JCPP JOURNAL OF CYBERSECURITY AND PUBLIC POLICIES

Vol. 1, Nº. 1 (Sep./Dec. 2025)
www.cybersecuritypolicies.com.br

CSPP ENTREVISTA

O BRASIL PODE SER POTÊNCIA EM CIBERSEGURANÇA MAS O TEMPO ESTÁ ACABANDO

ENTREVISTADO

Dr. Marcelo Antonio Osller Malagutti

Assessor Especial do Gabinete de Segurança Institucional (GSI) da Presidência da República e Secretário-Executivo do Comitê Nacional de Cibersegurança (CNCiber).

"Fale sobre o papel do Brasil no cenário global de cibersegurança"

CSPP O senhor possui uma formação acadêmica diversificada, com passagens, entre outros, pelo King's College London e Escola de Comando e Estado Maior do Exército (ECEME). Como essa combinação de experiências acadêmicas moldou sua visão sobre cibersegurança e defesa nacional? E, como sua experiência no setor privado influenciou sua abordagem atual em políticas públicas de cibersegurança?

M *Costumo considerar que boa parcela daquilo que somos é resultado de nossas experiências. Em outras palavras, nossas vivências prévias moldam em grande medida a forma como enxergamos o mundo. Afinal, como diz a "lei do instrumento" de Abraham Maslow, "se a única ferramenta que você tem é um martelo, todos os problemas começam a se parecer com pregos". Assim, ter uma* ***experiência variada*** *permite o entendimento de percepções diferentes, o que facilita a construção de consensos. Então não são apenas minhas experiências acadêmicas que moldam minha atuação, mas a soma delas com minha experiência nos setores privado e público. Aliás, me orgulho de ter atuado nos três elementos que constituem a chamada Tríplice Hélice do conhecimento e da inovação – universidade, indústria e governo.*

M *Somo a isso a* ***oportunidade de conhecer diferentes realidades*** *de outros países, ao longo da minha trajetória. O conjunto de vivências me conferiu uma percepção ampliada das demandas de cibersegurança, desde as necessidades práticas do mercado, conceituais da academia até a política da gestão pública, o que, hoje, contribui para um mapeamento mais eficiente das dificuldades e para o fornecimento de respostas mais factíveis e aprimoradas aos problemas.*

Linha DO TEMPO

Anos 1990-2000
Atuação no setor bancário por cerca de 30 anos, desenvolvendo soluções de segurança digital e automação.

2009
Conclui MBA em Estratégia Empresarial e apresenta propostas para fortalecer a indústria brasileira de software.

2010
Curso de Altos Estudos na ESG; caso Stuxnet desperta atenção para riscos cibernéticos no Brasil.

CSPP O que o motivou a dedicar sua carreira à cibersegurança e à defesa nacional?

M *Dediquei aproximadamente trinta anos ao desenvolvimento de tecnologia de automação bancária, onde a confidencialidade, integridade, autenticidade e disponibilidade de informações são fatores essenciais, desde muito antes da existência da série ISO 27000 ou da Lei Geral de Proteção de Dados Pessoais (LGPD), por exemplo. Nesse ambiente, sempre enfrentamos oponentes tecnicamente capazes e motivados, o que nos obrigava a atuar com foco na prevenção e na construção de soluções seguras. Paralelamente, lidei com iniciativas para o fortalecimento da indústria nacional e da qualidade do software.*

M *Tem ainda a famosa frase de John F. Kennedy (1961): "Não pergunte o que o seu país pode fazer por você, mas o que você pode fazer pelo seu país", que reflete um tanto de minha personalidade e da minha cultura familiar. Em 2009, pouco após a conclusão do MBA em Estratégia Empresarial com um trabalho final em que apresentei propostas para uma estratégia de desenvolvimento para a indústria brasileira de software, fui convidado a participar do Curso de Altos Estudos de Política e Estratégia, na Escola Superior de Guerra (ESG), em 2010. Aquele foi o ano do* ***Stuxnet,*** *e foi muito fácil perceber que se um malware semelhante tivesse como alvo o Brasil teria sido desastroso.* ***Não estávamos minimamente preparados para esse novo contexto****. Aprofundei, então, meus estudos sobre a cibersegurança e a sua relação com a defesa e a segurança nacionais, propondo ações que poderiam ser adotadas pelo Brasil. Em 2011, soube que algumas das propostas haviam sido efetivadas.*

M *Em 2013, o ano do Caso Snowden, fui condecorado pelo Ministério da Defesa com a Medalha do Pacificador e retornei para o meio acadêmico, sendo aceito no prestigioso Departamento de Estudos de Guerra do King´s College London para realização do mestrado, iniciado em 2015. Desse ponto foi um passo natural voltar ao Brasil e ingressar no recém-criado doutorado em Ciências Militares do Instituo Meira Mattos (IMM) da ECEME, tal e qual foi me aproximar do Comando de Defesa Cibernética, em particular, no Exercício Guardião Cibernético, o qual realiza, em 2025, sua 7ª edição.*

2011
Algumas de suas propostas são adotadas pelo governo.

2013
Recebe a Medalha do Pacificador do Ministério da Defesa.

2015
Inicia mestrado no King's College London, onde cria o conceito de "Software Power".

2016-2018
Faz doutorado na ECEME; aprofunda estudos em cibersegurança e atua no Comando de Defesa Cibernética.

