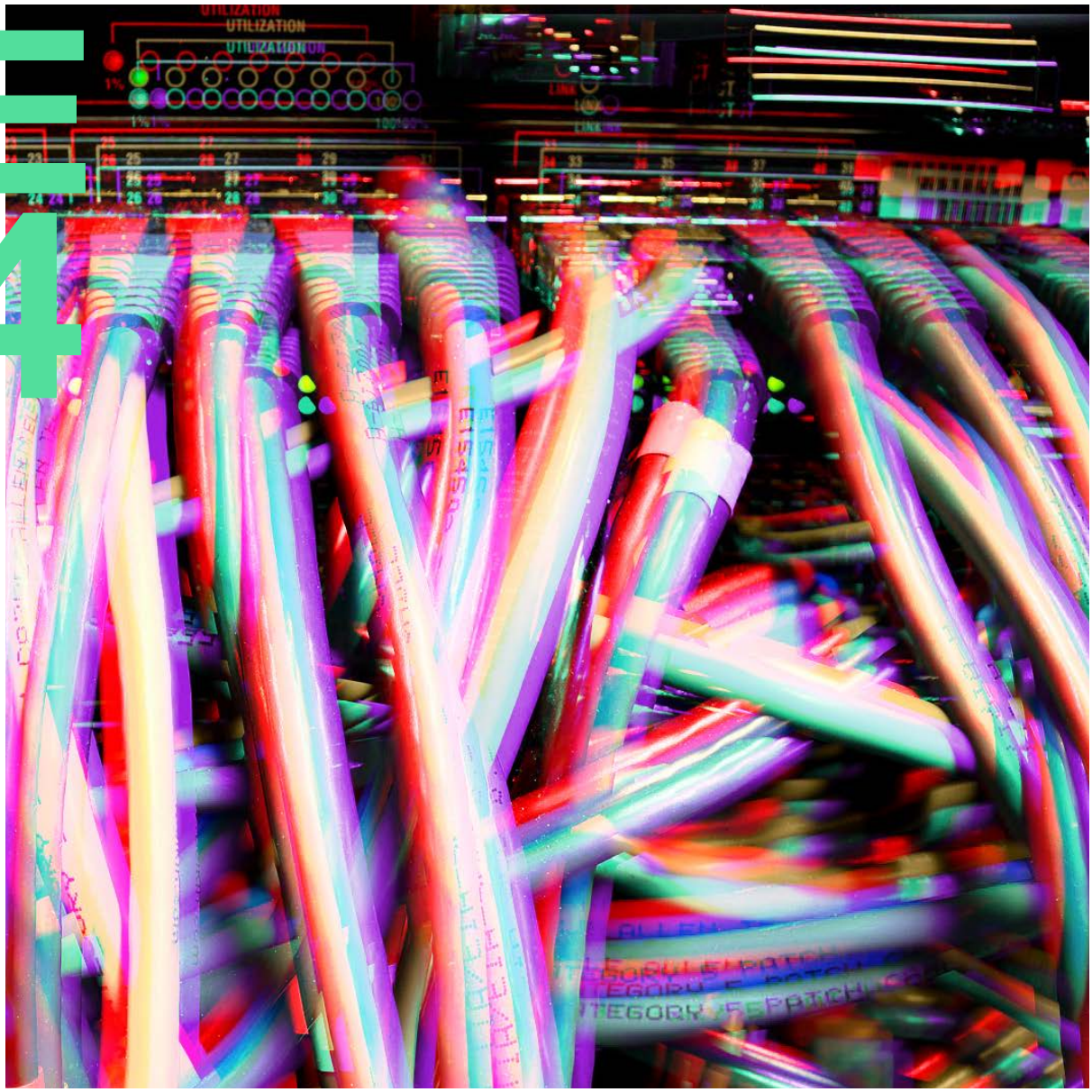
INSTITUTO IGARAPÉ
a think and do tank

AE 54

ARTIGO ESTRATÉGICO 54

ABRIL 2021



CIBERSEGURANÇA NO BRASIL: uma análise da estratégia nacional

Louise Marie Hurel

Índice

Foto da capa: ElasticComputeFarm da Pixabay

CIBERSEGURANÇA NO BRASIL: uma análise da estratégia nacional

Louise Marie Hurel

Sumário executivo

Em fevereiro de 2020, foi publicado o decreto 10.222 que estabeleceu a Estratégia Nacional de Segurança Cibernética do Brasil (E-Ciber) — o primeiro documento oficial que visa proporcionar um panorama sobre o papel do Brasil na segurança cibernética, bem como os objetivos e princípios norteadores para seu desenvolvimento entre os anos de 2020 e 2023.

Com a pandemia da Covid-19, milhares de pessoas, órgãos governamentais e empresas tiveram que rapidamente adaptar suas atividades para um ambiente majoritariamente virtual. Essa migração imediata trouxe consigo ameaças e novas superfícies para ataques e exploração de vulnerabilidades computacionais. Mais do que nunca, os diferentes setores precisam estar preparados e capacitados para responder e resistir a essas tentativas. No entanto, foi nesse momento que o Brasil sofreu o pior ataque cibernético de sua história, mostrando, mais uma vez, que muitos desafios permanecem para que a segurança se transforme em ações práticas no funcionamento de diferentes setores.

