SENADO FEDERAL

Gabinete do Senador **ESPERIDIÃO AMIN**

# SENADO FEDERAL

# COMISSÃO DE RELAÇÕES EXTERIORES E DE DEFESA NACIONAL

## RELATÓRIO DE AVALIAÇÃO DE POLÍTICA PÚBLICA

## A POLÍTICA NACIONAL SOBRE DEFESA CIBERNÉTICA

**PRESIDENTE: SENADOR RENAN CALHEIROS**

**RELATOR: SENADOR ESPERIDIÃO AMIN**

Brasília, 9 de dezembro de 2024

# SUMÁRIO

## 1. APRESENTAÇÃO

A avaliação de políticas públicas tem como objetivo principal aprimorar a gestão do Estado, por meio da mensuração de sua eficiência, eficácia e efetividade. O resultado da avaliação é fundamental para orientar as ações do Poder Público. A Resolução do Senado Federal n° 44, de 2013, prevê que a Casa Legislativa realize a avaliação de políticas públicas, que buscará, entre outras medidas, adequar os dispositivos normativos às necessidades sociais.

Nos termos do art. 1º dessa normativa, "as comissões permanentes selecionarão, na área de sua competência, políticas públicas desenvolvidas no âmbito do Poder Executivo, para serem avaliadas". Mediante a aprovação, no dia 25 de abril de 2024, do Requerimento nº 6, de 2024, a Comissão de Relações Exteriores e Defesa Nacional (CRE) decidiu avaliar a Política Nacional de Cibersegurança, o que foi impulsionado no âmbito da Subcomissão Permanente de Defesa Cibernética, instalada no dia 14 de maio de 2024.

No Brasil, os assuntos relacionados às vulnerabilidades digitais foram tratados, inicialmente, sob a égide da Segurança da Informação, pelo Decreto nº 3.505, de 2000, que instituiu a Política de Segurança da Informação, que foi revogado pelo Decreto nº 9.637, de 2018 (alterado pelo Decreto nº 9.832, de 2019; Decreto nº 10.631, de 2021; Decreto nº 10.641, de 2021; Decreto nº 10.849, de 2021; Decreto nº 11.856, de 2023).

O Decreto nº 10.222, de 2020, aprovou a Estratégia Nacional de Segurança Cibernética, válida para o quadriênio 2020-2023. Por fim, o

Decreto nº 11.856, de 2023, instituiu a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Importa ressaltar que a Política Nacional de Cibersegurança envolve a Estratégia Nacional de Segurança Cibernética e o Plano Nacional de Cibersegurança. Já o Comitê Nacional de Cibersegurança foi criado no âmbito da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, com a finalidade de acompanhar a implementação e a evolução da Política Nacional de Cibersegurança. Estes serão os pontos centrais de atenção para a avaliação da política pública em questão.

No âmbito da Defesa, o denominado Setor Cibernético foi destacado pela Estratégia Nacional de Defesa (END), aprovada pelo Decreto nº 6.703, de 2008, e considerado, ao lado do setor espacial e do setor nuclear, como um dos três setores estratégicos e essenciais para a Defesa Nacional. Desde então, o setor tem sido contemplado em destaque pelas demais Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END) formuladas. Pela Portaria Normativa nº 3.010/MD, de 18 de novembro de 2014, foi aprovada a Doutrina Militar de Defesa Cibernética, substituída pela nova doutrina, expressa na Portaria GM-MD n° 5.081, de 16 de outubro de 2023.

O interesse da Casa por esse tema não é novo. Em 2013, o Senado Federal instaurou uma Comissão Parlamentar de Inquérito (CPI) destinada a "investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar e-mails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal".

Na Câmara dos Deputados, em 2015, também foi instaurada Comissão Parlamentar de Inquérito (CPI), destinada a "investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país", para qual fui designado relator. O relatório final da CPI concluiu pela apresentação de cinco projetos de lei para aprimorar a legislação e tipificações penais relacionadas aos crimes cibernéticos, além disso, o trabalho também recomendou ao Executivo a adoção de diversas medidas para melhorar a segurança da infraestrutura de tecnologia da informação na Administração Pública.

De todos os projetos apresentados pela CPI, somente um ainda tramita, o PL nº 5200, de 2016, que tem como escopo a ampliação da abrangência do crime de invasão de dispositivo informático. A proposição aguarda análise da Câmara dos Deputados. Os demais projetos foram arquivados em 2019, em decorrência do fim da legislatura. Por fim, a CPI também recomendou a aprovação de vários projetos que foram considerados pertinentes por preencherem lagunas legais verificadas durante os trabalhos.

Em 2019, a Comissão de Relações Exteriores avaliou a política sobre defesa cibernética, da qual este Relator também teve a oportunidade de relatar e, como um dos resultados, justamente provocou a criação dessa Comissão da Subcomissão Permanente de Defesa Cibernética.

Conforme levantamento divulgado pela empresa de soluções de cibersegurança FORTINET, com base dos dados do FortiGuard Labs, o Brasil foi o segundo país mais atingido da América Latina e Caribe em 2022, com 103,16 bilhões de tentativas de ataques cibernéticos. O número implica aumento de 16% com relação ao ano anterior (88,5 bilhões) e representa

quase 30% do número total dos países da região que sofreram com mais de 360 bilhões de tentativas de ciberataques.

É evidente que organizações transnacionais do crime organizado são ameaças concretas não somente à estabilidade da região, como também do Brasil, uma vez que suas estratégias e métodos, embora diferentes na busca de seus objetivos, baseiam-se na aplicação limitada de boas práticas e padrões de cibersegurança nos níveis empresarial e estatal.

De acordo com a Cybersecurity Ventures, o crime cibernético deve custar ao mundo US$ 9,5 trilhões em 2024. Se fosse um país, o crime cibernético seria a terceira maior economia do mundo. No âmbito das relações internacionais, avaliar as iniciativas do Ministério das Relações Exteriores nesse campo, portanto, é de suma importância. É fundamental avaliar a participação do país em fóruns internacionais, redes de partilha de informações, exercícios conjuntos e esforços de investigação colaborativa. Tais atividades não apenas fortalecem a capacidade nacional de resposta às ameaças cibernéticas, mas também promovem normas globais de segurança cibernética, contribuindo para um ambiente digital mais seguro e resiliente.

Nesse contexto, entre 10 e 12 de abril de 2024, este Relator teve a honra de ir ao Panamá representar o Brasil na I Conferência STIC de Cibersegurança promovida pelo Governo da Espanha e apoiada pela Organização dos Estados Americanos - OEA e pelo Banco de Desenvolvimento Interamericano - BID.

Nesse evento, foi concordada entre os principais especialistas e profissionais de cibersegurança, bem como entre os Senadores e parlamentares ibero-americanos, a necessidade de formar uma “Bancada

Digital", como forma de preparação de uma futura convenção que abranja medidas de interesse coletivo para a cibersegurança. Assim, foi aceito e adotado pelos participantes o mote por mim sugerido, baseado em conceito matemático do MDC: “Mínimo Denominador Comum” que, em breve resumo, se revestiria na busca pelo desenvolvimento de uma legislação convergente entre países da América Latina sobre o tema. As iniciativas de cibersegurança existentes na área de inteligência também merecem atenção especial dessa avaliação de política pública.

No âmbito da Agência Brasileira de Inteligência (ABIN), dada a competência do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CEPESC) em áreas cruciais como tecnologia da informação, inteligência cibernética e segurança de dados, conforme o art. 7º, do Decreto nº 11.816, de 6 de dezembro de 2023, sua liderança tem um entendimento profundo das necessidades do País e dos desafios por nós enfrentados. Haja vista sua experiência em questões de segurança nacional e estratégias de combate a ameaças cibernéticas, a participação da ABIN nessa avaliação de política, como principal órgão responsável pela Inteligência brasileira, é, de igual modo, fundamental. Desse modo, o CEPESC-ABIN pode oferecer percepções valiosas e contribuir significativamente para o aprimoramento das políticas públicas relacionadas à cibersegurança, fortalecendo a defesa digital do País e protegendo os seus interesses estratégicos. Não se pode olvidar da dimensão humana que essa avaliação também carrega em seu âmago.

Avaliar os esforços nacionais na construção de uma força de trabalho capacitada em segurança cibernética é fundamental, seja por meio de programas educacionais, de treinamento ou de desenvolvimento

profissional. É crucial dispor de um conjunto robusto de talentos para atender à crescente demanda por expertise em segurança cibernética. Este exame pressupõe a análise das iniciativas das estruturas da administração pública para fazer frente a essas novas ameaças, bem como a reflexão sobre como o Congresso pode atuar para que uma nova geração de talentos capacitada surja e seja, ao mesmo tempo, retida em território nacional. Com efeito, a fuga de cérebros em busca de melhores condições de vida dificulta a retenção de profissionais qualificados em cibersegurança.

Assim, essa avaliação de política proposta pela CRE constitui importante e valioso instrumento para, a partir das análises a serem realizadas, retificar ou ratificar os planejamentos para a cibersegurança no País, sem desconectá-la da defesa cibernética. Reconhecemos que tais elementos podem indicar diferentes níveis de desenvolvimento da sociedade em termos de segurança cibernética, sendo essencial compreendermos como abordar essas questões para promovermos um ambiente digital mais seguro e resiliente.

## 2. REUNIÕES REALIZADAS

A Subcomissão Permanente de Defesa Cibernética (CREDC) realizou as seguintes reuniões:

- No dia 14/05/2024 ocorreu a 1ª Reunião de Subcomissão, com a eleição do Presidente (Senador Esperidião Amin), e demais integrantes: Senador Nelsinho Trad, Senador Fernando Dueire e o presidente como titulares, e Senador Sergio Moro, Senador Astronauta Marcos Pontes e Senador Chico Rodrigues como suplentes.

- No dia 21/05/2024 ocorreu a 2ª Reunião de Subcomissão, quando ocorreu a apreciação do plano de trabalho apresentado por esse Relator para a presente avaliação de política pública.

- No dia 18/06/2024 foi realizada a 3ª Reunião de Subcomissão, às 15h, com a realização de audiência pública para debater os seguintes temas: I – Política Nacional de Cibersegurança: Estratégia Nacional de Segurança Cibernética e Plano Nacional de Cibersegurança; II – Relações entre Segurança e Defesa Cibernética; e III – Anteprojeto de lei sobre Política Nacional de Cibersegurança (PNCiber) e o Sistema Nacional de Cibersegurança (SNCiber). Foram convidados o Senhor Marcos Antonio Amaro dos Santos, Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência (GSI), e o Senhor André Luiz Bandeira Molina, Secretário de Segurança da Informação Cibernética.

Na oportunidade, foi ouvido o Exmo. Sr. Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República, Marcos Antonio Amaro dos Santos.

O Sr. Marcos Antonio Amaro dos Santos começou sua exposição explanando sobre a estrutura organizacional do GSI; depois sobre a segurança da informação e cibersegurança de maneira geral no Brasil; fez uma síntese da Política Nacional de Cibersegurança (PNCiber), seus princípios e objetivos, os instrumentos da PNCiber e o Comitê Nacional de

Cibersegurança; trouxe alguns fatos e dados relacionados a esta temática; e apresentou algumas perspectivas antes de concluir.