2019
Integra o GSI e passa a liderar a Política Nacional de Cibersegurança (PNCiber) e o CNCiber.

2021/2022
Ganha o Prêmio Tiradentes por sua tese de doutorado.

2023
Assinatura da PNCiber; consolidação da agenda nacional de cibersegurança.

2025
Atua na criação da Agência Nacional de Cibersegurança (ANCiber) e coordena o 7º Exercício Guardião Cibernético.

"ME ORGULHO DE TER ATUADO NOS TRÊS ELEMENTOS DA TRÍPLICE HÉLICE UNIVERSIDADE, INDÚSTRIA E GOVERNO."

M *Desde então trabalhar para o GSI, na criação da Política Nacional de Cibersegurança (PNCiber), na criação e na secretaria-executiva do Comitê Nacional de Cibersegurança (CNCiber) e na articulação pela criação de uma Agência ou Autoridade Nacional de Cibersegurança (ANCiber), ainda em processo de discussão interna ao governo, e sobre a qual falaremos mais adiante, foram evoluções naturais.*

"Fale mais sobre qual será o papel da ANCiber"

CSPP O senhor aborda o conceito de "Software Power" como ferramenta de ciberdissuasão. Como essa ideia pode ser aplicada na prática pelas políticas públicas brasileiras?

"O CONJUNTO DE VIVÊNCIAS ME CONFERIU UMA PERCEPÇÃO AMPLIADA DAS DEMANDAS DE CIBERSEGURANÇA."

M *O conceito de Software Power surge no mestrado, quando em minha dissertação faço uma "brincadeira", isto é, um paralelo, com os conceitos de hard power e soft power do Joseph Nye, criando o conceito de* ***Software Power*** *como um potencial relevante para o Brasil. O conceito advinha da percepção de que* ***o Brasil perdera o timing de sua inserção no mercado de desenvolvimento de hardware****, mas que ainda seria possível "pegar o trem" do desenvolvimento de software de cibersegurança e ciberdefesa, aproveitando-se de um conjunto de características do institucionalismo brasileiro.*

M *No doutorado investi energia no aprofundamento da ideia e, essencialmente, defendo que o jogo de forças e interesses geopolíticos faz com que todo mundo desconfie dos interesses dos outros países. Logo, uns não vendem certas coisas para outros, com medo de serem atacados ou de que usem o know-how para desenvolvimento de novas armas. De outra parte, uns não compram certas coisas de outros, com medo de que existam backdoors ou outras vulnerabilidades que possam ser exploradas contra eles.* ***Considerando que o Brasil historicamente não é belicoso, beligerante, poderia vender ciberarmas defensivas, e os lucrativos serviços a elas associados, com mais facilidades, pois ninguém se sentiria ameaçado pelo Brasil****.*

*O Brasil, menos beligerante que outras potências do mesmo porte, poderia se valer de três das seis formas de dissuasão que identifico****[1]****, e se aproveitar da sua pujante indústria de software para desenvolver uma* ***indústria capaz*** *não apenas de proteger nossa soberania e interesses no campo cibernético, como também reduzir os prejuízos causados a nossa economia e sociedade pelos ciberataques, além de abrir*

GLOSSÁRIO

ANCiber (Agência Nacional de Cibersegurança)
Órgão proposto para regular e coordenar a cibersegurança no Brasil.

APTs (Ameaças Persistentes Avançadas)
Ataques digitais sofisticados e patrocinados por Estados, que invadem redes críticas de forma silenciosa.

Backdoor
Brecha proposital ou acidental que permite acesso secreto a sistemas.

Ciberdissuasão
Estratégia para desencorajar ataques aumentando custos e riscos para invasores.

CNCiber (Comitê Nacional de Cibersegurança)
Grupo que reúne governo, setor privado e sociedade civil para definir políticas nacionais de cibersegurança.

CTIR Gov (Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo)
Unidade do GSI que monitora e reage a ataques cibernéticos no setor público.

*um gigantesco mercado nacional e internacional de produtos e serviços em cibersegurança. **Um ótimo negócio, do ponto de vista estratégico, econômico e social.** Foi motivo de orgulho ser premiado no concurso de teses de doutorado em defesa nacional, o Prêmio Tiradentes, no biênio 2021/2022.*

Hoje, com informações e conhecimentos mais recentes, estou muito mais convicto das ideias que desenvolvi na tese, e de sua aplicabilidade ao Brasil, não apenas para minimizar riscos, mas fundamentalmente para gerar emprego e renda e inserir o País numa importante frente tecnológica global.

CSPP Quais são os principais desafios para implementar uma estratégia eficaz de ciberdissuasão no contexto brasileiro?

