Relatoria - 13º Fórum da Internet no Brasil - Uberlândia/MG

Título do workshop:
O Futuro da Cibersegurança Internacional

Objetivo do workshop:
A partir da exposição das principais questões com relação à cibersegurança em nível internacional, o workshop tem por objetivo debater quais os desafios que serão enfrentadas nos próximos anos e, nesse sentido, apresentar expectativas do que deve se desenrolar no cenário brasileiro e internacional.

Proponente: Pedro de Perdigão Lana | **Região:** Sul
Co-Proponente: Cynthia Picolo | **Região:** Sudeste

Painelistas:

- **Ada Rosenfeld** *(Tempest Security Intelligence)*

Mais de 18 anos de experiência no mercado de Cibersegurança, ajudou diretamente a Tempest Security Intelligence a se tornar a empresa líder no Brasil em segurança da informação através de sua experiência no mercado de segurança digital.

- **Franklin Silva Netto** *(Ministério Das Relações Exteriores)*

Conselheiro da Carreira Diplomática, Chefe da Divisão de Segurança e Defesa Cibernética.

- **Louise Marie Hurel** *(London School of Economics and Political Science (LSE))*

Louise Marie Hurel é doutoranda em Dados, Redes e Sociedade na London School of Economics and Political Science (LSE) e research fellow no Royal United Services Institute (RUSI) trabalhando com diferentes agendas de cibersegurança no âmbito global. Louise é fundadora da Rede Latinoamericana de Estudos sobre Cibersegurança (LA/CS Net) e membro do Advisory Board do Global Forum on Cyber Expertise (GFCE). Por mais de 7 anos, Louise trabalhou na interseção entre segurança e tecnologia no Brasil e na América Latina; estabeleceu e coordenou o Programa de Segurança Digital do Instituto Igarapé.

- **Michele Nogueira Lima** *(Universidade Federal De Minas Gerais)*

Membro titular do CNPD da ANPD. Doutora em Ciência da Computação pela Sorbonne Université, Pós-doutorado na Universidade Carnegie Mellon. É professora associada do programa de pós-graduação Departamento de Ciência da Computação da UFMG. Foi professora da UFPR por 10 anos. É membro sênior da ACM e do IEEE

- **Vanessa Copetti Cravo** *(ANATEL)*

Servidora da ANATEL. Coordenadora do Processo de Apuração de Descumprimento de Obrigações. Membro do Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica da Anatel (GT-Ciber). Participou de diversas delegações brasileiras para a UIT. Bacharel e Mestre em Direito pela UFRGS e Doutora em Estudos Estratégicos Internacionais (PPGEEI) pela UFRGS.

Moderação

- **Cynthia Picolo** *(Laboratório De Políticas Públicas E Internet (LAPIN))*

Advogada, bacharel em Direito pela PUC-Campinas, LL.M. em Direito Internacional Público pela Universidade de Leiden (Holanda) e especialista em Privacidade e Proteção de Dados e Inteligência Artificial. Atualmente, é diretora executiva do Laboratório de Políticas Públicas e Internet (LAPIN).

Relatoria

- **Pedro de Perdigão Lana** *(ISOC Brasil & IODA)*

Doutorando em Direito e graduado pela UFPR. Mestre em Direito pela Universidade de Coimbra. Pesquisador do Grupo de Estudos em Direito Autoral e Industrial. Diretor de projetos do capítulo brasileiro da ISOC, secretário do Instituto Observatório do Direito Autoral (IODA). Participa, representando o prof. Marcos Wachowicz, da Câmara Técnica de Segurança e Direitos do CGI.br.

Síntese do workshop:

Louise Marie Hurel, partindo da perspectiva internacional inerente ao tema, questiona qual o papel da América Latina na governança global de cibersegurança. Para ela, a falta de conscientização em relação aos perigos cibernéticos é um dos principais obstáculos enfrentados pela América Latina; por esse motivo, a região enfrenta um desafio ao desenvolver leis e regulamentos eficazes. Nesse contexto, cibersegurança não é um tema que vem a mente quando se pensa em America Latina, o continente é esquecido nos principais debates sobre o futuro. Isso ocorre porque a atenção do debate global paira sob polos muitos específicos, concentrando-se em regiões que afetam de forma mais direta e imediata a economia dos “países desenvolvidos”. Dessa forma, falta de legislação abrangente e atualizada na América Latina dificulta a responsabilizar os infratores e a garantir a cooperação entre os países em casos de crimes cibernéticos transfronteiriços. Assim, o processo de harmonizar as leis e construir estruturas de cooperação internacional são fatores-chave para fortalecer a cibersegurança na região. Contudo, compreende-se que a região latino-americana possui diversos outros diversos desafios, que acabam se sobressaindo ao definir prioridades políticos. Para Louise, todavia, o debate sobre o desenvolvimento e