Então, quanto à estrutura organizacional do Gabinete de Segurança Institucional da Presidência da República (GSI), destacou duas secretarias: a Secretaria de Acompanhamento e Gestão de Assuntos Estratégicos (Sagae) e a Secretaria de Segurança da Informação e Cibernética (Ssic).

Em relação à Sagae, ressaltou o Departamento de Assuntos do Conselho de Defesa Nacional e o Departamento de Assuntos da Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo (Dacreden). Em relação ao primeiro, sua importância à temática é a Coordenação-Geral de Apoio ao CDN - Conselho de Defesa Nacional; e a segunda, por ter a Coordenação-Geral de Segurança de Infraestruturas Críticas, que também trata de segurança cibernética.

Já a Secretaria de Segurança da Informação e Cibernética, há dois departamentos pertinentes: o Departamento de Segurança da Informação, com duas coordenações gerais - Coordenação-Geral do Núcleo de Segurança e Credenciamento e Coordenação-Geral de Gestão de Segurança da Informação; e o Departamento de Segurança Cibernética, com duas coordenações gerais.

O Ministro destacou a distinção que existe entre ciberdefesa - ou defesa cibernética - e cibersegurança - ou segurança cibernética. A segurança cibernética tem uma amplitude, tem um escopo maior. No nível político da Presidência da República, há o GSI, que trata desta temática sob a perspectiva de governança e gestão desse sistem. Depois, o Ministério da

Defesa, com as Forças Armadas, em nível estratégico, tem o Comando de Defesa Cibernética, que é um comando conjunto que envolve as três Forças Armadas, no âmbito do Ministério da Defesa. Nos níveis operacional e tático, há os comandos subordinados que podem ser estabelecidos, num caso do emprego de um comando conjunto. Há, assim, o nível operacional, em guerra cibernética, e o nível tático, em menor escalão, que é uma força conjunta de guerra cibernética.

Sobre o breve histórico da segurança da informação e cibersegurança no Brasil, o Ministro destacou a criação do Comitê Gestor da Internet do Brasil (Csirt) em 1995 e aperfeiçoado em 2003 (Decreto nº 4.829/2003); do Centro de Atendimento a Incidentes de Segurança (Cais) em 1997; do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br); a primeira política de segurança da informação na administração pública federal, já no GSI, por meio do Decreto nº 3.505/2000 (Revogado pelo Decreto nº 9.637/2018); o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, em 2004 (Ctir Gov); o Estatuto NIC.br (Núcleo de Informação e Coordenação do Ponto BR) em 2005; a Lei de Acesso à Informação em 2011; o Núcleo de Segurança e Credenciamento (Decreto nº 7.845, de 14 de novembro de 2012); o Marco Civil da Internet (Lei nº 12.965, de 2014); a Política Nacional de Segurança da Informação (Decreto nº 9.637/ 2018); a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 2018); a competência do GSI em matéria de segurança cibernética (Lei nº 13.844, de 2019); a primeira Estratégia Nacional de Segurança Cibernética, Decreto nº 10.222/2020; a Rede Federal de Gestão de Incidentes Cibernéticos (Regic), Decreto nº 10.748, de 2021; o Centro Integrado de Segurança Cibernética - Cisc (Portaria SGD/MGI nº 852, de 28 de março de 2023); e a Política Nacional

de Cibersegurança, pelo Decreto 11.856/2023. A Lei 14.600/2023, última lei de organização da Presidência da República e Ministérios, estabelece a Secretaria de Segurança da Informação e Cibernética, que antes era um departamento.

Posteriormente, o Ministro teceu um resumo sobre a defesa cibernética, a fim de distingui-la da segurança cibernética. Sobre a Política Nacional de Cibersegurança, que é o objeto desse relatório, o Ministro defende o Decreto de 26 de dezembro de 2023, pois não havia política dando essa orientação geral para os esforços na temática de cibersegurança, somente a Estratégica, que está em processo de revisão.

Dentre os princípios, a soberania nacional e a priorização dos interesses nacionais; a garantia dos direitos fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação; a prevenção de incidentes e de ataques cibernéticos, em particular aqueles dirigidos a infraestruturas críticas nacionais e serviços essenciais prestados à sociedade; a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos; a educação e o desenvolvimento tecnológico em segurança cibernética; a cooperação entre órgãos e entidades públicas e privadas em matéria de segurança cibernética e a cooperação técnica internacional na área de segurança cibernética.

Quanto aos objetivos da Política, estão o de promover o desenvolvimento de produtos, serviços e tecnologias de caráter nacional destinados à segurança cibernética; garantir a confidencialidade, integridade, autenticidade e disponibilidade das soluções e dos dados utilizados para o processamento, o armazenamento e a transmissão eletrônica ou digital de

informações; fortalecer a atuação diligente nos ciberespaços, especialmente das crianças, dos adolescentes e dos idosos; contribuir para o combate aos crimes cibernéticos e às demais ações maliciosas nos ciberespaços; estimular a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, incidentes e ataques cibernéticos e seus impactos; incrementar a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos; desenvolver a educação e a capacitação técnico-profissional em segurança cibernética na sociedade; fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança cibernética; incrementar a atuação coordenada e o intercâmbio de informações de segurança cibernética entre União, Estados, Distrito Federal e municípios, os Poderes Executivo, Legislativo e Judiciário, o setor privado e a sociedade em geral; desenvolver mecanismos de regulação, fiscalização e controle destinados a aprimorar a segurança e a resiliência cibernéticas nacionais; implementar estratégias de colaboração para desenvolver a cooperação internacional em segurança cibernética.

Foi destacado o objetivo de desenvolver mecanismos de regulação, fiscalização e controle do ambiente cibernético, que envolve a criação de um órgão que tenha essas atribuições. Isto poderia ser por meio de uma agência ou por meio de um centro; o que está sendo estudado pelo Comitê Nacional de Cibersegurança e será pelo formato de um projeto de lei.

Os instrumentos estabelecidos na política são a Estratégia Nacional de Segurança e o Plano Nacional de Cibersegurança. A estratégia pretende transformar os objetivos em medidas mensuráveis. Conforme

estudo do Banco Interamericano de Desenvolvimento (BID) sobre 17 países e mais de 30 estratégias nacionais, há uma evolução ao longo do tempo desse tipo de instrumento, das mais teóricas e acadêmicas para as operacionais, com objetivos, propósitos bem definidos e estabelecendo a necessidade de indicadores para acompanhar as políticas públicas na área da cibersegurança. Nesse sentido, já existe grupo de trabalho do CNCiber estudando a revisão da Estratégia Nacional de Cibersegurança brasileira, e, posteriormente, desdobrar num Plano Nacional de Cibersegurança.

O Comitê Nacional de Cibersegurança tem por finalidade justamente propor atualizações para o PNCiber, em relação a Estratégia Nacional de Cibersegurança, e elaborar o Plano Nacional de Cibersegurança; avaliar e propor medidas para incremento da segurança cibernética; formular proposta para o aperfeiçoamento da prevenção, detecção, análise e resposta às ameaças cibernéticas; propor medidas para o desenvolvimento da educação e segurança cibernética; promover interlocução com entes federativos; propor estratégias de colaboração para o desenvolvimento da cooperação técnica internacional; manifestar-se por solicitação do Presidente da Creden (Câmara de Relações Exteriores e Defesa Nacional) sobre assuntos relacionados à segurança cibernética.

A composição desse Comitê, com 25 integrantes, são os seguintes: o Gabinete de Segurança Institucional, a Controladoria-Geral da União, a Casa Civil, o Ministério do Desenvolvimento, Indústria, Comércio e Serviços; o Ministério da Fazenda, o Ministério da Defesa, o Ministério da Educação, o Ministério da Justiça e Segurança Pública, o Ministério das Comunicações, o Ministério da Ciência, Tecnologia e Inovação, o Ministério das Relações Exteriores, o Ministério de Minas e Energia, o Ministério da

Gestão e da Inovação em Serviços Públicos; o Comitê Gestor da Internet, a Anatel e o Banco Central; e mais nove integrantes, sendo três de entidades da sociedade civil, três de instituições científicas e tecnológicas de inovação e três de entidades do setor empresarial, todos, logicamente, relacionados à segurança cibernética.

Os três grupos de trabalho do Comitê em funcionamento, são para atualizar a Estratégia Nacional de Cibersegurança, coordenado pelo Comitê Gestor da Internet no Brasil; para definir os parâmetros de atuação internacional do Brasil em cibersegurança, sob coordenação do Ministério das Relações Exteriores; e um terceiro grupo, sobre governança, com a tarefa de elaboração da proposta de projeto de lei para a criação de um órgão para a governança da cibersegurança, possivelmente uma Agência Nacional de Cibersegurança ou um centro, e está a cargo do Ministério da Gestão e da Inovação em Serviços Públicos e da Anatel.

O Ministro acredita que regulações cibernéticas são consideradas um método eficaz para reduzir os riscos cibernéticos e cita pesquisas realizadas no Fórum Econômico Mundial, indagando se regulamentações cibernéticas e de privacidade reduzem efetivamente os riscos cibernéticos? De acordo comas as respostas obtidas, 39 % acreditam que sim, em 2022, e, em 2024, 60%, ou seja, tem aumentado a percepção de que uma agência ou um órgão regulador, controlador, fiscalizador, reduz os riscos cibernéticos.

O Senador Esperidião Amin indaga ser de fato o anteprojeto de lei está sendo retomado. O Ministro responde que o Comitê está analisando, mas sem dar prazo e seguiu: “A gente ouve dizer, Senador, que existe uma profusão de agências. Nós temos a Autoridade Nacional de Proteção de

Dados, recentemente criada a Autoridade Nacional de Segurança Nuclear, iremos propor um órgão de governança para a segurança cibernética... E não temos, também, um órgão de coordenação e governança de segurança de infraestruturas críticas. Então, talvez seja a oportunidade de juntarmos algumas dessas temáticas dentro de um mesmo órgão controlador e regulador".

E acrescenta, após pontuar que o Fórum Econômico Mundial estima em cerca de 14% do PIB dos países do mundo são consumidos pelos crimes cibernéticos, que, no Brasil: "Se as iniciativas relacionadas à criação de um órgão de governança, fiscalização e controle resultarem numa economia de 10% do que hoje ocorre, do que se perde, seriam R$150 bilhões. Lógico que não é uma matemática, é uma estimativa, talvez até grosseira, mas o volume de recursos que se perde com crimes cibernéticos, sem dúvida, é inimaginável".

- No dia 9/7/2024 ocorreu a 4ª Reunião, às 14h00, com audiência pública destinada a debater os riscos internacionais em segurança cibernética e a importância de uma agência nacional de segurança digital no Brasil. Foram convidados o Senhor Belisario Contreras, Diretor Sênior Representante de Venable Advocacia (LLP); Senhor Santiago Paz, Especialista Setorial em Segurança CibernéticaRepresentante de Banco Interamericano de Desenvolvimento (BID); Senhor Jorge Blanco, Diretor de Segurança da Informação (CISO) Representante de Google; Senhor Rafael Gonçalves, Executivo Representante de Trellix; Senhor Paulo Manzato, Chefe

da Área de Setor Público, Representante de Cloudfare; Senhora Patricia Soler, Líder no Colaborativo Conjunto de CiberDefesa Representante de CISA - Agência Americana de Cibersegurança e Infraestrutura.