E-Ciber (Estratégia Nacional de Cibersegurança)
Documento com diretrizes e metas para fortalecer a proteção digital do Brasil.

Edge Computing (Computação de Borda)
Processamento de dados próximo à origem, permitindo respostas mais rápidas e seguras.

ISACs (Information Sharing and Analysis Centers)
"Cooperativas" de empresas para compartilhar informações sobre ataques e defesas.

LLMs (Large Language Models)
Modelos de IA, como ChatGPT, que geram textos e são explorados por hackers para ataques mais sofisticados.

M *Minha pesquisa, e minha experiência, ao longo dos anos, mostraram que **algumas das nossas dificuldades advém justamente do nosso institucionalismo histórico**. A nossa certeza de que "Deus é brasileiro" nos faz achar que nada de mal nos acontecerá. Nossa confiança no "jeitinho brasileiro" nos faz acreditar que, numa eventual crise, vamos ter uma forma criativa de nos safarmos. Somos um país que encara com naturalidade a ideia de "leis que pegam e leis que não pegam". E a maioria dos brasileiros tem certeza de que, como não somos beligerantes, ninguém jamais nos atacará. Ainda, temos uma tradição de evitar o empoderamento do Estado, por medo de sua atuação contra o indivíduo, de sorte que evitamos ações como o fortalecimento de capacidades militares e de inteligência, consideradas normais às potências médias e grandes pelo mundo. Então, eliminamos, culturalmente, várias das formas de dissuasão. Kissinger, um dos expoentes do realismo nas Relações Internacionais, teria dito que "diplomacia sem recursos de poder é um mero exercício de retórica". Isto posto, nações com uma cultura pautada pelo Realismo não considerariam seriamente uma ameaça nossa.*

M *Dessa forma, sobram poucas alternativas para exercermos capacidades dissuasórias. Uma delas é a "**dissuasão pela negação**", elevando nossas capacidades defensivas para "negar ao oponente" um acesso fácil aos seus objetivos. Essencialmente, teríamos que "subir a barra" das defesas, subindo os custos e o risco de exposição do ataque e do atacante para superá-las, tornando a relação do custo/benefício do objetivo menos atrativa. Outra, bastante associada à primeira, consiste em capacidades de investigação e atribuição melhores,*

ReGIC / ReNGIC (Rede de Gestão de Incidentes Cibernéticos)
Sistema colaborativo de análise e resposta a ciberataques no Brasil.

de forma a permitir a dissuasão por individualização". Ao invés de acusarmos um país, o que não é do nosso perfil e tradição diplomática, acusaríamos um cidadão específico, denunciando-o em tribunais e, numa eventual condenação, acionaríamos ***sanções internacionais*** *- um instrumento a que EUA, Reino Unido, França, Alemanha, entre outros, têm recorrido cada vez mais. Essas capacidades defensivas e investigativas, também, permitem até um tipo de retaliação (elemento de deterrência ou dissuasão por ameaças), do tipo que cria constrangimentos, públicos ou mesmo privados.* ***Não são muitas as opções, mas temos algumas.***

CSPP Na sua visão, quais são as principais ameaças cibernéticas que o Brasil enfrenta atualmente?

M *Temos várias! No campo das ciberameaças* ***o ransomware é uma praga que nos assola****. Cresce muito o número de casos, o número de setores vitimados, e o número de gangues que nos atacam ano a ano. Vazamentos de dados, frequentemente associados ao ransomware, também crescem muito. São dezenas de milhares de casos aqui, centenas de milhares ali, e nunca para. Outro problema é a* ***proliferação de APTs*** *(as ameaças persistentes avançadas) que andam bisbilhotando nossas redes, em particular aquelas de provedores de serviços essenciais e de operadores de infraestruturas críticas. APTs atuam patrocinadas por Estados. Então não é uma questão exclusivamente de criminalidade, mas ter agentes a serviço de outro Estado Nacional dentro de nossas redes não é bom. Aliás, lá por meados dos anos 2010, um então comandante do USCyberCom disse algo mais ou menos como* ***"nada de bom pode vir de alguém bisbilhotando nossas redes".*** *Esse conceito ainda é 100% atual.*

Ransomware
Malware que sequestra dados e exige pagamento para liberá-los.

Software Power
Conceito criado por Malagutti: usar a força da indústria de software brasileira para proteger o país e gerar negócios.

Stuxnet
Malware famoso de 2010 que sabotou o programa nuclear do Irã; citado como marco global da cibersegurança.