Neste artigo estratégico identificamos as principais lacunas para o avanço da governança da segurança cibernética no país. Destrinchamos os principais elementos da E-Ciber, buscando compreender e posicionar a visão estratégica do país não só historicamente, mas também em relação a outras experiências internacionais. Propomos uma abordagem principiológica para fortalecer e informar a implementação de objetivos estratégicos para a segurança cibernética no Brasil, sendo estes: coordenação e cooperação nacional e internacional, integração de conhecimentos, sustentabilidade de esforços e capacitação em temas relacionados à segurança cibernética.

Este documento é o resultado de três meses de entrevistas com especialistas de diversos setores, análise temática de documentos, trabalho etnográfico em diferentes espaços, fóruns e diálogos sobre o tema.

Os desafios identificados nas entrevistas e no trabalho de campo foram:[1]

(i) A ausência de uma linguagem compartilhada para se referir às questões de segurança cibernética/digital na sociedade;
(ii) A associação de segurança cibernética com assuntos, responsabilidades e competências de instituições militares;
(iii) Desconhecimento de riscos específicos e compartilhados entre setores;
(iv) Ausência de mecanismos para o compartilhamento de informações sobre riscos/ameaças e conhecimento em segurança entre setores;
(v) Falta de alinhamento normativo, estratégico e operacional para responder a incidentes; e
(vi) Existência de diferentes níveis de maturidade da sociedade em segurança cibernética.

1 Ver Anexo 1 para maiores detalhes sobre os diferentes desafios identificados.

Acrônimos

Anatel – Agência Nacional de Telecomunicações

BACEN – Banco Central do Brasil

CBC – Comissão Brasileira de Comunicação

CBMs – Confidence-Building Measures / Medidas de Construção de Confiança

CDCiber – Centro de Defesa Cibernética

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

ComDCiber – Comando de Defesa Cibernética

CTIR Gov – Centro de Tratamento e Resposta a Incidentes Cibernéticos do Governo

DSI / GSI – Departamento de Segurança da Informação da Presidência da República

E-Ciber – Estratégia Nacional de Segurança Cibernética

EnaDCiber – Escola Nacional de Defesa Cibernética

ENSIC – Estratégia Nacional de Segurança de Infraestruturas Críticas

GSI - Gabinete de Segurança Institucional da Presidência da República

MRE – Ministério das Relações Exteriores

OEA – Organização dos Estados Americanos

PNSIC – Política Nacional de Segurança de Infraestruturas Críticas

REMJA - Reuniões de Ministros da Justiça e de Outros Ministros ou Procuradores-Gerais das Américas

SISBIN – Sistema Brasileiro de Inteligência

SMDC – Sistema Militar de Defesa Cibernética

UNGGE – United Nations Group of Governmental Experts

Introdução

A segurança de dados, sistemas, redes e infraestruturas digitais é uma importante dimensão de uma sociedade cada vez mais conectada. Todo dia, milhares de ataques são realizados em redes distribuídas globalmente, comprometendo empresas, serviços e dispositivos, e expondo dados pessoais e sensíveis de indivíduos. Isso ocorre em um contexto no qual mais da metade da população global está conectada à Internet e com grande parte de suas experiências de conectividade concentradas em smartphones. Só no Brasil, 70% das pessoas estão conectadas à Internet, sendo que 85% dos cidadãos das classes D e E acessam a Internet só pelo celular e com planos de telefonia limitados.[2] A pergunta que precisamos considerar é: como o Brasil tem respondido aos desafios associados à segurança cibernética nacional? O Brasil ocupa o 70º lugar no ranking internacional do Índice Global de Segurança Cibernética[3] da União Internacional de Telecomunicações e 6º na região das Américas — com Uruguai, México e Paraguai ultrapassando o país.

Desde 2015, o Brasil caminha gradualmente para uma crise social e econômica profunda, com alguns especialistas afirmando ser o início de mais uma "década perdida"[4] para o maior país da América Latina. Essas crises foram acompanhadas por desafios políticos

O Brasil ocupa o 70º lugar no ranking internacional do Índice Global de Segurança Cibernética da União Internacional de Telecomunicações e 6º na região das Américas — com Uruguai, México e Paraguai ultrapassando o país.

e ideológicos que marcaram um conturbado futuro para o Brasil — agora aprofundado pela pandemia da Covid-19. Nesse mesmo contexto, o Brasil e outros países da região se veem mais dependentes de sistemas, redes e da Internet para garantir transações, serviços e diálogos. Mais do que nunca, a pandemia expôs tanto a dependência da nossa sociedade no ambiente digital quanto as desigualdades de acesso e a falta de investimentos em segurança cibernética (especialmente no setor público).

De acordo com o relatório de riscos do Fórum Econômico Mundial de 2020,[5] **ataques cibernéticos e comprometimento de infraestruturas de informação estão entre os 10 maiores riscos globais em termos de impacto.** Esses riscos foram consideravelmente ampliados com a pandemia. A Covid-19 não só resultou em uma acelerada digitalização de empresas

2 SOPRANA, P. 70 milhões de brasileiros têm acesso precário à internet na pandemia do coronavírus. **Folha de São Paulo**. 2020. Disponível em: https://www1.folha.uol.com.br/mercado/2020/05/cerca-de-70-milhoes-no-brasil-tem-acesso-precario-a-internet-na-pandemia.shtml.