A 4ª Reunião da Subcomissão Permanente de Defesa Cibernética contou com vários oradores e teve como objetivo debater os riscos internacionais em segurança cibernética e a importância de uma agência nacional de segurança digital no Brasil.

Os convidados foram os seguintes: Sr. Belisario Contreras, Diretor Sênior da Venable Advocacia, com mais de 120 anos de experiência; Sr. Santiago Paz, Especialista Setorial em Segurança Cibernética do Banco Interamericano de Desenvolvimento; Sr. Jorge Blanco, Diretor de Segurança e Informação do Google; Sr. Rafael Gonçalves, Executivo da Trellix; Sr. Paulo Manzato, Chefe da Área de Setor Público da Cloudflare; e a Sra. Patricia Soler, Líder do Colaborativo Conjunto de CiberDefesa da Cisa, Agência Americana de Cibersegurança e Infraestrutura.

Registramos, a seguir, os principais trechos de posicionamento desses palestrantes, que foram divididos em dois blocos, um com ênfase no tema "A importância de uma agência nacional de cibersegurança para o Brasil", e o segundo, com o tema "A importância da cooperação entre o poder público e o setor privado no combate aos crimes cibernéticos".

- Sr. Santiago Paz, Especialista Setorial em Segurança Cibernética do Banco Interamericano de Desenvolvimento:

"Você tem setores onde tem organizações de energia, tem o setor bancário, com os bancos, tem o mercado financeiro, saúde, instituições médicas, produtos químicos, água potável, todos os setores que trabalham, de forma diferente, que têm culturas diferentes e que respondem a reguladores diferentes, mas, ao mesmo tempo, todos os operadores, todas as organizações que trabalham, em cada um dos setores...

"Tem algumas organizações que são públicas - pode ser um hospital público, pode ser a Petrobras, pode ser o Banco Central -, mas tem também organizações privadas - você tem empresas privadas, bancos privados. Então, na hora de ter um incidente, a coordenação não é somente entre setores diferentes, não é somente entre o setor elétrico e o setor de infraestrutura digital, mas é também entre o setor público e o setor privado. Eles têm diferentes interesses, e é muito complexo fazer isso ao mesmo nível que a organização que está sendo afetada".

"Oitenta por cento das estratégias consideram que a parceria público-privada tem que ser feita, tem que ser levada em conta; sessenta por cento das estratégias mais modernas consideram também a promoção do setor local, da indústria de cibersegurança como uma indústria próspera em seus países".

"Também estamos fazendo outro estudo, que é um estudo de agências de segurança cibernética nacionais, agências nacionais de segurança cibernética dos países mais avançados, especialmente Europa, Espanha, França, Itália, Austrália e Estados Unidos, em que encontramos que o objetivo principal de todas as agências nacionais de cibersegurança é a coordenação, obviamente, mas a coordenação de quem? Do setor público, do setor privado e do de defesa".

- Senhor Jorge Blanco, Diretor de Segurança da Informação (CISO) Representante de Google.

O Senhor Jorge Blanco ressaltou que, à medida em que o Brasil continua a crescer em significância econômica e geopolítica, vai permanecer alvo para vários atores com diversas motivações. Esse cenário é uma arena complexa e em expansão, pela convergência de ameaças globais e locais.

O primeiro passo é estabelecer uma estratégia de cibersegurança e, mesmo assim, alguns intercorrências ou circunstâncias inesperadas podem surgir: atores que antes não eram ameaças, mudanças políticas globais, como temos agora com o nosso ambiente geopolítico, ou qualquer um dos eventos disruptivos. Dada essa realidade, as estratégias que sejam adaptáveis, flexíveis e responsivas são as mais efetivas.

Cada uma das agências criadas em outros Países têm diferentes responsabilidades, mas todas compartilham o objetivo de coordenar os esforços de cibersegurança nacionais e internacionais, criando mecanismos robustos para a colaboração privada e pública. Desenvolvem plano para emergência nacional e de resposta.

Uma das responsabilidades de uma agência de cibersegurança é investir em educação de cibersegurança, com caminhos formais e informais, durante a carreira do profissional. Isso impacta não somente na segurança nacional, mas também no setor privado, criando um sistema efetivo entorno da cibersegurança, que pode ter um impacto direto no PIB do país.

O estabelecimento de uma cibersegurança robusta é tarefa multifacetada, requer planejamento estratégico e colaboração em vários

setores. Uma entidade central coordenadora modelada em exemplos internacionais de sucesso ajuda a harmonizar o esforço, ajudando as colaborações privadas para emergências nacionais.

- Sr. Rafael Gonçalves, da Trellix

De acordo com o Senhor Rafael, a criação de uma agência voltada à cibersegurança, para coordenar e padronizar, é indispensável e urgente, afimando:

"Então, dentro de todas as dificuldades que a gente percebe na gestão pública, na gestão dos recursos financeiros, o principal entrave para se conseguir um arcabouço básico que permita aos gestores públicos conhecerem os incidentes e responderem a contento é justamente a falta de um ecossistema integrado, e isso joga a luz exatamente sobre grande parte dos pontos da proposta, em que a centralização e a padronização seriam funções vitais da agência. Isso, para não dizer também um ponto importante, que é a orientação ou o embasamento para que agências do setor público possam buscar parâmetros definitivos e diretos em como elas podem construir esse ambiente favorável para o monitoramento e defesa contra ataques cibernéticos".

Acrescenta que acreditar ser a agência também como catalisador da reformulação da própria carreira pública em torno da tecnologia da informação e da cibersegurança.

O Senador Sérgio Mora faz a seguinte indagação: "As agências nacionais que foram mencionadas têm, entre as suas tarefas, a de combater ameaças cibernéticas, tanto à defesa nacional como à infraestrutura crítica,

mas também crimes cibernéticos contra o setor público e o setor privado? É possível misturar todas essas tarefas numa única agência nacional? (...) como as entidades que os senhores representam, por exemplo, o próprio BID, o Google ou a Trellix, poderiam ajudar o Brasil na criação de uma agência nacional de segurança cibernética, com modelos, projetos, assessoria, e, talvez, especificamente ao BID, com financiamento? “

O Sr. Santiago Paz defende um centro integrado com a cibersegurança, cibercrime e ciberdefesa. Em geral, as agências nacionais são as instituições responsáveis pela coordenação entre os órgãos de law enforcement - a polícia, o Ministério Público, a Justiça, com ciberdefesa, no âmbito civil e com infraestruturas críticas.

Habitualmente, os órgãos centrais de coordenação de cibersegurança têm uma visão mais operativa e regulação mais direta. O *fusion center* (instituições que relacionam o público e o privado) produzem conhecimento e desenvolvem capacidades, mas não tem o poder de gerar a regulação, e não tem a capacidade de sancionar. Portanto, não é uma substituição do órgão central de coordenação de cibersegurança.

O Sr. Jorge Blanco, sobre uma agência única, menciona a Espanha, por exemplo, que instituiu duas agências diferentes. Uma lida com o setor público e com a inteligência e as ameaças militares. A outra cuida do setor privado, especialmente de empresas pequenas e médias e de cidadãos, mas ambas são coordenadas pelo Departamento de Segurança Nacional.

O Sr. Rafael Gonçalves, a respeito da criação da agência, considera que, num primeiro momento, figuraria muito importante, de

maneira a orientar e a regular o ciclo de vida da segurança de informação, para depois embasar um processo de resposta a incidentes.

Textualmente afirma: "Então, o papel da agência para lidar com o próprio volume de eventos precisaria ter um corpo muito, muito maior, mas, em termos de proposição mandatória do compartilhamento de dados, este eu acredito que já não seria exatamente o caminho para a agência, mas sim o de regulamentar, o de propor ações e até mesmo fiscalizar as empresas que não adotam a postura mínima, que não adotam a padronização, cuja criação seria vital".

- Sra. Patricia Soler, Líder no Colaborativo Conjunto de Ciberdefesa da CISA (Agência Americana de Cibersegurança e Infraestrutura), por videoconferência.

A Senhora Patrícia discorreu sobre parcerias público-privadas e o papel da CISA (Agência Americana de Cibersegurança e Infraestrutura) nos Estados Unidos.

Eles são responsáveis pela infraestrutura crítica nos Estados Unidos e, recentemente, foram beneficiados por um esclarecimento feito pela Casa Branca, em abril desse ano, especificando, em um memorando de segurança nacional sobre infraestrutura, segurança e resiliência críticas, que a Cisa lidera o Governo nesse assunto.

A Cisa tem pouco mais de cinco anos de idade, mas algumas das suas competências e programas já existiam antes da criação da agência. Ela está submetida ao Departamento de Segurança Interna, composta por

civis, não são agentes de segurança e não fazem parte do setor de inteligência ou de defesa.

A Cisa não só trata de cibersegurança, mas também de segurança de infraestrutura, possuindo dez escritórios regionais, que são responsáveis por entender as necessidades da região e das empresas locais de pequeno, médio ou grande porte.

Como avaliar o risco coletivo a que todos estamos sujeitos para não sempre estarmos atrasados, indaga Patrícia? A Cisa tem parcerias entre agências e especificamente com o Departamento de Defesa, são parte do DHS (Department of Homeland Security), Departamento de Justiça, NSA (National Security Agency) e FBI. Trabalham igualmente com parceiros interagências e parceiros internacionais.

Em relação a reportar ataques cibernéticos, afirmou que a recomendação é olhar várias formas diferentes de relatórios obrigatórios. Quanto tempo a empresa tem para relatar? Em alguns países, elas têm que ligar para o Governo em até quatro horas e têm 72 horas para enviar relatório escrito.

- Sr. Paulo Manzato, chefe da área de setor público da Cloudflare.

O Sr. Paulo Manzato considera que a a cooperação entre o poder público e o setor privado é essencial para enfrentar esses desafios de forma eficiente.

Seguem algumas opiniões:

"Os crimes cibernéticos, que incluem desde o roubo de dados pessoais até ataques de ransomware, espionagem digital, afetam não apenas a segurança nacional, mas também a estabilidade econômica e a privacidade individual. Os recursos e a expertise necessários para combater essas ameaças são vastos e diversificados, e nenhuma entidade isolada pode enfrentar esses desafios de maneira adequada".

"O setor privado, com suas inovações tecnológicas e rápida adaptação às mudanças no mundo digital, como foi mencionado anteriormente, desempenha um papel crucial na identificação e mitigação das ameaças cibernéticas. Empresas de tecnologia, como provedores de serviços de internet, desenvolvedores de softwares de segurança e firmas de consultoria em cibersegurança, possuem conhecimentos especializados e recursos avançados que são vitais na detecção precoce de ataques e na implementação de medidas preventivas".

