões e mais de um bilhão de vítimas de violação em 2024. O phishing continua sendo o principal vetor de ataque, responsável por 90% das violações de dados. O Health-ISAC emprega um Traffic Light Protocol (TLP) para compartilhamento de informações, onde os membros aderem voluntariamente às diretrizes de compartilhamento de informações.

Com mais de 40 funcionários, incluindo uma presença europeia, a Health-ISAC está expandindo seu foco regional e setorial. Anderson destacou a necessidade de alavancar estruturas existentes para evitar silos e aprimorar o compartilhamento efetivo, defendendo o estabelecimento de um conselho LATAM dentro do National Council of ISACs. Ela também discutiu os desafios da HIPAA no manuseio de dados e a importância da colaboração entre organizações de prestação de serviços de saúde e fabricantes para lidar com ameaças emergentes.

Taylor Grossman, vice-diretor de Segurança Digital do Instituto de Segurança e Tecnologia (IST), destacou que o ransomware se tornou uma ameaça significativa, com extorsão atingindo US$ 1 bilhão em 2023 e vários setores, incluindo saúde e finanças, sendo fortemente visados.
Grossman enfatizou o desafio de relatórios inconsistentes, que impedem a análise de tendências e estratégias de resposta. A Ransomware Task Force, composta por mais de 60 especialistas de vários setores, defende uma abordagem multissetorial para abordar o problema. Essa abordagem envolve correções técnicas de empresas de software, insights da sociedade civil e esforços regulatórios de governos.

Enquanto a ideia de proibir pagamentos de resgate foi debatida, o consenso é que maior transparência e regulamentação, como o aviso de 24 horas proposto para pagamentos de resgate sob a CIRCIA, são medidas mais práticas a serem tomadas primeiro, já que uma proibição completa não seria prática neste momento. A estrutura da Força-Tarefa visa impedir ataques, interromper o modelo de negócios de ransomware e aprimorar a preparação organizacional.

As iniciativas em andamento incluem melhorar a colaboração internacional, desenvolver um modelo para defesa de ransomware e aumentar o compartilhamento voluntário de informações.

O painel também discutiu a importância das práticas "seguras por design" e a necessidade de mecanismos de preparação e resposta mais eficazes antes de considerar qualquer proibição de pagamentos de ransomware.
Michael Richards, Diretor Sênior de Políticas do US Chamber of Commerce Technology Engagement Center (C_TEC), fez uma apresentação sobre o cenário em evolução da política de IA e suas implicações para as empresas. Liderando o grupo de trabalho de IA na US Chamber of Commerce, que abrange mais de 200 empresas em 33 setores, Richards descreveu seu papel na formação da política de IA tanto nacional quanto internacionalmente.

Richards enfatizou a importância das parcerias público-privadas na governança de IA, defendendo uma abordagem baseada em risco e a necessidade de uma força de trabalho bem preparada e pronta para IA. Ele destacou os princípios de política da Câmara para IA, que enfatizam a importância de equilibrar a inovação com estruturas de privacidade robustas e proteções de propriedade intelectual. À medida que os EUA continuam a avançar no desenvolvimento de IA, Richards observou que, embora o país lidere na pesquisa de IA, ele também deve abordar riscos potenciais e colaborar com os governos para garantir investimento e desenvolvimento responsáveis. A Câmara está no processo de atualizar seus princípios para refletir essas prioridades e preocupações emergentes com a segurança cibernética.

Durante o evento, foi anunciado que o LATAM CISO Summit 2025 será realizado no Brasil. Esta decisão destaca a crescente proeminência do Brasil no cenário global de segurança cibernética. Ela reflete um compromisso em continuar o diálogo e a cooperação iniciados em DC. Este evento fortaleceu a parceria de segurança cibernética entre o Brasil e os EUA e estabeleceu um precedente para a futura cooperação internacional entre as partes interessadas de ambos os países.

Participantes do intercâmbio Brasil/EUA sobre melhores práticas de cibersegurança, em Washinton D.C. 09 de Agosto

É o relatório.

Chico Rodrigues
Senador da República