3 2018 Global Cybersecurity Index (GCI). **International Telecommunications Union**. 2018. Disponível em: https://www.itu.int/dms pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

4 STOTT, M. Latin America faces a second 'lost decade'. **Financial Times**. 2019. Disponível em: https://www.ft.com/content/07f0e09e--0795-11ea-9afa-d9e2401fa7ca.

5 WEF. Global Risks Report. **World Economic Forum**. 2020. Disponível em: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.

e serviços,[6,7] mas na criação de uma nova superfície de ataques e vulnerabilidades. O aumento de pessoas trabalhando de casa e/ou o pouco conhecimento sobre boas práticas de segurança podem acabar potencializando as vulnerabilidades dos sistemas do setor público e privado, expondo-os a novos tipos de ataques. Esse foi o caso do ataque ao Superior Tribunal de Justiça, em novembro de 2020. Categorizado como o "pior ataque cibernético da história do país"[8], o *ransomware* criptografou todos os arquivos do segundo órgão de maior importância no sistema judiciário, ressaltando, mais uma vez, as falhas nos sistemas e no preparo dos órgãos da Administração Pública Federal em responder a ataques.

Novas tecnologias de comunicação e informação precisam ser integradas na sociedade de forma sustentável. Para tal finalidade, torna-se **indispensável assegurar não só o seu pleno funcionamento, mas o entendimento dos diferentes riscos e impactos que essas tecnologias introduzem no exercício de direitos, no funcionamento da economia, nas infraestruturas críticas e para a confiabilidade dos indivíduos nos benefícios associados às mesmas.** Conforme apontado pela Estratégia de Transformação Digital lançada em 2018, a confiança no ambiente digital envolve a atuação estatal em proteção de direitos e privacidade e segurança e defesa.[9]

A garantia da segurança digital e cibernética depende de múltiplos atores, tais como: empresas, governos, da sociedade civil, da academia e da comunidade técnica. Cada um desempenha uma importante função no aprimoramento, manutenção e construção de uma sociedade resiliente e preparada para responder aos crescentes desafios de segurança. Essas respostas vão desde programas de capacitação para grupos da sociedade civil e jornalistas investigativos, até a elaboração de leis como a Lei Geral de Proteção de Dados e de documentos estratégicos como a Estratégia Nacional de Segurança Cibernética (E-Ciber) lançada em fevereiro de 2020.

Conforme apontado pelo relatório da Global Partners Digital sobre abordagens multissetoriais para o desenvolvimento de estratégias nacionais de segurança cibernética,[10] nem todos os atores e setores precisam estar sempre envolvidos em todas as dimensões do processo governamental de consolidação de capacidades e políticas**, mas todos compõem um espectro de expertise e desempenham um papel importante na sensibilização do setor público sobre**

---

6 Isso inclui a proliferação de serviços por aplicativos e a expansão dos trabalhadores da chamada "gig economy" – uma economia baseada em trabalho informal mediado por plataformas digitais. Mudanças drásticas na economia durante a pandemia resultaram em uma oferta e concentração de trabalho informal via plataformas. Conforme muitos estudos já apontaram, a expansão da gig economy afeta desproporcionalmente classes médias e baixas (De Stefano, 2016; van Doorn, 2017). No Brasil, as manifestações do "Breque dos Apps" em julho de 2020 foram um momento significativo no qual os entregadores de diferentes aplicativos de diferentes estados se reuniram para reivindicar a criação de uma tabela mínima para o serviço (Ribeiro, 2020).

7 DE STEFANO, V. The Rise of the "Just in Time Workforce": On Demand Work, Crowdwork and Labour Protection in the "Gig Economy". **Conditions of Work and Employment Series,** n. 71 (Geneva: International Labour Organization);
VAN DOORN, N. Platform labor: on the gendered and racialized exploitation of low-income service work in the 'on-demand' economy. **Information, Communication & Society**, v. 20, n. 6, p. 898-914. 2017. DOI: 10.1080/1369118X.2017.1294194;
RIBEIRO, C. Breque dos Apps: entregadores paralisam atividades novamente e fazem atos no país. **Agência Brasil.** 2020. Disponível em: https://agenciabrasil.ebc.com.br/radioagencia-nacional/acervo/geral/audio/2020-07/breque-dos-apps-entregadores-paralisam-atividades-novamente-e-fazem-atos-no-pais/.

8 MARIN, J. "Ataque hacker ao STJ é o pior da história do Brasil". **TecMundo.** 2020. Disponível em: https://www.tecmundo.com.br/seguranca/206233-ataque-hacker-ter-atingido-stj-pf-investiga.htm

9 BRASIL. Estratégia Brasileira para a Transformação Digital (E-Digital). 2018.

10 SHEARS, M.; SCHNIDRIG, D. & KASPAR, L. Multistakeholder Approaches to National Cybersecurity Strategy Development. **Global Partners Digital**. 2018. Disponível em: https://www.gp-digital.org/publication/multistakeholder-approaches-to-national-cybersecurity-strategy-development/

diferentes dimensões da segurança cibernética — que vão desde a proteção de infraestruturas críticas, gestão de incidentes, mobilização de expertise diversa em processos de atribuição cibernética[11] até a preservação de direitos humanos no processo de desenvolvimento e implementação de políticas. Dessa forma, cada setor tem um papel importante na construção e operacionalização de uma visão estratégica para o país. Ocupam uma posição essencial para a integração da segurança na economia, sociedade e defesa do Brasil.