"Por outro lado, o setor público possui a autoridade legal e os recursos necessários para coordenar esforços em uma escala nacional e internacional. Agências governamentais podem promulgar leis e regulamentos que incentivem práticas de segurança cibernética robustas, além de facilitar a troca de informações entre diferentes setores. Além disso, as forças de segurança e as agências de inteligência possuem a capacidade de conduzir investigações criminais e desmantelar redes de criminosos; neste caso, cibercriminosos".

"A colaboração entre esses dois setores permite a criação de um ecossistema de segurança resiliente. Programas de parceria público-privada, como a partilha de informações sobre as ameaças em tempo real e a realização de treinamentos conjuntos, podem melhorar significativamente a

capacidade de resposta a incidentes. Além disso, iniciativas conjuntas podem promover a conscientização sobre cibersegurança entre o público em geral e as pequenas empresas, que são muitas vezes alvos fáceis dos atacantes".

"Um último ponto é a educação e a capacitação, também como áreas de cooperação entre o poder público e o setor privado. São áreas em que a cooperação tem um impacto significativo. Programas de formação desenvolvidos conjuntamente podem equipar tanto os funcionários do setor público quanto os do privado, com habilidades e conhecimentos necessários para enfrentar os desafios cibernéticos. Workshops, seminários e cursos de cibersegurança podem ser realizados para disseminar as melhores práticas e mais recentes inovações de ciberdefesa".

- Sr. Belisario Contreras, da Venable

O Senhor Belisario discorre que na era digital a nossa dependência de nova tecnologia vem crescendo, e isso traz oportunidades, mas também risco. E estamos em uma encruzilhada de progresso e temos que tomar ações para salvar o nosso futuro digital.

Para o Brasil, as implicações são profundas. O país é um dos principais alvos de ciberataques e foi responsável por 42% de todos os incidentes na América Latina na primeira metade de 2023. De acordo estimativas, o mercado de cibersegurança no Brasil foi avaliado em 8,3 bilhões em 2023 e vai chegar a 20 bilhões em 2028.

A segurança não é só uma questão de segurança corporativa ou individual, mas uma responsabilidade coletiva que exige unidade e colaboração. A falta de educação do usuário e a configuração errada das

tecnologias deixam lacunas significativas que permitem os criminosos explorarem.

A abordagem no Brasil é fragmentada e as responsabilidades são de diversas agências. Esse sistema desagregado cria confusão e impede a habilidade de responder às ciberameaças de forma eficiente. É preciso de uma entidade centralizada para dar uma direção, acelerar a execução da estratégia nacional de cibersegurança, além da coordenação e supervisão para garantir que os esforços sejam unificados e eficientes.

Essa agência também liderará iniciativas de educação e promoverá carreiras, construindo um pipeline de talento bem robusto. Além disso, uma agência nacional de segurança digital seria elevada ao mais alto nível de governo, fornecendo a direção necessária para coordenar ações e monitorar a implementação da estratégia nacional. Ela agiria como uma autoridade competente para definir, esclarecer papéis, responsabilidades, processos e atividades necessárias para implementar a estratégia e outras ações relacionadas à ciber-resiliência.

A agência também identificaria stakeholders, estabeleceria alvos de performance e criaria planos de ação para cumprir com os objetivos de cibersegurança do país. Além disso, uma agência coordenaria a colaboração intergovernamental em ciberiniciativas, garantindo que todos os esforços sejam alinhados e mutuamente reforçados. Isso inclui trabalho com parceiros internacionais para compartilhar práticas, melhorar o compartilhamento de informações e fortalecer as capacidades de ciberdefesa.

- 5ª Reunião da Subcomissão Permanente de Defesa Cibernética, com objetivo de debater as relações entre segurança e defesa cibernética

A 5ª Reunião da Subcomissão Permanente de Defesa Cibernética, para debater as relações entre segurança e defesa cibernética, recebeu como convidado o Exmo. Sr. General de Divisão Alan Denilson Lima Costa, Comandante de Defesa Cibernética do Exército Brasileiro.

O Comando é composto pelo Centro de Coordenação de Operações Cibernéticas, o Centro de Gestão Estratégica, o Centro de Defesa Cibernética e a Escola Nacional de Defesa Cibernética.

Seguem alguns posicionamentos do Comandante:

"(...) o nosso Comando de Defesa Cibernética é o responsável por conduzir o setor cibernético no âmbito da defesa, e isso nasce na nossa Estratégia Nacional de Defesa, que é a de 2008. Então, um detalhe interessante é que o Brasil percebe muito cedo a ameaça cibernética como uma ameaça à segurança nacional e cria um setor estratégico próprio a ser desenvolvido para se contrapor a essa ameaça percebida. Então, nós já tínhamos dois setores clássicos: o setor nuclear, que já vinha sendo conduzido pela nossa Marinha do Brasil; o setor espacial, conduzido pela Força Aérea, e surge um setor novo, o setor cibernético, que, nessa época, em dezembro de 2008, ainda era bastante desconhecido".

"O nosso comando nasce somente em 2016, então nós temos oito anos como Comando de Defesa Cibernética. A estrutura se tornou mais

robusta e nós, a partir daí, começamos a intensificar a cooperação internacional nessa área"

"A computação quântica vai suplantar qualquer sistema criptográfico, o mais atual que seja. E hoje isso já está sendo tratado em publicações. Hoje ataques estão sendo feitos, e essas informações estão sendo guardadas, essas que estão criptografadas, para que, quando a computação quântica estiver disponível, esses dados classificados, sigilosos, possam ser descriptografados".

"E o nosso Comando de Defesa Cibernética é o encarregado de conduzir esse setor no âmbito da defesa. Então nós somos um comando operacional conjunto, permanentemente ativado e com capacidade interagências".

"Então, em nível político, a segurança cibernética é atribuição do GSI. Ele faz a coordenação, normatiza, em âmbito nacional, a segurança cibernética. E o Comando de Defesa Cibernética atua no nível estratégico, implantando esse sistema no âmbito das Forças, no âmbito da defesa; atua como um comando operacional permanentemente ativado; e entrega capacidades para o nível tático".

A missão é "desenvolver e aplicar capacidades militares - é a nossa essência. Mas também nós colaboramos com o GSI nos assuntos relacionados à segurança de infraestruturas críticas de interesse da Defesa Nacional".

"Um outro ponto importante nessa relação nossa com o GSI, especificamente com o Centro de Prevenção, Tratamento e Resposta a

Incidentes Cibernéticos de Governo, é a nossa Rede Federal de Gestão de Incidentes Cibernéticos. Então, o Comando de Defesa Cibernética é o coordenador da nossa setorial de defesa. Nós temos diversas equipes de tratamento de incidentes de rede no nosso sistema que nós coordenamos, nós somos a cabeça do sistema. Mas não é só essa coordenação, a gente provê recursos para a montagem da infraestrutura dessas equipes, nós proporcionamos treinamento para os especialistas dessas equipes e exercícios também de adestramento dessas equipes de tratamento de incidentes. Então, nós podemos dizer que temos uma setorial, realmente, que funciona e que os incidentes cibernéticos que acontecem na nossa estrutura são tratados e são reportados ao GSI por intermédio do nosso Centro de Tratamento de Incidentes de Redes do Governo".

"A diplomacia militar é um instrumento das relações internacionais do país. Nesse sentido, nós estamos participando de diversos fóruns internacionalmente. O primeiro deles é esse fórum dos comandantes cibernéticos, que reúne comandantes de cinco continentes. São 46 comandantes cibernéticos de diversos países que se reúnem para a troca de informações, atualidades, sobre como eles estão implementando a defesa cibernética nos seus países".

"Outra atividade que materializa essa cooperação com a segurança cibernética é o nosso exercício, o Guardião Cibernético, que nós fizemos agora, de 14 a 18 de outubro. Nós já estamos com todos os setores das infraestruturas críticas participando efetivamente do nosso exercício. (...) começamos em 2018 com 23 organizações. Este ano, (...) passamos de 140 organizações, passamos de 600 pessoas participantes do exercício. E levamos esse exercício para a Escola Superior de Defesa, com instalações

muito apropriadas para receber não só um efetivo desse tipo, mas para conduzir um exercício dessa magnitude, que é o Guardião Cibernético".

"(...) é um momento também de treinarmos a crise, com os atores que estariam presentes, para solucionar esse problema. Isso tudo está dentro do Guardião Cibernético. A gente trabalha no nível das organizações, daquele pequeno gabinete de crise das organizações, trabalhamos no nível técnico e trabalhamos também, no nível político, a resposta a uma crise no espaço cibernético".

## 3. A POLÍTICA NACIONAL DE CIBERSEGURANÇA (PNCIBER) E O POSICIONAMENTO DO GSI CIBERSEGURANÇA

A Política Nacional de Cibersegurança foi instituída pelo Decreto nº 11.856, de 26 de dezembro de 2023, porém, a ideia original não era essa. Houve, meses antes, o debate sobre anteprojeto do Poder Executivo que pretendia instituir **por lei** a Política Nacional de Cibersegurança, o Sistema Nacional de Cibersegurança e a agência que regularia as atividades de cibersegurança no País.

Esse anteprojeto foi submetido a audiência pública, na manhã do dia 16 de maio de 2023, atendendo a convite do Ministro Marcos Antônio Amaro, do Gabinete Institucional da Presidência da República (GSI), que aconteceu no auditório do Anexo I do Palácio do Planalto. Segundo o plano original, as manifestações e sugestões feitas na oportunidade seriam sistematizadas e até o mês de agosto de 2023 a proposição deveria ser enviada ao Parlamento para análise.

De acordo com a exposição de motivos desse anteprojeto, a Política Nacional pretendida seria:

> "uma proposta voltada a unificar a "colcha de retalhos" regulatória existente no país, minimizar o crescente número de incidentes que acometem o país, gerando enormes prejuízos para a sociedade brasileira, buscar diminuir o débito tecnológico nacional no setor, e ampliar a participação brasileira na cooperação internacional sobre a temática"

O modelo proposto segue, em termos gerais, a Diretiva NIS2 do Parlamento Europeu (igualmente foram considerados o documento pertinente da União Internacional de Telecomunicações - UIT/ONU; o Modelo de Maturidade da Universidade de Oxford, adotado pela OEA; o relatório do TCU de 2022 sobre a Lista de Alto Risco na Administração Pública; as recomendações do Senado Federal; o relatório da CPI da Espionagem Cibernética de 2014; a avaliação de política pública da CRE, de 2019; e proposições legislativas de ambas as casas do Congresso Nacional), com existência de um órgão central nacional, que seria a Agência Nacional de Cibersegurança, de um "ente" fiscalizador, no caso vinculado ao Gabinete de Segurança Institucional, o Comitê Nacional de Cibersegurança e um Gabinete de Gerenciamento de Cibercrises.