M *Acredito que nossa principal ameaça não é o malware, e não vem de fora. É a nossa* ***falta de cultura de cibersegurança e segurança da informação****. Demora-se a convencer um decisor, público ou privado, de que cibersegurança é investimento, e não despesa; ou de que ela pode ser uma questão existencial para uma instituição. Isso dificulta muito as coisas. Num recente artigo intitulado "Cibersegurança: O Custo de Não Fazer"* ***[2]*** *eu e meu colega do CNCiber Rony Vainzof apontamos argumentos para mostrar que investir na governança nacional da cibersegurança é um ótimo investimento para sociedade e governo. Todo mundo sempre soube que o número de ataques ao setor Financeiro era grande, bem como aos setores Governo e Justiça. Mas setores*

"FOI MUITO FÁCIL PERCEBER QUE, SE UM MALWARE COMO O STUXNET TIVESSE COMO ALVO O BRASIL, SERIA DESASTROSO."

que sempre se sentiram poucos atrativos agora disputam, e até superam, aqueles, como Saúde, Varejo, e Manufatura, dentre outros tantos. Ninguém está imune! ***Não se trata mais de "SE alguém vai ser atacado, mas de QUANDO".*** *E a questão que trabalhamos agora é:* ***COMO responderemos****. A resiliência - capacidade de seguir operando, ainda que de forma limitada, evitando uma total disruptura das operações - é fundamental no contexto de Serviços Essenciais.*

"EM 2011, SOUBE QUE ALGUMAS DAS PROPOSTAS HAVIAM SIDO EFETIVADAS."

M *Uma outra questão é que o Brasil tem diversas ilhas de excelência em cibersegurança. Mas elas são pequenas. Muito pequenas! Razão pela qual costumo dizer que temos uma "****micronésia de ilhas de excelência****" no tema, como alguns setores do GSI, CERT.Br, RNP, ANATEL e Banco Central, MGI e SERPRO, Polícia Federal e algumas polícias estaduais, para citar algumas. E que produzem dezenas de boas iniciativas isoladas. Mas nos falta capacidade de coordenação e de multiplicação dos resultados.* ***Precisamos com urgência de uma ANCiber, uma entidade especializada, tecnicamente qualificada, de natureza permanente*** *(de Estado),* ***de abrangência nacional*** *(três poderes, União, estados e municípios, iniciativa privada),* ***e civil*** *(mas com boa interação com a ciberdefesa, que toca aos militares e na qual, a despeito de recursos limitadíssimos, fazem um trabalho de excelência), para regular, fiscalizar, coordenar e controlar a cibersegurança nacional. Quando começamos o processo, há pouco mais de dois anos, diziam que seria impossível. Hoje não acho mais apenas possível, mas provável, termos isso, e sinto que não vai demorar muito mais. Em termos de "tempo de Estado", digo.*

ANCiber

"O BRASIL PERDEU O 'TIMING' DO HARDWARE, MAS AINDA PODE PEGAR O TREM DO SOFTWARE."

"Cite algumas das ilhas de excelência para o conhecimento dos leitores."

CSPP Como o país pode equilibrar a necessidade de segurança cibernética com a proteção das liberdades individuais e da privacidade dos cidadãos?

M ***Essa é sempre a questão fundamental a ser debatida****. Diz um ditado popular que "a virtude está no meio". Há que sempre haver um equilíbrio. Uma das funções precípuas do Estado é garantir a liberdade do cidadão. Outra é garantir a segurança desse mesmo cidadão. Thomas Hobbes nos ensinou que o preço da segurança é ceder uma parte de nossa liberdade. Se todo mundo faz o que quer, com total liberdade, não há segurança. E John Philpot Curran estabeleceu que o preço da liberdade é a eterna vigilância. Quem estabelece os limites*

dessas coisas é a lei. E para garantir a lei o Estado precisa ter força. Sem a presença do Estado não há a aplicação da lei. E um dos princípios da soberania de um Estado é a sua capacidade de aplicar a lei. Tudo somado, temos que ter um Estado forte, soberano e vigilante, para fazer valer a lei estipulada livremente por seu povo, assegurando a esse povo liberdade e segurança, inclusive contra excessos desse mesmo Estado. Isso só se consegue com um debate franco, aberto, e com base em princípios e conceitos claros. Fácil, não é?

"O BRASIL PODE VENDER CIBERARMAS DEFENSIVAS SEM AMEAÇAR NINGUÉM."

M *Fácil não é! Mas Einstein dizia que "Tudo deve ser feito o mais simples possível, mas não mais simples do que isso". Então, devemos simplificar as coisas tanto quanto possível, mas sem que essa simplificação as tornem irrelevantes nem incompreensíveis. Vamos exemplificar com um dos problemas da cibersegurança, que é a mistura de conceitos. Por exemplo, algumas pessoas associam a cibersegurança com o controle de conteúdo de plataformas digitais. Mas, são coisas muito diferentes.*

"A INDÚSTRIA DE SOFTWARE É UMA OPORTUNIDADE ESTRATÉGICA, ECONÔMICA E SOCIAL."