No entanto, apesar da interdependência da segurança cibernética e da responsabilidade compartilhada dos setores no fortalecimento do ecossistema digital, a agenda de segurança cibernética no país permanece profundamente fragmentada e os setores encontram-se, por vezes, isolados em seus esforços por diversos motivos[12] — os quais iremos explorar neste documento. Essa fragmentação tem severas consequências para que o Brasil possa responder de forma rápida e efetiva a ataques, bem como pautar uma visão que seja implementável e sustentável no longo prazo.

Com isso em mente, um importante questionamento permanece: **como podemos melhor integrar a discussão sobre segurança cibernética no Brasil?** Em nossa publicação "Uma Estratégia para a Governança da Segurança Cibernética no Brasil"[13] procuramos mapear esforços de diferentes setores e iniciativas que buscaram criar elos intersetoriais. Identificamos que grande parte dos esforços em respostas a incidentes e ao compartilhamento de informações em períodos críticos, como nos megaeventos, foram bem sucedidos em estabelecer boas práticas e instituições para iniciar essa troca de informações. No entanto, quando olhamos para processos de desenvolvimento de políticas, a segurança cibernética permanece um elemento desafiador no relacionamento entre setor público e os grupos da sociedade civil.

Neste artigo, focamos na Estratégia Nacional de Segurança Cibernética (E-Ciber), buscando melhor compreender as propostas da Estratégia vis à vis os desafios para a integração de conhecimentos e práticas para a cibersegurança do país. Este trabalho é o resultado de entrevistas semi estruturadas e não estruturadas com especialistas de diferentes setores, extensa revisão de documentos primários, e trabalho etnográfico em fóruns e diálogos nacionais e internacionais sobre a segurança cibernética no Brasil. As próximas seções apresentam os principais conceitos e políticas, bem como identificam as principais lacunas para a construção de um sistema de governança mais integrado.

---

11 EGLOFF, F.J. Contested public attributions of cyber incidents and the role of academia. **Contemporary Security Policy**, v. 41, n.1, p. 55-81. 2019. DOI: 10.1080/13523260.2019.1677324. Disponível em: https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1677324.

12 O reconhecimento público da fragmentação do debate sobre segurança cibernética não exclui os mecanismos já existentes e políticas dentro de cada setor – e a sua importância para a governança da cibersegurança no país. Um exemplo é o estabelecimento de equipes e planos de segurança da informação em diferentes Ministérios com o objetivo de desenvolver boas práticas para a garantir a confidencialidade, integridade e acessibilidade da informação.

13 HUREL, L.M. & LOBATO, L.C. Uma Estratégia para a Governança da Segurança Cibernética. **Instituto Igarapé**. 2018. Disponível em: https://igarape.org.br/uma-estrategia-para-a-governanc%cc%a7a-da-seguranc%cc%a7a-cibernetica-no-brasil/.

O que é segurança cibernética?[14]

Não existe consenso global sobre a definição de segurança cibernética. De acordo com padrões como **ISO/IEC 27032:2012**, o termo se refere à preservação da confidencialidade, integridade e disponibilidade de informações no ciberespaço, ou seja, aos princípios que norteiam as atividades de segurança. A **União Europeia**, por outro lado, adota uma definição mais abrangente na qual segurança cibernética é definida como as atividades necessárias para proteger redes e sistemas de informação, os usuários desses sistemas e outras pessoas afetadas por ameaças cibernéticas. Nesse caso, a segurança não tem como objetivo final a segurança do ciberespaço, mas dos sistemas, usuários e informações que compõem, atuam e são afetados por ameaças e ataques cibernéticos. Já o **Reino Unido** define o termo como a proteção dos sistemas interligados (hardwares, softwares e infraestruturas associadas), dos dados neles contidos e dos "serviços que disponibilizam, contra o acesso não autorizado, prejuízos (*harm*) ou uso indevido. Isso inclui prejuízos causados pelo operador do sistema, seja intencional ou acidentalmente, ao não seguir os procedimentos de segurança ou ao ser manipulado para provocar tais prejuízos." Tal definição introduz elementos específicos de riscos, danos e impactos associados às atividades maliciosas, incluindo os dados e sistemas. Por fim, a **Colômbia** cita explicitamente que a segurança cibernética é compreendida como uma capacidade do Estado de minimizar o nível de riscos aos quais seus cidadãos estão expostos. Sua finalidade é a de proteger os cidadãos e os "ativos do Estado" e compreende um conjunto de recursos, políticas, conceitos de segurança, salvaguardas, diretrizes, métodos de investigação e gestão de riscos. Ao passo que essa definição inclui o cidadão como elemento central, entende que o Estado é o principal ator na facilitação e provisão dessa segurança.