Outro ponto importante foi o objeto prioritário dessa política, que deixa de ser focado em infraestruturas críticas identificadas, para se dedicar a transversalidade da cibersegurança, com foco em serviços essenciais para o bom funcionamento da sociedade. Setores como fornecimento de água urbana; barragens; biossegurança; radiodifusão; serviços postais; telecomunicações; defesa; eletricidade; óleo e gás; financeiro; bem como transporte aéreo, aquaviário e terrestre são considerados como infraestruturas críticas, mas isso não abrangem vários outros, como justiça, saúde, educação, por exemplo. Incluir esses novos setores como infraestruturas críticas não solucionaria, pois sempre aparecerá outro. Portanto, o conceito de serviços essenciais é mais adequado.

Esse anteprojeto foi versado em 44 artigos, disposto do seguinte modo: Capítulo I - Da Política Nacional de Cibersegurança [Seção I - Disposições Gerais (Arts. 1º - 4º), Seção II - Dos Princípios (Art. 5º), Seção III Dos Objetivos (Art. 6 º), Seção IV - Das Diretrizes (Arts. 7 º - 9º), Seção V - Dos Instrumentos (Art. 10)]; Capítulo II - Do Sistema Nacional de Cibersegurança (Arts. 11-12) [Seção I - Do Comitê Nacional de Cibersegurança (Arts. 13 – 16), Seção II - Da Agência Nacional de Cibersegurança (Arts. 17-19), Seção III - Do Gabinete de Gerenciamento de Cibercrises (Art. 20-25)]; Capítulo III - Da Estratégia Nacional de Cibersegurança (Arts. 26-27); Capítulo IV - Do Plano Nacional de Cibersegurança (Arts. 28-29); Capítulo V - Da Cooperação Internacional (Art. 30); Capítulo VI - Do Ensino, Pesquisa, Desenvolvimento e Inovação Tecnológica em Cibersegurança (Arts. 31-36); Capítulo VII - Disposições Finais e Transitórias (Art. 37-44).

Do ponto de vista de construção legislativa, havia desequilíbrio no texto do anteprojeto. Tinha capítulo com dez artigos (capítulo I) e outro com um artigo (capítulo V), além de ter capítulo dividido em seções que inicia com dois artigos "soltos" antes da Seção I, no caso o Capítulo II, o que deveria compor outra Seção, a de Disposições Gerais, tal qual o feito no Capítulo I.

Além disso, o texto se encerra com a imprópria norma de revogação genérica: *Art. 44. Revogam-se todas as disposições em contrário ao disposto nesta Lei*. De acordo com o Art. 9º da Lei Complementar nº 95, de 1998, a cláusula de revogação deverá enumerar, expressamente, as leis ou disposições legais revogadas.

Sobre o conteúdo do anteprojeto, o Art. 4º traz conceituações chaves, dentre as quais a da própria cibersegurança, no seu inciso XIV, que seria o conjunto de ações voltadas à confidencialidade, integridade, autenticidade e disponibilidade de ciberativos. Sugerimos incluir a proteção às pessoas no conceito.

Por ciberativo, o inc. I do mesmo artigo conceitua como envolvendo *hardware, software ou dados utilizados para o processamento e transmissão eletrônicos de informações*.

Com o objetivo de completar o conceito jurídico de ciberativo, abrangendo outros ativos não contemplados anteriormente e colocando as pessoas como foco central, sugerimos o seguinte:

> Art. 4º
>
> I - ciberativo (ou ativo cibernético): hardware, software, dados, conjunto de dados, códigos, sistemas de computação, redes de computadores ou informações utilizadas para o processamento ou transmissão eletrônicos de informações;

Igualmente o conceito de ciberexploração merecia reparos:

| Atual | Proposto |
|---|---|
| XII - ciberexploração (ou exploração cibernética): conjunto de atividades voltadas ao robustecimento da consciência situacional, à produção de | XII - ciberexploração (ou exploração cibernética): conjunto de atividades voltadas ao robustecimento da consciência situacional, à produção de |

| | |
|---|---|
| conhecimento de inteligência de fonte cibernética e ao levantamento de vulnerabilidades, que utiliza técnicas, táticas e procedimentos semelhantes àqueles empregados nos ciberataques, diferindo deles principalmente por não buscar a produção de ciberefeitos; | conhecimento de inteligência de fonte cibernética e **de ameaças cibernéticas** e ao levantamento de vulnerabilidades, que utiliza técnicas, táticas e procedimentos semelhantes àqueles empregados nos ciberataques, diferindo deles principalmente por não buscar a produção de ciberefeitos; |

As tecnologias de ciberexploração, em especial *Threat Intelligence* e *Open Source Intelligence* (OSINT) fornecem conhecimento, informações e dados sobre ameaças de segurança cibernética e outras exposições específicas de ameaças. O resultado dessa exploração tem como objetivo fornecer ou auxiliar na curadoria de informações sobre as identidades, motivações, características e métodos de ciberameaças, comumente referidos como táticas, técnicas e procedimentos. Assim, a adição do termo "produção de conhecimento de inteligência de fonte cibernética e de ameaças cibernéticas", adequa-se melhor a esta possibilidade.

Os artigos 11 e 12 definem o Sistema Nacional de Cibersegurança, com o objetivo de envolver todos os poderes da União, dos Estados, do Distrito Federal e dos Municípios, além dos Tribunais de Contas e dos Ministérios Públicos, bem assim do setor privado, das instituições de ensino e pesquisa, e dos demais agentes da sociedade. Esse sistema é composto do Comitê Nacional de Cibersegurança (CNCiber), da Agência

Nacional de Cibersegurança, do Gabinete de Gerenciamento de Cibercrises e do Complexo Nacional de Cibersegurança.

O Comitê Nacional de Cibersegurança é órgão de assessoramento do Presidente da República sobre cibersegurança, integrado por representantes da sociedade, do setor público, do setor privado e da academia. Dentre outras funções, cabe a ele aprovar a Estratégia Nacional de Cibersegurança, o Plano Nacional de Cibersegurança e o Complexo Nacional de Cibersegurança (composto pelo conjunto de ciberativos que dão sustentação a serviços essenciais). O Gabinete de Gerenciamento de Cibercrises é órgão de assessoramento ao Presidente da República, tal qual o Comitê, mas dedicado especificamente na gestão de cibercrises.

Notamos que, na composição do Comitê, ao contrário do preconizado do anteprojeto como um todo, estão três representantes de entidades representativas das infraestruturas críticas (Art. 15, inciso XVI). O conceito de "infraestrutura crítica" foi suprimido pelo de "serviços essenciais" em todo o anteprojeto. Prudente seria adequar igualmente para a composição do Comitê, com "três representantes de entidades representativas dos serviços essenciais". Além disso, notamos a ausência de representante da Polícia Federal como membro do Comitê e do Gabinete de Cibercrises.

Igualmente, se o anteprojeto pretendia eliminar a fragmentação e sobreposição regulatória, a exemplo dos Decretos nº 9.637/2018 (Institui a Política Nacional de Segurança da Informação), o nº 10.569/2020 (Estratégia Nacional de Segurança de Infraestruturas Críticas), e a Res. CNJ 396/2021 (Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário), seria importante incluir todas as agências regulatórias no Comitê,

pois muitas delas também possui preocupação com a segurança cibernética (Anatel, Anac, Aneel...).

A Agência Nacional de Cibersegurança seria autarquia sob regime especial, com autonomia administrativa e financeira e patrimônio próprio, vinculada ao Gabinete de Segurança Institucional da Presidência da República, com sede em Brasília.

Dentre as funções da Agência está, no Art.18, inc. VI, a de *desenvolver capacidades nacionais de prevenção, monitoramento, detecção, análise e resposta, para detectar e gerenciar ciberincidentes*. Defendemos que seria prudente alterar essa competência para *desenvolver e fomentar capacidades nacionais de prevenção, monitoramento, detecção, exploração, análise e resposta, para detectar e gerenciar ciberincidentes*.

Por fim, quanto ao tema do ensino, pesquisa, desenvolvimento e inovação tecnológica, consideramos que o louvável objetivo dado ao Ministério da Educação, no Art. 32, de promover o ensino de cibersegurança na educação fundamental e média, pública e privada, com base I – nas boas práticas de cibersegurança; II - na ética no uso da internet; III - na utilização segura de aplicativos IV - no uso de redes sociais; e V - na proteção de dados; igualmente deveria fundar-se VI - na intimidade e na proteção da privacidade; VII - na proteção da criança e do adolescente na internet; e VIII - nos direitos fundamentais.

Contudo, esse projeto de lei jamais foi apresentado e, em seu lugar, foi editado o **Decreto nº 11.856, de 26 de dezembro de 2023**, que institui a Política Nacional de Cibersegurança (PNCiber), composta da

Estratégia Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança (CNCiber).

Esse Decreto possui quinze artigos, fixando **princípios** da Política Nacional da Cibersegurança, nomeadamente (i) a soberania nacional e a priorização dos interesses nacionais; ii) a garantia dos direitos fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação; iii) a prevenção de incidentes e de ataques cibernéticos, em particular aqueles dirigidos a infraestruturas críticas nacionais e a serviços essenciais prestados à sociedade; iv) a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos; v) a educação e o desenvolvimento tecnológico em segurança cibernética; vi) a cooperação entre órgãos e entidades, públicas e privadas, em matéria de segurança cibernética; e vii) a cooperação técnica internacional na área de segurança cibernética; e **objetivos**, a saber i) a promoção do desenvolvimento de produtos, serviços e tecnologias de caráter nacional destinados à segurança cibernética; ii) a garantia da confidencialidade, integridade, autenticidade e disponibilidade das soluções e dos dados utilizados para o processamento, o armazenamento e a transmissão eletrônica ou digital de informações; iii) o estímulo da adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, incidentes e ataques cibernéticos, e seus impactos; e iv) o incremento da atuação coordenada e o intercâmbio de informações de segurança cibernética entre entes da federação, poderes do Estado, setor privado e sociedade em geral.

Por sua vez, o CNCiber, nos termos do art. 5º, é instituído no âmbito da Câmara de Relações Exteriores e Defesa Nacional do Conselho de

Governo e tem por finalidade acompanhar a implementação e a evolução da PNCiber, com a competência de: i) propositura de atualizações para a PNCiber, a Estratégia Nacional de Cibersegurança e o Plano Nacional de Cibersegurança; ii) avaliação e propositura de medidas para incremento da segurança cibernética no País; iii) formulação de propostas para o aperfeiçoamento da prevenção, da detecção, da análise e da resposta a incidentes cibernéticos; iv) proposição de medidas para o desenvolvimento da educação em segurança cibernética; v) promoção da interlocução com os entes federativos e a sociedade em matéria de segurança cibernética; vi) proposição de estratégias de colaboração para o desenvolvimento da cooperação técnica internacional em segurança cibernética; e VII) e manifestação, por solicitação do Presidente da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, sobre assuntos relacionados à segurança cibernética.

A Secretaria-Executiva do CNCiber ficará a cargo do Gabinete de Segurança Institucional da Presidência da República.

Houve estranhamento duplo com a edição desse decreto. O primeiro, em razão de todos esperarem a submissão do anteprojeto de lei acima referido, em que seria criada uma agência reguladora, prevista para contar com 800 (oitocentos) servidores após 5 (cinco) anos de sua instalação pelo Poder Executivo. Desse modo, o decreto regula lei inexistente, lançando dúvidas até mesmo de sua possível contrariedade ao art. 48, XI, e ao art.84, VI, “a”, da Constituição Federal.