A cibersegurança, essencialmente, consiste na garantia da Confidencialidade, da Integridade, da Autenticidade e Disponibilidade (resumidas no acrônimo CIAD) da informação processada, transmitida ou armazenada em ciberativos (hardware, software ou dados). *Mas a cibersegurança não se ocupa do conteúdo dessa informação (ou desinformação). Então, temos que pensar em como uma determinada informação será acessada apenas por quem de direito (confidencialidade), que ela vem de quem deveria vir (autenticidade), que ela não foi adulterada no processamento ou transporte (integridade), e que ela esteja disponível quando e onde necessária (disponibilidade). Logo, em nenhum momento o conteúdo dela é relevante do ponto de vista da cibersegurança. O conteúdo pode vir a ser um caso de calúnia ou difamação, ou de apologia ao crime, ou de outros ilícitos penais. E como tal deve ser tratado, por quem de direito. Mas isso, reitero, não é uma questão de cibersegurança. Similarmente, se algum algoritmo impulsiona artificialmente determinado tipo de mensagem, com base em seu conteúdo, e isso beneficia ou prejudica alguém de forma indevida, isso também não é uma questão de cibersegurança.*

"A NOSSA CERTEZA DE QUE 'DEUS É BRASILEIRO' NOS FAZ ACHAR QUE NADA DE MAL NOS ACONTECERÁ."

Se uma pessoa cai num golpe a partir de uma mensagem recebida numa rede social, e entra voluntariamente na sua conta bancária e envia dinheiro para o fraudador, há que se separar o problema em suas componentes. Um golpe é uma fraude, que é crime. Mas, seria também se o usuário caísse

na conversa de alguém na porta de uma agência bancária, entrasse, sacasse dinheiro, e desse para o criminoso em troca de um "bilhete premiado de loteria". Não se trata de uma questão de cibersegurança. Mas se alguém envia uma mensagem com um malware que se instala em seu celular, e depois rouba os dados de acesso ao seu banco, isso é um problema de cibersegurança.

"SOMOS UM PAÍS QUE ENCARA COM NATURALIDADE A IDEIA DE 'LEIS QUE PEGAM E LEIS QUE NÃO PEGAM'."

M *Outra questão um tanto mal-entendida é a cibersegurança e o vazamento de dados. Há quem ache que a ANPD (Autoridade Nacional de Proteção de Dados) seria o bastante para garantir a cibersegurança nacional. Ledo engano! Costumo dizer que a cibersegurança é ex-ante, enquanto o vazamento de dados é ex-post. Ainda, o vazamento de dados pode ocorrer por meios físicos, não digitais. Então, é possível ocorrer um vazamento de dados sem um ciberincidente. Por exemplo, se alguém entra numa sala e rouba dados de uma pasta de documentos de um gaveteiro. Assim como, existem diversos ciberincidentes graves que não vazaram dados. Mais ainda, a ANPD trata de dados pessoais sensíveis. E há vazamento de dados que não envolvem dados pessoais, e muito menos ainda dados pessoais sensíveis. Exemplos são os vazamentos de dados de projetos industriais (a chamada espionagem industrial). Então,* ***não podemos achar que a cibersegurança se limita à proteção de dados pessoais.***

"KISSINGER DISSE: 'DIPLOMACIA SEM PODER É MERA RETÓRICA'."

Entendidos esses conceitos, fica mais fácil evoluirmos o debate sobre a necessidade de cibersegurança, e de como é possível fazermos isso sem avançarmos sobre os direitos individuais. Mas é preciso termos serenidade e honestidade intelectual nesse debate. E senso de urgência!

"NÃO SE TRATA MAIS DE 'SE' VAMOS SER ATACADOS, MAS DE 'QUANDO'."

Até agora, os exemplos que dei foram relativos ao cidadão comum, coisas que todos sofremos ou conhecemos alguém próximo que já sofreu. Mas a cibersegurança no Brasil vai muito além disso. Um ciberataque recentemente paralisou o INCA (Instituto Nacional do Câncer), impedindo a realização de cirurgias e tratamentos para pacientes em situações delicadas. Outro ciberincidente afetou as operações do IPEN (Instituto de Pesquisas Energéticas e Nucleares), paralisando a produção de radiofármacos por mais de duas semanas. E esses fármacos, por sua natureza de decaimento radiativo, têm ciclo de vida muitíssimo curto, sendo difícil sua importação. Logo, essa paralisação da produção prejudicou a realização, por exemplo, de exames de imagem com contraste, o tratamento de radioterapia, e provocou tantos outros problemas. Imagine-se o impacto da paralisação do sistema

elétrico, por exemplo. Ou do PIX. Ou da rede de telefonia. ***A prevenção desses incidentes envolvendo serviços essenciais e infraestruturas críticas, notadamente por causa cibernéticas, é uma questão de cibersegurança de enorme relevância. E deve ser uma questão de Estado, sem ideologia.*** *Não é de esquerda ou de direita. O governo trabalhista do Reino Unido está incrementando a já avançada (em relação à nossa) cibersegurança britânica. O governo conservador italiano também. Assim como o governo socialista de Portugal. Os EUA, a Rússia, a China, o Japão, a Coreia, a Alemanha, a França, a Austrália, o Canadá, o Uruguai, o Chile... Todos eles estão trabalhando forte para aumentarem o escopo de suas ações. E todos eles já têm suas "agências de cibersegurança", como são chamados esses órgãos no jargão da área, há alguns anos.* ***O Brasil está bastante atrasado nisso.*** *E, em parte, por causa da dificuldade de se discutir o tema com serenidade, por conta da mistura de assuntos que são muito mais polêmicos que a cibersegurança em si. Se a gente separar o debate, tenho convicção de que o tema da cibersegurança avança fácil.*

"TEMOS UMA MICRONÉSIA DE ILHAS DE EXCELÊNCIA EM CIBERSEGURANÇA."