No Brasil, a segurança cibernética se refere a:

"Ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis" — Glossário de Segurança da Informação.

A definição reitera os chamados "princípios CIA" (*Confidentiality, Integrity and Availibility*) comumente compartilhados pela comunidade de segurança da informação, conforme apontado acima. No entanto, ressalta o papel da resiliência de sistemas, bem como introduz, em sua segunda parte, a preocupação com dados "armazenados, processados ou transmitidos", uma linguagem diretamente incorporada da Lei Geral de Proteção de Dados Brasileira aprovada em 2018. Diferente da Colômbia ou da União Europeia, o Brasil não se refere ao papel do indivíduo na sua definição de segurança cibernética.

14 Tradução livre de definições. ISO/IEC 27032:2012; EU (2019) Regulation (EU) 2019/881. European Parliament; Colombia (2020); Conpes 3995: Política Nacional de Confianza y Seguridad Digital. Consejo Nacional de Política Económica y Social República de Colombia; Brasil (2020). Glossário de Segurança da Informação. GSI/PR.

O que é a governança da segurança cibernética?

A ***governança[15,16] da segurança cibernética*** se refere a uma visão holística e integrada da segurança das redes, dos sistemas e serviços e das infraestruturas em uma sociedade. Para tanto, **ela inclui as instituições, iniciativas, políticas, programas e entre outros mecanismos (formais e informais) que integram um ecossistema de competências e responsabilidades distribuídas para a segurança cibernética**. A Estratégia Nacional de Segurança Cibernética (E-Ciber), por exemplo, é um componente essencial para o estabelecimento de uma visão e estrutura de governança para um país, bem como para a expansão de novos horizontes para desenvolvimento de capacidades. Apesar de ser um termo recente, a *governança da segurança cibernética* foi incluída, pela primeira vez, na E-Ciber*:*

> A governança na área cibernética está relacionada às ações, aos mecanismos e às medidas a serem adotados com o fim de simplificar e modernizar a gestão dos recursos humanos, financeiros e materiais, e acompanhar o desempenho e avaliar os resultados dos esforços empreendidos nesse campo.
>
> Essa governança visa incorporar elevados padrões de conduta em segurança cibernética, e orientar as ações de agentes públicos e de agentes privados, ao considerar o papel que exercem em suas organizações, conforme a finalidade e a natureza de seu negócio.
>
> Inclui, ainda, o planejamento voltado à execução de programas, de projetos e de processos, e o estabelecimento de diretrizes que irão nortear a gestão de riscos. Nesse contexto, orienta pessoas e organizações quanto à observância das normas, dos requisitos e dos procedimentos existentes em segurança cibernética.[17]

O Livro Verde de Segurança Cibernética,[18] publicado em 2010, já fazia menção à necessidade do estabelecimento de uma "macro coordenação e governança" que pudesse apoiar o desenvolvimento de "um conjunto de ações colaborativas entre o governo, o setor privado, a academia, o terceiro setor e a sociedade".[19] Dez anos depois, concretiza-se a primeira Estratégia Nacional de Segurança Cibernética.

Ao longo dos últimos anos, diversas instituições e especialistas buscaram desenvolver e articular diferentes conceitos associados a essa governança. O Global Cyber Security Capacity Centre (GCSCC) da Universidade de Oxford, por exemplo, desenvolveu um modelo de análise de *maturidade* em cibersegurança nacional (CMM). O modelo divide maturidade em cinco

15 Governança é um conceito bastante controverso e debatido em diferentes disciplinas. De acordo com Rosenau e Czempiel (1992), a governança é um conceito que transcende o escopo de governo e abraça mecanismos informais, não governamentais dentro de um sistema (nacional ou internacional). Gbikpi e Grote (2002), por outro lado, trabalham com o conceito de governança participativa, ou seja, o entendimento de que o desenvolvimento de políticas no sentido de encorajar atores a articularem seus interesses e deliberarem sobre seus propósitos comuns é parte da solução para alcançar políticas públicas sustentáveis.

16 ROSANAU, J. N.; CZEMPIEL, E.-O. **Governance without Government: Order and Change in World Politics**. Cambridge: Cambridge University Press. 1992.
GBIKPI, B.; GROTE, J.R. From Democratic Government to Participatory Governance. Em: GBIKPI, B.; GROTE, J.R. (org.). **Participatory Governance: Political and Societal Implications**. Springer Nature. 2002.

17 Definição extraída da E-Ciber.

18 Documento desenvolvido e publicado pelo Gabinete de Segurança Institucional em 2010 que apresentava potenciais diretrizes estratégicas para o estabelecimento da Política Nacional de Segurança Cibernética no seu curto, médio e longo prazo.

19 MANDARINO, R. & CANONGIA, C. **Livro Verde de Segurança Cibernética**. GSI/DSI. 2010. (Página 14)

dimensões: (i) políticas e estratégias, (ii) cultura e sociedade, (iii) educação, (iv) legislação e (v) padrões e tecnologias. Outras organizações como o Potomac Institute desenvolveram um índice de *preparo*[20] (*readiness*, em inglês) cibernético para auxiliar líderes em diferentes países a identificarem lacunas entre a postura atual de um país e as capacidades necessárias para se atingir uma visão de desenvolvimento econômico.[21] Esses e outros modelos ocupam um importante espaço na consolidação de parâmetros mínimos para a segurança cibernética a nível nacional. Contudo, apesar dos diagnósticos proporcionados por esses modelos, a pergunta permanece sobre como podemos atingir maior **integração** e troca entre diferentes componentes dessa governança da cibersegurança.