interconectividade da região não pode estar dissociado do debate sobre cibersegurança. Finaliza citando alguns avanços, como a legislação chilena, que recolocou a cibersegurança em posição de destaque na agenda pública do país; e as tentativas brasileiras e colombianas que estão em andamento. Por fim, ressalta que o papel da academia é fomentar um debate crítico, conetar as bibliografias que estão sendo desenvolvidas e dar visibilidade para as pesquisas latino-americanas.

Na sequência, Franklin Silva Netto traz uma abordagem sobre as Tecnologias da Informação e Comunicação (TICs) no cenário da segurança internacional. Inicialmente, com uma abordagem histórica, ressalta a dificuldade de formular conceitos e definições no ambiente da ONU - com diversos atores e Estados envolvidos. Nesse cenário das relações internacionais, um dos temas mais complexos e politicamente relevante se relaciona à definição de "agressão". Este estudo é contínuo e ainda hoje se dedica a determinar quais ações podem ser consideradas uma agressão à luz do direito internacional. Porém, se há uma dificuldade em delimitar agressão no sentido tradicional do uso, ao envolver as novas tecnologias se adiciona um obstáculo a mais. As TICs têm um papel crucial no cenário da cibersegurança internacional, pois com o avanço tecnológico e a interconexão global, afetam diversos aspectos da segurança, tais como a defesa nacional, a inteligência, o combate ao terrorismo e a segurança das infraestruturas críticas — nos meios físicos e virtuais. Assim, se torna necessário a busca por uma conceituação de agressão no cenário cibernético. Nesse sentido, a ONU possui os Grupos de Peritos Governamentais — Group of Governmental Experts (GGE) -, mecanismo pelo qual especialistas são chamados a estudar um tema e propor recomendações. Os GGE podem ser sobre diversos temas, mas sobre TICs e segurança internacional já ocorreram seis. Por fim, o painelista destaca a participação do Brasil nesses grupos, principalmente qual ao pedido para que houvesse maior representatividade dentre os participantes.

A terceira exposição foi conduzida pela painelista Ada Rosenfeld, que iniciou sua fala com um panorama diverso das anteriores: o distanciamento entre os debates teóricos e a prática no cenário da cibersegurança. Ao trabalhar com empresas de grande porte, a principal preocupação está relacionada aos investimentos necessários para garantir a cibersegurança, bem como quais os riscos reais ao não implementar os mecanismos de defesa. À vista disso, os setores que mais investem em cibersegurança são o financeiro e órgãos governamentais de países desenvolvidos. O setor financeiro, por abranger transações de alto risco e valores elevados, acaba sendo suscetível a uma maior atenção dos infratores. No cenário brasileiro recente, a Lei Geral de Proteção de Dados (LGPD) fez com que muitas empresas passassem a prestar maior atenção no debate sobre cibersegurança, impulsionando o investimento nessa área. A painelista destaca que novas técnicas e métodos de ataque surgiram com o avanço da tecnologia e, com isso, surgem preocupações antes inexistentes. Atualmente, os principais alvos são os setores que menos investem em segurança cibernética, pois isso facilita o sucesso dos infratores. Diversos ataques a empresas pequenas, indústrias e hospitais, por exemplo, estão acontecendo cada vez com mais frequência, sendo este um desafio

para os próximos anos. Em suma, o cibercrime é uma grande ameaça no mundo digital de hoje, e a evolução tecnológica requer respostas igualmente sofisticadas. Somente por meio de medidas de precaução, cooperação internacional e conscientização podemos enfrentar esse desafio e proteger a integridade e a segurança dos usuários da Internet.

Na mesma linha, Michele Nogueira Lima aponta que é possível perceber um distanciamento entre a prática e a literatura, que não dá conta de acompanhar a evolução tecnológica. O avanço da tecnologia aprimora tanto os ataques quanto a prevenção, é preciso se especializar nesses temas e a principal dificuldade está na falta de tempo hábil e investimento para tal. Com a sofisticação dos ataques, muitos usuários não possuem o conhecimento necessário para identificar ameaças online ou adotar medidas de proteção adequadas. Isso se deve, em parte, à rápida adoção da tecnologia, que nem sempre é acompanhada por programas de educação em cibersegurança. Desse modo há uma ramificação das áreas do saber concernentes à tecnologia, como a segurança de dados e segurança de rede, sendo apenas dois exemplos em um rol de diversas questões específicas. Um exemplo que deve ser analisado com atenção é a espionagem cibernética, a painelista deixa um alerta sobre esses ataques. Assim, com obstáculos complexos a serem vencidos, é necessário a especialização de profissionais de cada um desses ramos e em paralelo buscar uma internacionalização do conhecimento produzido sobre o tema.