CSPP A PNCiber foi assinada em fins de 2023, estabelecendo diretrizes estratégicas para a proteção dos ativos digitais do país. Na sua avaliação, quais são os principais desafios que o Brasil enfrenta atualmente para sua efetiva implementação?

M *A situação fiscal do país é complexa, e como eu disse muita gente pensa na criação de um órgão de governança como um custo, e não como um investimento. Avalio que a criação da PNCiber, e em seu bojo a do CNCiber, colocou na pauta nacional o tema da cibersegurança. O assunto foi amadurecendo, e foi ganhando mais e mais apoios. Estamos, hoje, em um contexto, no qual a sociedade civil, que tem uma representação importante no CNCiber, pede ativamente uma ação mais incisiva do Governo. O Legislativo, que criou uma Frente Parlamentar de Apoio à Cibersegurança e à Defesa Cibernética, também. As engrenagens se movimentam. Numa recente reunião do CNCiber houve um momento em que um representante do Governo comentou que, em 20 anos de vida pública, era a primeira vez que ele via a iniciativa privada pedir regulação. E um representante da Sociedade respondeu, com humor: "e gasto público"! Isso porque* ***a percepção já começa a mudar para a visão de que não é gasto, mas investimento.*** *E que os riscos de não ter regulação desse tema num país como o nosso já estão inaceitáveis. Acho, ou melhor, sinto, que estamos perto de grandes avanços.*

"PRECISAMOS DE UMA ENTIDADE ESPECIALIZADA, TÉCNICA, CIVIL, NACIONAL E PERMANENTE."

CSPP Considerando os avanços obtidos até agora, quais seriam, na sua visão, os próximos passos estratégicos para consolidar um ecossistema nacional de cibersegurança robusto, inclusivo e adaptado aos riscos emergentes?

M *Temos alguns passos essenciais iniciados. Primeiro, uma* ***atualização da nossa Estratégia Nacional de Cibersegurança****, a E-Ciber, que agora o decreto da E-Ciber foi assinado em 04/08/25 e publicado em 05/08/25. Segundo, a discussão de um Marco Legal da Cibersegurança e do Órgão de Governança da Cibersegurança. Quanto a esse, em minha visão pessoal, o melhor arranjo, considerando o institucionalismo histórico nacional, seria o de uma Agência Reguladora. Mas não creio que minha opinião deva ser um entrave no processo, motivo pelo qual acredito que um arranjo institucional como o do IBAMA ou INMETRO, autarquias reguladoras que não são agências reguladoras, pode funcionar também. Como diz a sabedoria popular, "o ótimo é inimigo do bom". E o bom seria muitíssimo melhor do que nada! Podemos avançar, aprender, desenvolver processos, conhecimento, normas, e depois evoluir institucionalmente, quando condições mais propícias se apresentarem. "Uma longa jornada começa com um primeiro passo", diz o provérbio chinês.*

"CIBERSEGURANÇA NÃO SE OCUPA DO CONTEÚDO DA INFORMAÇÃO."

M *No tocante aos riscos emergentes, temos uma questão muito importante a considerar, que são as chamadas Tecnologias Computacionais Emergentes, um conjunto de tecnologias computacionais que têm capacidades disruptivas e que certamente afetarão a cibersegurança da sociedade num tempo não muito distante.*

Todo mundo pensa logo em Inteligência Artificial (IA). Isso porque os Grandes Modelos de Linguagem (LLMs), estão em evidência para o grande público, e assim chamam a atenção da mídia e dos legisladores, por exemplo. ***Já temos muitos ciberincidentes envolvendo exploração de vulnerabilidades e phishing gerados por sistemas de IA baseados em LLMs recentemente, aumentando a velocidade e a precisão dos ataques****, e elevando a capacidade técnica de atacantes não muito qualificados. Mas a IA é muito mais que apenas os LLMs. Temos ainda em desenvolvimento a IA Geral, com a capacidade de compreender, aprender e realizar qualquer tarefa intelectual que um ser humano seja capaz de fazer, além apenas da linguagem. E a IA Física, a IA integrada a sensores, dispositivos, máquinas ou robôs que têm uma presença tangível no mundo real.*

"TEMOS QUE SEPARAR CIBERSEGURANÇA DE REGULAÇÃO DE CONTEÚDO."

“A CIBERSEGURANÇA É EX-ANTE. O VAZAMENTO DE DADOS É EX-POST.”