É importante ressaltar que a *governança* não se restringe ao estabelecimento de uma "cultura de cibersegurança"[22,23] tampouco a esforços de conscientização sobre os riscos associados ao ambiente digital. Apesar de estarem intimamente conectados, a **governança** se refere a uma constelação de arranjos de normas, políticas, padrões e práticas que coordenam e compõem o desenvolvimento da segurança cibernética; ao passo que a **cultura** se refere a conceitos, paradigmas, ideias, narrativas e práticas que estão continuamente e, às vezes, inconscientemente, moldando as múltiplas percepções e práticas sobre segurança.

A governança nos permite compreender a cultura como um componente que permeia e informa quais arranjos e mecanismos podem ser adotados para responder, identificar e preservar sistemas, redes, dados e infraestruturas, bem como fortalecer direitos fundamentais em um país.

Conforme as próximas seções evidenciam, tanto órgãos do governo quanto o setor privado avançaram no desenvolvimento de políticas específicas de segurança cibernética e da informação, mas isso trouxe novas questões para o alinhamento de visões e cooperação em, pelo menos, três eixos:

- Primeiro, uma falta de alinhamento entre os formuladores de políticas públicas e especialistas técnicos trabalhando em seus respectivos departamentos de segurança da informação.
- Segundo, uma falta de alinhamento entre diferentes órgãos, associações, e setores para cooperação nesses temas.
- Terceiro, uma falta de alinhamento de conceitos e vocabulários para identificar ameaças e riscos, bem como para desenhar estratégias para uma governança abrangente da segurança cibernética no Brasil.

---

20 Cyber Readiness Index, em inglês (CRI).

21 Em contraste ao CMM de Oxford, o índice de preparo cibernético destaca sete elementos para se medir e analisar preparo: (i) estratégia nacional; (ii) respostas a incidentes; (iii) crime digital e investigações; (iv) compartilhamento de informação; (v) investimento em pesquisa e desenvolvimento; (vi) diplomacia e comércio; (vii) defesa e resposta a crises.

22 Não existe uma só definição sobre "cultura da cibersegurança", no entanto duas dimensões do debate merecem atenção. Primeiro, a cultura está associada ao ambiente intraorganizacional. Estudos organizacionais e relatórios do setor privado compreendem cultura como algo que está centrado no "fator humano" envolvido na segurança cibernética. Ao estabelecer uma cultura organizacional, a organização deve levar em consideração os artefatos, valores, premissas tacitamente compartilhadas e níveis de conhecimento sobre segurança cibernética ou segurança da informação (Van Niekerk & Von Solms, 2009). Campanhas de conscientização seriam uma forma de criar essa cultura, tornando a segurança da informação e cibersegurança parte de suas rotinas (Von Solms, 2000). Segundo, a noção de "cultura de cibersegurança" surgiu como uma pauta internacional em 2003, com a aprovação da Resolução da Assembleia Geral da ONU sobre o estabelecimento de uma cultura global para a segurança cibernética. Desde então, o documento serve como referência central em debates internacionais e regionais sobre a construção de capacidades para a cibersegurança (A/RES/57/239).

23 VON SOLMS, B. Information security – the third wave? **Computers & Security**. v. 19, n. 7, p.615–20. 2000. DOI: https://doi.org/10.1016/S0167-4048(00)07021-8

VAN NIEKERK, J. F. & VON SOLMS, R. (2009). Information Security Culture: A Management Perspective. **Computers and Security.** v. 29, n. 4, p. 476-486. 2009. DOI: https://doi.org/10.1016/j.cose.2009.10.005

Com base nos modelos já desenvolvidos para análises de capacidades cibernéticas,[24,25] estudos sobre governança, e entrevistas semiestruturadas e não estruturadas, esse documento analisa os diferentes componentes dessa governança no contexto da E-Ciber, buscando compreender como a Estratégia configura a integração[26] e cooperação.

As dimensões tratadas[27] neste trabalho são: a cooperação nacional e internacional, coordenação, integração de conhecimentos, sustentabilidade de esforços e capacitação em temas relacionados à segurança cibernética. Todas as dimensões estão intimamente ligadas, porém, ao separá-las, podemos identificar desafios e boas práticas específicas para o desenvolvimento de cada pilar.

Cooperação (nacional e internacional) – Se refere à troca ou trabalho entre diferentes partes com uma finalidade comum. Neste caso, remete, por exemplo, tanto a acordos, planos e cooperação operacional, como ao desenvolvimento de mecanismos para aprimoramento do trabalho entre setores, ministérios e agências dentro e fora da administração pública federal, bem como práticas (formais e informais) de colaboração entre atores.

Coordenação – Estabelecimento de canais, pontos de contato, boas práticas, protocolos e/ou outros mecanismos para coordenação de atividades ligadas à segurança cibernética. Tal coordenação é potencializada em contextos institucionais com claros papéis e responsabilidades bem como mecanismos específicos intra e interagências e multissetoriais.