Segundo, que o Decreto revoga dois dispositivos do Decreto nº 9.637, de 26 de dezembro de 2018, que *institui a Política Nacional de Segurança da Informação,* extraindo a segurança cibernética da segurança

da informação, o que é um equívoco. Este Decreto tem por finalidade assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação). Similarmente, o Decreto nº 11.856/2023, que estabelece a Política Nacional de Cibersegurança, tem por um de seus objetivos garantir a confidencialidade, a integridade, a autenticidade e a disponibilidade das soluções e dos dados utilizados para o processamento, o armazenamento e a transmissão eletrônica ou digital de informações (art. 3º, II).

Se lermos atentamente o Decreto nº 9.637/2018, notamos que a segurança da informação abrange a segurança cibernética, a defesa cibernética, a segurança física e a proteção de dados organizacionais; e as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação (art. 2º).

O Decreto nº 11.856/2023, ao revogar o inc. I, do art. 2º, e o inc. I do art. 6º do Decreto nº 9.637/2018, exclui a segurança cibernética da Política Nacional de Segurança da Informação e da Estratégia Nacional de Segurança da Informação, o que carece de sentido lógico. Um dos princípios da Política Nacional de Segurança da Informação, não revogado, é revelador desse equívoco:

> "*articulação entre as ações de segurança cibernética, de defesa cibernética e de proteção de dados e ativos da informação"* (art. 3º, X, do Decreto nº 9.637/2018).

Além disso, a Estratégia Nacional de Segurança da Informação (Decreto nº 10.222/2020) é formada por esse conceito integrador e envolve a segurança cibernética, a defesa cibernética, a segurança das infraestruturas

críticas, a segurança da informação sigilosa e a proteção contra vazamento de dados. Essa estratégia, inclusive, é intitulada Estratégia Nacional de **Segurança Cibernética** (E-ciber).

A governança do setor, ao invés do prometido pelo anteprojeto de lei citado[1], de "unificar a 'colcha de retalhos' regulatória existente no país", ao invés de integrar, auxilia para desintegrar as relações da segurança da informação, segurança cibernética, defesa cibernética e proteção de dados pessoais

Conforme o anteprojeto, segurança da informação envolve as ações que objetivam assegurar a confidencialidade, a integridade, a autenticidade e a disponibilidade das informações; cibersegurança (ou segurança cibernética) é o conjunto de ações voltadas à confidencialidade, integridade, autenticidade e disponibilidade de ciberativos; e, ciberdefesa (ou defesa cibernética), as ações coordenadas pelo Ministério da Defesa com a finalidade de: a) assegurar a cibersegurança de ciberativos de interesse da defesa nacional; e b) buscar superioridade no domínio cibernético sobre os ciberativos do oponente.

Ademais, a Cibersegurança e a ciberdefesa no Brasil são estrutradas em nível **político** (segurança cibernética, aos cuidados da Presidência da República / GSI), **estratégico** (defesa cibernética, sob responsabilidade do Ministério da Defesa, Estado-Maior Conjunto das Forças Armadas e dos Comandos das Forças), **operacional** (guerra

[1] Minuta do projeto de lei que institui a Política Nacional de Cibersegurança (PNCiber) e o Sistema Nacional de Cibersegurança (SNCIber). Disponível em: <https://www.gov.br/gsi/pt-br/ssic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf> Acesso em; 23/02/2024.

cibernética, cuidada pelo comando operacional ativado) e **tático** (guerra cibernética, encarregado pela Força Conjunta de Guerra Cibernética ou um Destacamento Conjunto de Guerra Cibernética.).

Veja que são conceitos e estruturas necessariamente interligados e que merecem governança e regulação igualmente integradas, o que o Decreto nº 11.856/2023 não entregou.

Consciente dessa realidade, o próprio CNCiber, composto por integrantes do poder executivo federal, do Comitê Gestor da Internet, da sociedade civil, de instituições científicas e do setor empresarial, instituiu os seguintes grupos de trabalho para melhorar o sistema: GTT-1: Grupo de Trabalho Temático para atualização da Estratégia Nacional de Cibersegurança – e-Ciber; 2 - Grupo de Trabalho Temático para Elaboração de Proposta de Projeto de Lei para criação de Órgão para a Governança da Cibersegurança Nacional; 3 - Grupo de Trabalho Temático para Definição de Parâmetros de Atuação Internacional do Brasil em Cibersegurança.

## 4. AVALIAÇÃO DO TRIBUNAL DE CONTAS DA UNIÃO

O Tribunal de Contas da União (TCU), em Auditoria Operacional fiscalizando o Gabinete de Segurança Institucional da Presidência da República (GSI) e Casa Civil da Presidência da República (TC 010.387/2024-2), sob relatoria do Relator: Ministro Benjamin Zymler, avaliou em que medida a Política Nacional de Cibersegurança (PNCiber) está de acordo com as boas práticas, em especial comparada ao previsto no Referencial de Controle de Políticas Públicas do TCU. Em outros termos, a adequação do modelo da PNCiber para enfrentar a ameaça cibernética e os

riscos que essa ameaça representa para o país[2]., em especial ao fato de a "superfície de ataque" [3]brasileira estar em tendência de aumento e entre as mais vulneráveis do mundo e não possuirmos organização eficaz e devidamente organizada para fazer frente a essas ameaças.

Para tanto, essa auditoria definiu quatro questões chaves, nomeadamente:

> Questão 1: Em que medida são necessárias as proteções cibernéticas ao ambiente digital sob a governabilidade do Brasil?
>
> Questão 2: Em que medida as ações previstas na PNSI, relativas à segurança cibernética, executadas entre dez/2018 e dez/2023 (entre a publicação da PNSI e da PNCiber) contribuíram para tornar seguro o ambiente digital sob a governabilidade do Brasil?
>
> Questão 3: Em que medida a Política Nacional de Cibersegurança (PNCiber) foi formulada segundo as boas práticas, em especial comparada ao previsto no Referencial de Controle de Políticas Públicas do TCU?

---

[2] Conexos a essa avaliação estão os processos TC 001.873/2020-2 (Rel. Min. Vital do Rêgo), que consistiu em levantamento da governança e gestão de segurança da informação (SegInfo) e de segurança cibernética (SegCiber) na Administração Pública Federal (APF); e TC 010.390/2024-3 (Rel. Min. Augusto Nardes), sobre controles de Segurança da Informação nas organizações do SISP (avaliação via SGD: Auditoria - Tema Segurança da informação e segurança cibernética - LAR 2023- 2024).

[3] A superfície de ataque é o conjunto de ativos, serviços, sistemas e ambientes por onde um invasor pode tentar entrar, causar um efeito ou extrair dados, correspondendo à superfície que está exposta ao risco da ameaça cibernética.

Questão 4: A quais riscos o país está submetido ao não se alcançar os objetivos de segurança cibernética estabelecidos pelo Estado brasileiro?

Conforme ressalta a auditoria, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) exerce a coordenação e supervisão da atividade de segurança cibernética no âmbito da administração pública federal, mas o Brasil ainda não possui uma autoridade central e nem norma federal que discipline a matéria para além do Poder Executivo Federal. Isto demonstra a falta de priorização do tema da segurança cibernética no Estado brasileiro.

Diante esse quadro, há sucesso dos ataques contra organizações e cidadãos brasileiros, gerando *danos em diversas dimensões por perda da confidencialidade, integridade e disponibilidade de informações e sistemas (e.g., fraudes contra cidadãos, paralisação de serviços prestados à sociedade, prejuízos à imagem das organizações públicas e privadas, perdas financeiras), o que impacta negativamente a soberania digital, a confiança no ambiente digital e a aceleração da transformação digital no país*.

Dentre os ataques mais comuns estão o ransomware (tipo de malware para sequestrar dados de um sistema ou dispositivo, criptografando-os e exigindo um resgate para descriptografar e restaurar o acesso aos dados) e phishing (engenharia social que induz a vítima a compartilhar informações ou realizar alguma ação capaz de permitir acesso às suas contas, ao seu computador ou à sua rede).

Urge buscar a soberania digital, capacitando o País para controlar e proteger suas infraestruturas críticas, redes eletrônicas, bancos de

dados e infraestruturas políticas que facultam a própria governança. Em sentido preocupante, o que ser nota são os frequentes ataques cibernéticos contra tribunais, empresas, ministérios e unidades administrativas, causando enorme prejuízo financeiro e prejudicando a eficiência do serviço público. O sistema ideal demanda investimento, como a criação de agência nacional de segurança cibernética, mas seguramente esse investimento rapidamente se pagaria se fosse contabilizado os prejuízos sofridos pelos ataques.

Como exemplo de fragilidade, o TCU aponta que os órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp) não implementam a contento o conjunto básico de medidas de segurança cibernética e não há organização que consolide dados para o restante do setor público e para o setor privado.

Já sobre os efeitos do Decreto 11.856/2023 (PNCiber), o TCU aponta dois fatores impeditivos de orientação da segurança cibernética no País: o caráter preparatório da atual PNCiber e limitações na origem da política pública. Assim, de um lado, CNCiber não possui a competência de coordenação e execução de uma política pública, mais semelhante a um grupo de trabalho que órgão operacional. Portanto, o CNCiber seria "preparatório" para marco legal futuro. De outro lado, a política pública no setor falta alcance nacional e carece de estrutura de execução.

A PNCiber, instituída por decreto, é limitada ao Poder Executivo Federal, sem a capilaridade necessária para enfrentar a ameaça cibernética, que é multidimensional, multissetorial e transnacional, em especial diante os seguintes riscos: *baixa competitividade do país em produtos, serviços e tecnologia de Segurança Cibernética; usuários mais vulneráveis, em especial crianças, adolescentes e idosos, por não estarem*

*conscientizados adequadamente sobre ataques cibernéticos; baixa resiliência das organizações públicas e privadas, aumentando as chances de sucesso e a magnitude dos impactos decorrentes de ataques de ransomware e outros incidentes de segurança; estagnação na inovação e fuga de talentos; ausência de orientação às instituições de ensino para alinharem suas atividades às demandas nacionais sobre segurança cibernética; e ausência de orçamento nacional dedicado à segurança cibernética.*

Assim, se o problema afeta todos os níveis do setor público, setor privado e sociedade civil, necessariamente a política pública que busca enfrentá-la – PNCiber – deve ser intergovernamental e coordenada. Isto somente seria atingido por lei federal, capaz de estruturar coordenação nacional, com cargos e funções. De acordo com o TCU o anteprojeto de lei proposto para uma PNCiber sim tinha essa característica de coordenação nacional, ao propor : I - o Sistema Nacional de Cibersegurança; II - a Estratégia Nacional de Cibersegurança III - o Plano Nacional de Cibersegurança IV - a cooperação internacional; e V - o ensino, a pesquisa, o desenvolvimento e a inovação tecnológica em cibersegurança.