Para além da IA, temos a materialização da promessa da Computação Quântica, que promete mudar a escala da capacidade computacional, trazendo o potencial de revolucionar diversas indústrias e resolver problemas considerados intratáveis pela computação clássica. *Um impacto direto desse aumento da capacidade computacional seria a capacidade de quebra dos algoritmos de criptografia hoje em uso, que levariam séculos de processamento com os atuais computadores para serem quebrados, em alguns minutos ou mesmo segundos. Por isso, há relatos de nações que estariam copiando gigantescas bases de dados criptografadas de outras nações, para decriptografá-las daqui a alguns anos e ter acesso aos dados que hoje estão protegidos. É claro que algumas informações, naquele momento, terão perdido seu valor. Mas, é fácil pensarmos em muitos dados que continuarão relevantes daqui a 20 anos. O combate a isso pode ser feito com o uso de algoritmos de criptografia quantum-resistant, comumente (e erroneamente) chamados de pós-quânticos.*

M *Outra tecnologia que preocupa no âmbito da cibersegurança são as redes de alta velocidade e baixa latência (5G e 6G, por exemplo), que permitiriam que volumes cada vez maiores de dados fossem exfiltrados (roubados) mais rapidamente, ou que microcâmeras e microfones, cada vez menores e com melhor definição, sejam implantados de forma a permitirem a captura de dados sensíveis.*

“O BRASIL ESTÁ ATRASADO. MAS HOJE NÃO ACHO MAIS APENAS POSSÍVEL – ACHO PROVÁVEL.”

Exemplifiquei apenas algumas que já colocam problemas de segurança reais para os países, empresas e pessoas. Mas a lista não acaba aí. Temos um rol enorme, que inclui Computação de Alto Desempenho (HPC), Computação de Borda (Edge Computing), Computação em Nuvem, Computação Espacial, Computação Neuromórfica, Computação Verde, Computação Distribuída por Software, Biocomputação, Interfaces Neurais (BCI), Automação Robótica, Robótica Avançada, Robótica Colaborativa, Sistemas Autônomos, Veículos Autônomos, IoT Avançada, IoT Industrial, Manufatura Aditiva Avançada... Tem para todos os gostos! E desgostos, quando pensamos em termos de cibersegurança e segurança da informação.

E uma coisa interessante dessas tecnologias é que elas se realimentam. Umas potencializam, e amplificam o alcance e o risco, de outras. Tecnologias que pareciam dominadas, e com riscos controlados, passam a oferecer novos riscos. Posso citar como exemplos Big Data, Cidades Inteligentes (Smart Cities), Criptoativos, Energias Renováveis Inteligentes, Identidade Digital, Realidade Estendida (XR), Redes Inteligentes (Smart

Grids), e Tecnologias de Descentralização. Várias delas são potencializadas pelos sensores, elemento fundamental do IoT, e pela capacidade de processamento ampliada, oferecendo pontos de preocupação relevantes que precisam ser pensados, debatidos, e quase certamente, em alguma medida, regulados, fiscalizados e controlados. E isso tudo está aí, à nossa porta!

CSPP Como o Comitê Nacional de Cibersegurança está estruturado e qual é o papel das diferentes entidades governamentais e da sociedade civil nesse comitê?

M *Integram o CNCiber 13 entidades da administração federal direta (ministérios), 3 entidades da administração indireta (ANATEL, BACEN e CGI) e 9 representantes da sociedade, divididos em 3 grupos: 3 entidades de direito digital; 3 entidades de ciência, tecnologia e inovação; e 3 entidades representando o setor empresarial. Participam ainda, como convidados, e assim apenas com direito a voz, sem voto, a ABIN e o TCU.*

"ESSE DEBATE PRECISA DE SERENIDADE, HONESTIDADE INTELECTUAL E SENSO DE URGÊNCIA!"

O papel desse Comitê é o de formular propostas para a evolução da PNCiber, e por extensão do contexto da cibersegurança nacional. *A forma usual de trabalho é a criação de grupos de trabalho temáticos, os GTTs, que se debruçam sobre determinado tema por alguns meses, e elaboram propostas que depois são apreciadas pelo Pleno do CNCiber e, se aprovadas, encaminhadas para o Governo Federal. Essa estrutura assegura às discussões uma visão bastante plural dos temas discutidos. Todos os partícipes apresentam seus argumentos, e ouvem os argumentos dos demais. Na grande maioria dos casos os documentos produzidos são elaborados num processo colaborativo, em que cada termo é escolhido de forma consensuada. No próprio Pleno do CNCiber a enorme maioria das deliberações se resolve por unanimidade, depois de apresentados os argumentos de todos os interessados. Posso dizer que é um processo muito produtivo e muito rico.*

"A CIBERSEGURANÇA DEVE SER UMA QUESTÃO DE ESTADO, SEM IDEOLOGIA."

CSPP Qual é o papel do setor privado na construção de uma estratégia nacional de cibersegurança?