Capacitação – Inclui elementos como a formação e treinamento em segurança cibernética e as ações destacadas para elevar o grau de capacidades em responder a ameaças cibernéticas. O estabelecimento de protocolos de compartilhamento de informação e de vulnerabilidade, entre agências do governo e com outros setores, são alguns exemplos de boas práticas adotadas por diferentes paíes, que viabilizam a circulação e comunicação de conhecimentos para o desenvolvimento informado de respostas a ameaças.

Integração de conhecimentos – Desde atividades de resposta e tratamento de incidentes à proteção de dados e preservação de direitos humanos, a segurança não só depende da articulação entre diferentes grupos, mas de diferentes conhecimentos e *expertise*.

Sustentabilidade de esforços – O desenho de mecanismos, parcerias e atividades que possam ter um impacto duradouro e/ou que possam perdurar e se adaptar de acordo com as mudanças no panorama de ameaças e riscos. Sendo assim, a sustentabilidade é compreendida em *lato sensu*, podendo se referir à sustentabilidade financeira e de mecanismos de governança, estratégias, canais de cooperação, medidas de transparência e prestação de contas, bem como a *frameworks* para monitoramento e implementação de atividades/objetivos.

---

24 "Capacidades cibernéticas" se refere ao conjunto de iniciativas que visa empoderar indivíduos, sociedades e governos para desfrutarem dos benefícios da digitalização. Não existe uma só definição sobre capacidades. Dada a sua subjetividade e os múltiplos contextos e realidades sociais, econômicas e políticas nas quais essas capacidades são identificadas, podem variar grandemente de acordo com o país. No entanto, Pawlak e Barmpaliou (2017), apresentam pelo menos cinco perspectivas que informam o debate sobre construção de capacidades cibernéticas (CCB). A perspectiva de desenvolvimento, a qual se assemelha à definição acima, ressalta como essas capacidades são fundamentais para o desenvolvimento sustentável de uma segurança cibernética na qual os benefícios são distribuídos nas mais diversas esferas da sociedade.

25 PAWLAK, P.; BARMPALIOU, P-N. Politics of cybersecurity capacity building: conundrum and opportunity. **Journal of Cyber Policy**. v. 2, n.1, p. 123-144. 2017. DOI: 10.1080/23738871.2017.1294610

26 Nesse sentido, integração se refere a indicadores específicos para o desenvolvimento de uma governança mais inclusiva em temas relacionados à cibersegurança no Brasil.

27 As dimensões foram extraídas a partir da análise de documentos e entrevistas, bem como foram inspiradas pelo trabalho: HOHMANN, M; PIRANG, A; BENNER, T. Advancing Cyebrsecurity Capacity Building: Implementing a Principle-Based Approach. **GPPi**. 2017. Disponível em: https://www.gppi.net/2017/03/06/advancing-cybersecurity-capacity-building-implementing-a-principle-based-approach

O Panorama Multissetorial da Governança da Cibersegurança[28]

Ao longo dos últimos anos, a segurança cibernética foi continuamente associada a um grupo específico de órgãos: o Gabinete de Segurança Institucional, as Forças Armadas, os órgãos de inteligência, a Polícia Federal e os centros de resposta a incidentes.[29] O GSI (Departamento de Segurança da Informação) e as Forças Armadas (Comando de Defesa Cibernética e Centro de Defesa Cibernética) se colocam como ponto central das responsabilidades e competências associadas com a segurança e defesa cibernética, respectivamente. Isso ocorre, em grande parte, devido à rápida institucionalização das capacidades e responsabilidades cibernéticas nesses dois órgãos durante o período dos megaeventos.

O que a imagem abaixo mostra é que, apesar desses polos de concentração de competências, a responsabilidade prática e atuação em temas relacionados à segurança cibernética depende de um grupo maior de atores que vem, ao longo dos últimos anos, moldando diferentes dimensões desse debate.[30]

Uma perspectiva da governança da cibersegurança no Brasil nos permite visualizar segurança não só como algo que é levado a cabo pelas políticas e instituições do governo, mas como um panorama mais amplo que inclui organizações da sociedade civil, setor financeiro e entre outros.[31] A figura abaixo retrata a pluralidade das instituições atuais e a visão de um campo complexo, no qual todos esses atores (e suas respectivas políticas setoriais e normas) estão posicionados. O reconhecimento da segurança cibernética como uma responsabilidade compartilhada é o primeiro passo para se visualizar as lacunas e identificar as oportunidades para o fortalecimento da resiliência do país em segurança.