A ausência Sistema Nacional de Cibersegurança no Decreto 11.856/2023, até por suas limitações normativas, frusta a expectativa da boa prática, pois esse Sestama contaria com: I - Comitê Nacional de Cibersegurança; II - Agência Nacional de Cibersegurança; III - Gabinete de Gerenciamento de Cibercrises; e IV - Complexo Nacional de Cibersegurança. E, apesar de o Decreto 11.856/2023 propor a Estratégia Nacional de Cibersegurança e Plano Nacional de Cibersegurança, por não ser lei, não mereceriam ser adjetivadas como “nacionais.

Se, no anteprojeto de lei, a Agência Nacional de Cibersegurança exerceria o papel de órgão executor da política pública, o Decreto 11.856/2023 não propõe nada similar. Conforme o TCU, a *estrutura em questão deve possuir autoridade e prerrogativas também em sua função de liderança, quando atuar de forma a coordenar esforços descentralizados, visto que precisará cooperar com atores relevantes (p. ex.: agências reguladoras de setores críticos e agências internacionais) em ações que envolvam compartilhamento de dados, inteligência e infraestrutura*.

A conclusão é que não há priorização governamental. A Agência, de início, iria precisar de criação de 687 cargos e um orçamento anual de cerca de R$ 540 milhões. Em contraste, o orçamento para implementar as ações de segurança cibernética em 2023, no âmbito da Política Nacional de Segurança da Informação não alcançou R$ 600 mil.

Sobre as respostas as questões propostas, são as seguintes:

Questão 1: Em que medida são necessárias as proteções cibernéticas ao ambiente digital sob a governabilidade do Brasil? Resposta: São necessárias proteções cibernéticas em nível de política pública nacional, a partir da avaliação de risco pelo Estado brasileiro, uma vez que a ameaça cibernética é relevante para o Brasil e apresenta uma tendência de agravamento no cenário nacional.

Questão 2: Em que medida as ações previstas na PNSI selecionadas, relativas à segurança cibernética, executadas entre dez/2018 e dez/2023 (entre a publicação da PNSI e da PNCiber) contribuíram para tornar seguro o ambiente digital sob a governabilidade do Brasil? Resposta: As ações previstas na PNSI foram parcialmente executadas pelo GSI/PR

durante o período de dez/2018 e dez/2023 (entre a publicação da PNSI e da PNCiber), e as limitações decorrentes do modelo federal (e não nacional) da PNSI comprometeram a eficácia de tais ações no sentido de alcançar os objetivos da PNSI, o que pode levar à insegurança do ambiente digital sob a governabilidade do Brasil. (art. 4º, Decreto 9.637/2018).

Questão 3: Em que medida a Política Nacional de Cibersegurança (PNCiber) foi formulada segundo as boas práticas, em especial comparada ao previsto no Referencial de Controle de Políticas Públicas do TCU? Resposta: O estágio de formulação (Blocos I, II e III do RCPP), momento no qual problemas e intervenções públicos são analisados e selecionados para compor a agenda pública e o portfólio de ações governamentais, da PNCiber está razoavelmente alinhado às boas práticas, sendo a principal falha a incoerência do modelo adotado com o problema identificado, o que não contribui, de forma suficiente, para alcance dos seus objetivos (art. 3º, Decreto 11.856/2023). Ressalta-se que a equipe de auditoria entende que a PNCiber se demonstra como um ato preparatório para, possivelmente, um marco regulatório que virá e que endereçará o problema de forma nacional, após conclusões dos trabalhos do GTT-2.

Questão 4: A quais riscos o país está submetido ao não se alcançar os objetivos de segurança cibernética estabelecidos pelo Estado brasileiro? Resposta: Caso os objetivos da PNCiber não sejam alcançados e, consequentemente, sejam materializados os riscos e consequências expostos, o Brasil pode perder o poder e o controle sobre infraestruturas e dados digitais, impactando negativamente na soberania digital (consequentemente, na soberania nacional), na confiança no ambiente digital e na aceleração da transformação digital do país.

O TCU, desse modo, conclui pela necessidade de lei federal, de iniciativa privativa da Presidência da República, com conteúdo nacional para estabelecer política pública de segurança cibernética, além de criar estrutura de coordenação nacional com autoridade suficiente em todo território brasileiro para execução da política pública. A recomendação recai, mais especificamente, à Casa Civil e ao GSI/PR, a fim de gerenciar o risco:

> *Não há priorização do tema segurança cibernética no Estado brasileiro, o que leva a uma Política Nacional de Cibersegurança que não tem alcance Nacional e à ausência de estrutura com autoridade e prerrogativas suficientes para coordenar a execução dessa política, o que leva à insuficiência de orientação do Estado brasileiro para a atividade de segurança cibernética no país, o que leva a atividades de segurança cibernética insuficientes, as quais combinadas com ataques cibernéticos, leva ao sucesso dos ataques contra organizações e cidadãos brasileiros, o que leva a danos em diversas dimensões por perda da confidencialidade, integridade e disponibilidade de informações e sistemas (e.g., fraudes contra cidadãos, paralisação de serviços prestados à sociedade, prejuízos à imagem das organizações públicas e privadas, perdas financeiras), o que impacta negativamente a soberania digital, a confiança no ambiente digital e a aceleração da transformação digital no país.*

## 5. ORGANIZAÇÕES PÚBLICO/PRIVADA CONTRA O CRIME CIBERNÉTICO

O Relatório do TCU foi claro e essa é uma realidade do mundo cibernético, a de que os ataques são multidimensional, multissetorial e transnacional, o que exige a cooperação do público e do privado, dos

governos, das empresas e da sociedade civil. As audiências públicas igualmente ressaltaram a importância e o imperativo de o setor público estar aliado ao privado no combate aos ataques cibernéticos. A Agência Nacional de Cibersegurança deveria cumprir com essa função e é o que defendemos.

Contudo, a Subcomissão estudou outras formas previstas no direito comparado, como é a *National Cyber-Forensics and Training Alliance* (NCFTA), que é uma sociedade sem fins lucrativos, criada em 2002, nos Estados Unidos da América (EUA), com sede em Pittsburgh [pelo site oficial, ou, segundo outras fontes, como a do *Federal Bureau of Investigation* (FBI), em 1997]. Essa instituição congrega forças policiais, como o FBI, a academia e empresas, possui vocação internacional, e propicia ambiente confiável e confidencial entre os setores público e privado para identificar e neutralizar ameaças cibernéticas.

Trata-se, portanto, de "troca de inteligência estratégica", com livre fluxo de informação entre os parceiros. Atualmente, a NCFTA dedica-se sobretudo a combater vírus informáticos maliciosos (*malware*), esquemas de manipulação de ações, fraudes de telecomunicações e outras fraudes financeiras perpetradas por grupos do crime organizado.

Inspirados nessa organização, outros países instituíram as suas, como o Japão, que criou em 2014 a *Japan Cybercrime Control Center* (JC3), após estudos do Conselho de Política de Segurança de Informação e do Gabinete do Primeiro-Ministro Shinzo Abe. No mesmo sentido, o órgão japonês partilha as respectivas informações, experiências e conhecimentos com base em acordos de confiança e de não divulgação, ao mesmo tempo em que desenvolvem atividades para eliminar ameaças, elucidando as condições reais das ameaças e especificando e perseguindo os perpetradores.

Além disso, formam recursos humanos aptos a enfrentar esses ataques e trabalham com cooperação internacional. Por exemplo, JC3 e NCFTA possuem acordo.

Poder-se-ia classificar a NCFTA e a JC3 como *hubs* confiáveis para circular a informação. Essas organizações possuem quatro políticas fundamentais, que são "Uma só equipe" (a demonstrar o grau de confiança entre os parceiros), "Um objetivo", "Cara a cara" (*face to face*, que são acordos de confidencialidade), "Indústria em primeiro lugar", e "Foco sobre o que você pode compartilhar e se sente confortável em compartilhar".

Entretanto, a NCFTA possui um tamanho bem maior que a JC3, envolvendo mais de quinze agências policiais internas, além das externas, enquanto a JC3 possui o seu próprio corpo de agentes policiais cedidos dos vários agrupamentos policiais. Outra diferença é que a JC3 divulga todos os nomes das empresas participantes, enquanto a NCFTA não.

Os programas da NCFTA dizem respeito, primeiramente, ao programa MCT (ameaças cibernéticas ou, em inglês, *cyber threats*), em que se conecta com equipes de parceiros intersetoriais para compartilhar coletivamente informações sobre ameaças cibernéticas em evolução ou em tempo real. A equipe interna se concentra na identificação, análise e validação de variantes de *malware* e *ransomware* emergentes e existentes e trabalha com parceiros para interromper as ameaças causadas por cibercriminosos, em *deep web* ou fontes abertas.

Outro programa existente destina-se à proteção contra ataque cibernético financeiro (Cyfin), em vários aspectos:

1. A “Iniciativa contra Lavagem de Dinheiro” permite que instituições financeiras compartilhem informações técnicas e transacionais relacionadas ao abuso ou intrusão em contas financeiras e atividades suspeitas de lavagem de dinheiro.

2. A “Iniciativa *Business E-mail Compromise* (BEC)” consulta vítimas de BEC, apoia a divulgação de dados de beneficiários conhecidos associados a eventos de BEC e facilita a repatriação de fundos mal direcionados e roubados através da *Financial Fraud Kill Chain*.

3. A “*Digital Payment Fraud Initiative*” concentra-se na utilização de serviços de pagamento digital, incluindo criptomoedas e pagamentos móveis *peer-to-peer* (P2P) para perpetrar o crime cibernético, a fraude e a lavagem de dinheiro.

4. A “Iniciativa *Crime-as-a-Service* (CaaS)” facilita o desenvolvimento de informações relacionadas com grupos transnacionais do crime organizado que criam, mantêm, vendem ou distribuem serviços criminosos, especialmente branqueamento de capitais como serviço, para promover muitas variantes de crime cibernético;

5. A “Iniciativa contra o Tráfico de Seres Humanos” centra-se na utilização de meios cibernéticos para anunciar e vender acesso a quem é traficado para exploração sexual e na utilização de instrumentos financeiros para facilitar o pagamento por esta atividade.

6. A “Iniciativa contra Fraude com Cartões de Pagamento” mantém duas subiniciativas para apoiar a interrupção do roubo de dados de cartões de pagamento em caixas eletrônicos e pontos de venda (POS): a “Iniciativa Ponto Comum de Compra (CPP)”, que permite que instituições financeiras e autoridades policiais identificar, priorizar, validar e mitigar violações de locais com cartão presente (CP) e cartão não presente (CNP) que resultam no roubo de dados de cartão de pagamento; e a “Iniciativa *Skimming*”, a qual permite que instituições financeiras e autoridades policiais identifiquem, validem e interrompam grupos criminosos transitórios que utilizam dispositivos técnicos implantados (*skimmers* ou *shimmers*) para roubar dados de cartões de pagamento de locais de pagamento, incluindo caixas eletrônicos e pontos de venda.

7. A “*Securities Fraud Initiative*” apoia o setor de corretagem na identificação, validação, mitigação e interrupção do abuso ou intrusão em contas de corretagem e/ou uso de tais contas para negociar ou manipular valores mobiliários de forma fraudulenta (por exemplo, “*pump-and-dump*”), mediante *malware*, *phishing* ou engenharia social.