M *É um papel enorme, "gigante", como se diz popularmente! Diversas instituições apresentaram propostas de temas a serem tratados. Outras cobraram atenção a esse ou àquele tema. Tivemos dezenas de encontros, seminários, reuniões, visitas. E posso assegurar que vamos sair de uma E-Ciber de primeira geração para uma E-Ciber quase de terceira*

geração. Quase pelo fato de que não teremos como dar um "salto quântico" e pular todos os pontos das estratégias de segunda geração pelo atraso institucional que ainda temos em relação às nações mais avançadas no tema, várias das quais já foram citadas.

"INTELIGÊNCIA ARTIFICIAL, COMPUTAÇÃO QUÂNTICA E 6G TRAZEM RISCOS REAIS E IMINENTES."

E esse papel persiste nos demais temas. Nas audiências no Senado temos reiteradamente ouvido manifestações do Setor Privado em apoio às nossas iniciativas, e costumeiramente pedindo mais ações e celeridade. Essa cobrança permanente é um importante combustível para a ação da administração pública.

CSPP Como o governo federal tem trabalhado para fomentar parcerias com empresas e instituições acadêmicas nessa área?

M *Além dos representantes formalmente participando do CNCiber, temos instituições outras que interagem bastante conosco. No campo acadêmico posso exemplificar com a SBC (Sociedade Brasileira de Computação), que nos prestigia convidando a participar de seus eventos e discussões. No campo das empresas temos um bom exemplo com a FECOMÉRCIO-SP, que mantém contato permanente conosco. E há várias outras empresas, associações e congêneres participando ativamente, embora de forma indireta, dos debates. E apresentando ideias. Temos também nossos amigos do BID (Banco Interamericano de Desenvolvimento) que nos dão um suporte incrível, geram relatórios de altíssimo nível, com informações importantes, promovem eventos, entre outros instrumentos.*

"O ÓTIMO É INIMIGO DO BOM. PRECISAMOS AVANÇAR COM O QUE FOR POSSÍVEL."

M *Como o processo administrativo-burocrático-legal dos poderes Executivo e Legislativo é mais lento do que a capacidade de organização e inovação do setor privado e da academia, estamos tentando fomentar, por exemplo, a auto-organização do setor produtivo em arranjos de* ***Centros de Análise e Compartilhamento de Dados, internacionalmente conhecidos como ISACs, para a melhoria da proteção e resiliência contra ciberataques.*** *Basicamente, ao invés de cada instituição tentar se proteger sozinha, contratando profissionais que são raros e caros, elas se associam numa espécie de "cooperativa", em que os associados pagam uma taxa, e a "cooperativa" tem pessoal e recursos para receber, analisar e compartilhar dados com os cooperados. E essa cooperativa se associa a uma "federação de cooperativas", no caso a ReGIC (Rede Federal de Gestão de Incidentes Cibernéticos), mantida pelo Centro de Prevenção e Tratamento de Resposta a Incidentes*

Cibernéticos de Governo (CTIR Gov), localizado no GSI. Aliás, esperamos que em breve a ReGIC passe a ser uma ReNGIC (Rede Nacional, e não Federal) e que o CTIR Gov possa passar a ser o CTIR Br, ampliando sua abrangência para o âmbito nacional. E é bom esclarecer que o CTIR Gov também trabalha em cooperação com seus congêneres nacionais, o CERT.Br, ligado ao Comitê Gestor da Internet no Brasil, e o CAIS-RNP, que foca nas redes acadêmicas brasileiras. E também com seus similares internacionais. Portanto, expande-se a abrangência por meio de ***uma estrutura de "rede de redes" de análise e compartilhamento de informações de ameaças, permitindo que a identificação de um potencial problema seja transformada num alerta e em recomendações de como evitar ou interromper um ciberataque****.*

"A CIBERSEGURANÇA NÃO É COISA DE NERD DE TI. NÃO MESMO!"

CSPP Para os jovens profissionais interessados em seguir carreira na área de cibersegurança, que conselhos o senhor daria?

M ***Esse é um campo fantástico. Altamente promissor.*** *E que oferece, e demanda, muitas perspectivas de conhecimento distintas. Minhas duas filhas estão enveredando por esta área. Uma cursou Relações Internacionais, fez mestrado em Conflitos Internacionais (dissertação em cibersegurança) e MBA em cibersegurança. A outra graduou-se em Ciência da Computação e agora cursa um MBA em cibersegurança. As duas já me ajudaram na elaboração de material e na condução dos Exercícios Guardião Cibernético, e em vídeos sobre cibersegurança.*

"É UMA ÁREA ENORME, APAIXONANTE E EM EXPANSÃO. TEM LUGAR PARA TODOS."

M *Então, recomendo aos jovens, de todas as idades, que se interessem, que procurem identificar que tipo de conhecimento podem associar ao seu cabedal, ou background, para ingressarem na área.* ***Há fóruns, cursos e certificações gratuitos****, aos montes, na Internet, para os mais variados níveis de conhecimento. Leiam, pesquisem, atualizem-se. Vocês verão que é uma área enorme, e apaixonante. E é fácil perceber que não é só "coisa dos nerds de TI". Não mesmo*!

CSPP Nosso muito obrigado Dr. Marcelo A. O. Malagutti.