Para fechar a rodada de exposições, Vanessa Copetti Cravo inicia sua fala ressaltando como há muitas perspectivas envolvendo o debate sobre cibersegurança. Cibersegurança envolver as práticas, tecnologias e políticas usadas para proteger sistemas de computador, redes, dispositivos eletrônicos e dados de ameaças cibernéticas. O objetivo da segurança cibernética é garantir a confidencialidade, integridade e disponibilidade das informações digitais e proteger essas informações contra possíveis ataques. Assim, as organizações internacionais precisam e estão debatendo o tema com profundidade e frequência; porém, é preciso melhor incluir os países em desenvolvimento e “não desenvolvidos”. A perspectiva de um país desenvolvido será necessariamente diversa e até oposta à dos demais, por partirem de necessidades e realidades diferentes. Assim, não é do interesse de países desenvolvidos aprofundar os debates sobre certas problemáticas que envolvem cibersegurança, visto que não seria vantajoso resolver os problemas que afetam diretamente apenas países não desenvolvidos.

Perguntas presenciais:

- **Emerson, delegado de polícia e pesquisador de cibercrime**

A percepção que tem sobre políticas de cibersegurança é de que a polícia não está referenciada nos principais debates sobre o tema. Dessa forma, não tem um padrão na aplicação das medidas adotadas sobre responsabilização. Poderiam comentar sobre?

Respostas:

- Louise — Muitas vezes separam cibersegurança de cibercrime, mas, na prática, existe uma cooperação entre ambos para a aplicação das normas. A polícia federal acaba por aplicar as políticas no nível doméstico, então precisa ser instruída para tal. Federalmente vem sendo estabelecido essa conexão, buscando amadurecer o entendimento do papel de cada ator.
- Franklin — Existe a necessidade de uma melhor organização interna, visto que a convenção sobre cibercrime será aprovada e precisamos saber como aplicá-la. Esse é um desafio interessante e importante.
- Vanessa — Mesmo buscando prevenir e mitigar os danos, nos casos em que o ataque aconteça, é necessário haver punição adequada e, para isso, educação de quem ira aplicar a punição. É preciso buscar pensar nesses desafios para, na prática, ter uma efetiva aplicação das normas que estão por vir.

- **Valentina, Programa YOUTH**

Pergunta direcionada à Ada: com a chegada da LGPD muitas empresas começaram a procurar treinamento sobre cibersegurança, porém, na prática, como a balança entre o investimento em infraestrutura de cibersegurança e no conhecimento dos colaboradores sobre o tema.

Resposta:

- Ada — Os principais ataques antes aconteciam através da estrutura (equipamentos), percebendo isso as empresas passaram a investir na infraestrutura. Depois, os ataques migraram para o nível de desenvolvimento, as empresas passaram a investir em softwares e programas melhores. Hoje em dia se há uma lacuna no treinamento dos usuários, os ataques vão se direcionar a eles. Percebendo isso, precisa investir no treinamento e conhecimento das pessoas, sem deixar de investir na infraestrutura e no desenvolvimento.

Pergunta remota:

- **Cristiano Martins**

Qual a opinião de vocês sobre a educação digital fornecida na formação das crianças? Vejo gente cometendo crimes como pirataria, quebra de direitos autorais e, inclusive, quebra da própria segurança.

Respostas:

- Louise — Concorda e diz que é importante agregar diversas áreas ao pensar em educação. É necessário também pensar na formação dos educadores.
- Franklin — Construção de segurança envolve vários conceitos e um deles diz respeito ao direito internacional. Vários desses desafios envolvem a educação, como definir ‘agressão’. Precisamos de mais estudo sobre essa parte conceitual, mais pesquisas para subsidiar a participação dos Estados nos debates globais. Isso deve começar desde a base.

- Vanessa — Há a necessidade de incluir cibersegurança em todos os níveis de ensino, mas vários outros pontos, como a proteção de crianças e adolescentes, também precisam de atenção.
- Michele — Precisamos de mais investimento nas pessoas, em pesquisadores e pesquisas. Temos muitas pessoas saindo do país ou deixando a pesquisa incompleta por falta de investimento. É necessário investir para manter as pessoas no país e aprofundar a especialização destas.