8. A “Iniciativa contra a Fraude de Identidade Sintética” permite a partilha de inteligência de identidade sintética entre a indústria e as autoridades policiais e interrompe proativamente a utilização de identidades sintéticas ou

artificiais para fraudes, como a proteção e a "eliminação" de linhas de crédito e o branqueamento de capitais.

Por fim, "Programa sobre Marca e Consumidor (BCP)" promove a partilha de informações a respeito de comunidade dedicada a perturbar a distribuição e venda global de produtos contrafeitos; drogas ilícitas, produtos farmacêuticos e tabaco; e fraudes que impactam o setor varejista.

Organizações semelhantes à NCFTA e à JC3 existem em outros países também, como o Reino Unido, com a *Cyber Defence Alliance* (CDA), estabelecida em 2015 por uma coalizão de quatro bancos internacionais e que possui sua sede em Canary Wharf, Londres; e a Ucrânia com a *Global Cyber Cooperative Center* (GC3), criada em 2004. Em síntese, são instituições que possuem um tripé Governo/Academia/Empresas para compartilhar informações de modo seguro e atuar de modo preventivo ou repressivo (sempre há envolvimento de agentes de segurança) contra crimes cibernéticos.

Outro modelo de relacionamento entre os setores público e privado para combate a crimes cibernéticos é o levado a cabo pela Interpol, utilizando-se o centro de dados "*DNA Gateway*". Esse projeto foi criado pela Assembleia Geral da Interpol em 2018 e consiste em um modelo jurídico para que sejam realizadas parcerias com empresas privadas para troca de inteligência, tendo por *hub* o "*Cyber Fusion Center* (CFC)" da Interpol, e, desse modo, criar operações internacionais. O Banco do Brasil, por exemplo, participa desse projeto.

Além disso, o projeto *Gateway* igualmente promove treinamento para os países membros. Dentre os exemplos de operação a envolver o Brasil, citamos o caso, concluído este ano, em que Brasil e Espanha, em conjunto com a Interpol, conseguiram deter cinco programadores no Brasil por trás de uma operação de *trojan* (programas maliciosos disfarçados de softwares comuns, capazes de infectar computadores e causar estragos sem o conhecimento da vítima) bancário de Grandoreiro. O *malware* Grandoreiro tem causado grandes danos desde 2017, introduzido mediante de e-mails de *phishing* que se fazem passar por organizações reconhecidas, como tribunais ou empresas de telecomunicações e energia. Uma vez instalado, o *malware* rastreia as entradas do teclado, simula a atividade do mouse, compartilha telas e exibe pop-ups enganosos, coletando dados como nomes de usuário, informações do sistema operacional, tempo de execução do dispositivo e identificadores bancários. Neste ponto, os criminosos passam a esvaziar contas e enviam os fundos para rede de mulas monetárias, a fim de finalmente, com o dinheiro lavado, transferi-lo para o Brasil. Milhões de euros foram fraudados dessa maneira.

Enfim, instituições como National Cyber-Forensics and Training Alliance (NCFTA) são sem fins lucrativos que atuam como um centro de colaboração e investigação no campo da cibersegurança. Foi fundada para melhorar a segurança cibernética por meio de parcerias entre agências governamentais, empresas do setor privado e outras organizações relevantes. A NCFTA se concentra em identificar, investigar e mitigar ameaças cibernéticas, como fraudes, crimes cibernéticos e ataques de hackers. Contudo, não substitui a necessidade de uma agência pública e, no caso do Brasil, que não possui órgão centralizador, não há que se falar em

algo como a NCFTA. Após a criação da Agência Nacional de Cibersegurança e de sua consolidação regulatória, claro, podemos pensar em modelos complementares.

**CONSIDERAÇÕES FINAIS**

**SENADO FEDERAL**

**COMISSÃO DE RELAÇÕES EXTERIORES E DE DEFESA NACIONAL**

RELATÓRIO DE AVALIAÇÃO DE POLÍTICA PÚBLICA

A POLÍTICA NACIONAL SOBRE DEFESA CIBERNÉTICA

A avaliação de políticas públicas tem como objetivo principal aprimorar a gestão do Estado, por meio da mensuração de sua eficiência, eficácia e efetividade. O resultado da avaliação é fundamental para orientar as ações do Poder Público. A Resolução do Senado Federal n° 44, de 2013, prevê que a Casa Legislativa realize a avaliação de políticas públicas, que buscará, entre outras medidas, adequar os dispositivos normativos às necessidades sociais.

Conforme levantamento divulgado pela empresa de soluções de cibersegurança FORTINET, com base dos dados do FortiGuard Labs, o Brasil foi o segundo país mais atingido da América Latina e Caribe em 2022, com 103,16 bilhões de tentativas de ataques cibernéticos. O número implica aumento de 16% com relação ao ano anterior (88,5 bilhões) e representa quase 30% do número total dos países da região que sofreram com mais de 360 bilhões de tentativas de ciberataques.

Já de acordo com estimativas do Fórum Econômico de Davos, o crime cibernético deve custar ao mundo US$ 9,5 trilhões em 2024. Se fosse um país, o crime cibernético seria a terceira maior economia do mundo.

E foi neste cenário de crescente preocupação com os crimes e as ameaças cibernéticas que propormos, através do Requerimento nº 20/23, a criação da Subcomissão Permanente de Defesa Cibernética, que por sua vez foi instalada, após aprovação deste plenário, em 14/05/2024.

A Subcomissão Permanente presidida por mim é composta por 3 membros titulares e 3 suplentes, onde pudemos contar com a participação ilustre dos Senadores Sérgio Moro, Astronauta Marcos Pontes, Chico

Rodrigues, Fernando Dueire, Nelsinho Trad, além da participação expressiva do Senador Jorge Seilf em missões internacionais.

Em razão da pertinência do assunto decidimos que o foro mais adequado para realização dos trabalhos afetos à Avaliação da Política Pública de Cibersegurança, amparada pelo Requerimento n. 06, aprovado nesta Comissão em 25 de abril do corrente ano, seria a Subcomissão de Defesa Cibernética.

Durante os trabalhos procuramos realizar Audiências Públicas com os segmentos mais importantes do Estado Brasileiro em matéria de Defesa Cibernética, como foi o caso da ABIN e do Exército Brasileiro.

Também abrimos o debate à sociedade civil onde tivemos o cuidado de ouvir e debater com os principais representantes da sociedade civil organizada, atividade privada e demais segmentos de Cibersegurança tanto em nível nacional como em escala mundial, como foi o caso do Banco Interamericano de Desenvolvimento -BID.

Tivemos a oportunidade de conhecer cenários internacionais e, de certa forma, mais desenvolvidos que o nosso em matéria de CiberSecurity como foi o caso da NCFTA, com sede em Pittsburg. A missão teve a iniciativa do Senador Sérgio Moro.

A NCFTA começou a Sua modelação após os lamentáveis atentados sofridos pelos EUA em 09/11, quando se constatou que as principais agências de inteligência dos EUA: FBI, NSA e CIA tinham informações sobre os ataques, mas o sistema de inteligência deles não funcionou. Eram informações fragmentadas.

Deste modo, por iniciativa do setor privado nascia um novo modelo batizado de ‘Fusion Centers”, Parceria Público Privada que resultou em uma interface permanentemente conectada para compartilhamento de informações permitidas e de interesse da nação. Entendemos o NCFTA como uma espécie de Serasa da Segurança Cibernética que deu certo, e que deveria ser implementado no nosso país, devido à sua alta efetividade e baixo custo para os cofres públicos.

Por outro lado, também tivemos a oportunidade de estarmos em Washington D.C, participando de um intercâmbio entre Brasil e EUA, sobre ‘as melhores práticas de Cybersegurança”, com participação de representantes de agências e instituições dos dois países.

Lá, pudemos interagir diretamente com variados segmentos da área, além de observar como o público e o privado funcionam de forma exitosa, sob a coordenação da CISA - A Agência Norte-Americana de Cibersegurnaça e Infraestrutura.

E por estas razões, ficou cada vez mais nítido para os membros da Comissão, sobre a necessidade, cada vez mais urgente, do Brasil contar com uma Agência Nacional de Cibersegurnaça para proteção das nossas infraestruturas críticas.

Não se pode olvidar, que os crimes cibernéticos incluem desde o roubo de dados pessoais, ataques de ransomware, espionagem digital e afetam não apenas a segurança nacional, mas também a estabilidade econômica e a privacidade individual.

Constatamos também que hoje a abordagem no Brasil é fragmentada e as responsabilidades são de diversas agências. Esse sistema desagregado cria confusão e impede a habilidade de responder às ciberameaças de forma eficiente. É preciso de uma entidade centralizada para dar uma direção, acelerar a execução da estratégia nacional de cibersegurança, além da coordenação e supervisão para garantir que os esforços sejam unificados e eficientes, interagindo tanto no setor privado como no público.

Ela agiria como uma autoridade competente para definir, esclarecer papéis, responsabilidades, processos e atividades necessárias para implementar a estratégia e outras ações relacionadas à ciber-resiliência.

Segundo estudo do BID, que é um estudo de agências de segurança cibernética nacionais, agências nacionais de segurança cibernética dos países mais avançados, especialmente Europa, Espanha, França, Itália, Austrália e Estados Unidos, concluiu-se que o objetivo principal de todas as agências nacionais de cibersegurança é a coordenação, obviamente, mas a coordenação de quem? Do setor público, do setor privado e do setor de defesa.

Por corolário, importante transcrever alguns trechos que o Tribunal de Contas da União – TCU concluiu em auditoria n. TC 010.387/2024-2, relatada pelo Eminente Ministro Benjamin Zymler, e aprovada em novembro deste ano:

"O Estado brasileiro não possui organização responsável para orientar a atividade cibernética do país em âmbito nacional, de forma que os esforços empregados no âmbito do poder executivo federal são insuficientes

para alcançar todo o país. Isso pode levar a uma situação de desigualdade cibernética no país em que as organizações com nível de maturidade baixo em segurança não conseguem mitigar adequadamente eventos cibernéticos e representam uma ameaça para todo o ecossistema do país".

Portanto, o presente relatório aponta, após inúmeros debates e análise, considerando que o Decreto nº 11.856, de 2023, instituiu a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança, é falho e o abandono do anteprojeto de lei apresentado pelo GSI, com a proposição de regulação nacional e de criação de uma agência nacional de cibersegurança é essencial.

Desta forma, a presente avaliação da política apresentou três prioridades:

1) conhecer e avaliar o diálogo institucional entre segurança e defesa cibernética;

2) priorizar a participação do nosso país junto ao concerto dos países da América, especialmente da América Latina, em esforços de investigação colaborativa;

3) considerar a necessidade da definição do modelo mais adequado de uma Autoridade de Cibersegurança (agência) para o Brasil. Para tanto, sugerimos que o Executivo encaminhe, com maior brevidade possível, um projeto de lei que estabeleça a forma de funcionamento dessa autoridade.

S.M.J. é o relatório.

Relator,

Sala da Comissão,