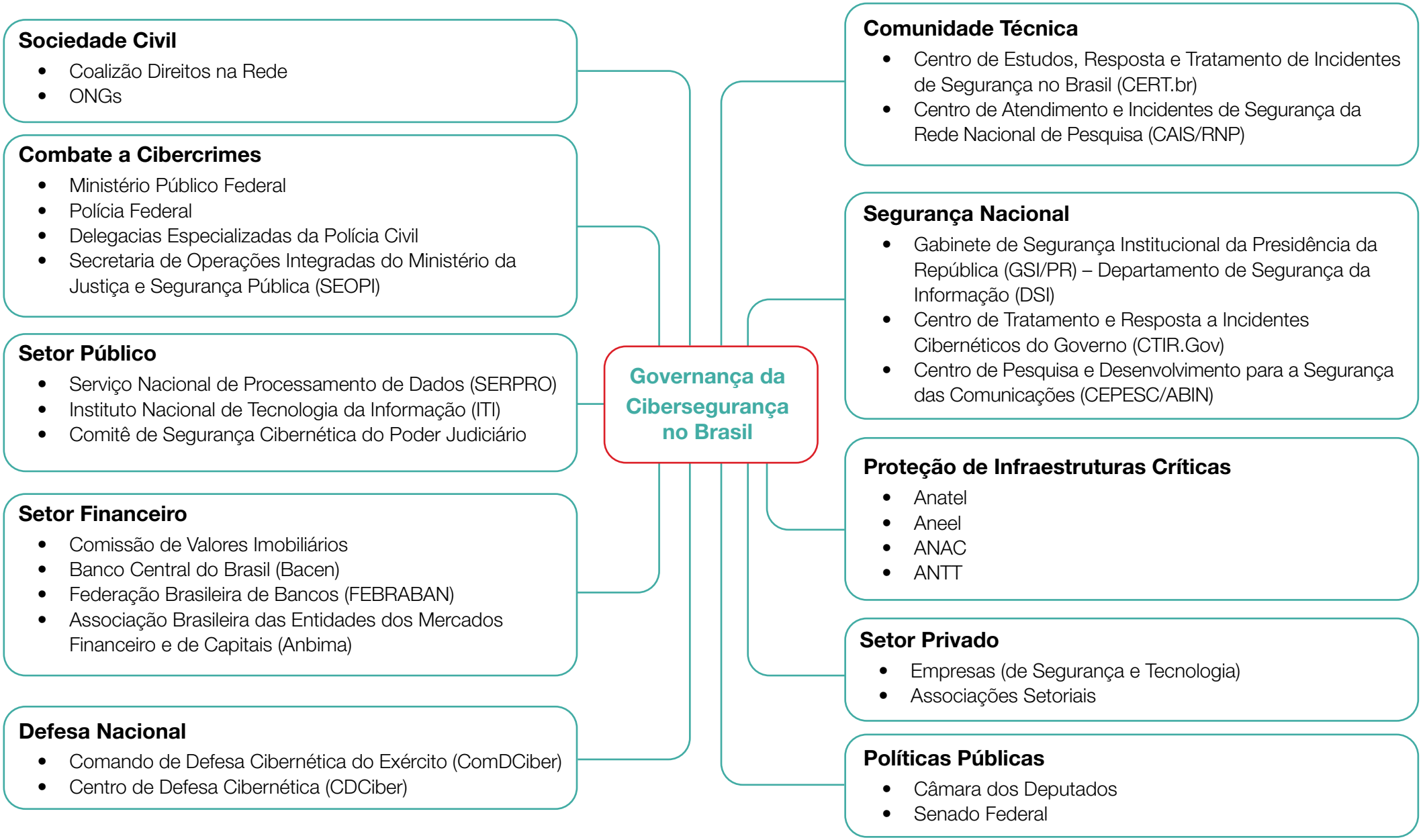
28 A imagem da governança da cibersegurança no Brasil não é exaustiva. A seleção dos setores e atores surgiu a partir das entrevistas, análise de documentos e mapeamento de iniciativas dos diferentes setores.

29 DINIZ, G.; MUGGAH, R.; GLENNY, M. Deconstructing cyber security in Brazil: Threats and responses. Rio de Janeiro: **Instituto Igarapé**, p. 3-32. (Strategic Paper 11). 2014.

30 HUREL, L. M. "Securitização e governança da Segurança Cibernética no Brasil". Em REIA, J.; FRANCISCO, P.A.P.; BARROS, M.; MAGRANI, E. (org.). **Horizonte presente: tecnologia e sociedade em Debate.** Belo Horizonte: Letramento. 2018.

31 HUREL, L.M. & LOBATO, L.C. Uma Estratégia para a Governança da Segurança Cibernética. **Instituto Igarapé**. 2018. Disponível em: https://igarape.org.br/uma-estrategia-para-a-governanc%cc%a7a-da-seguranc%cc%a7a-cibernetica-no-brasil/.

Governança da Cibersegurança no Brasil



Desafios para a Governança da Segurança Cibernética no Brasil

Após três meses de entrevistas com especialistas de diferentes setores, análise de documentos e trabalho etnográfico em diferentes espaços, fóruns e diálogos sobre o tema, identificamos seis desafios centrais para a governança da segurança cibernética no Brasil — que serão abordados no contexto da E-Ciber:

- A ausência de uma linguagem compartilhada para se referir às questões de segurança cibernética/digital na sociedade;
- A associação de segurança cibernética com assuntos, responsabilidades e competências de instituições militares;
- Desconhecimento de riscos específicos e compartilhados;
- Ausência de mecanismos para o compartilhamento de informações sobre riscos/ameaças e conhecimento em segurança entre setores;
- Falta de alinhamento normativo, estratégico e operacional; e
- Existência de diferentes níveis de maturidade da sociedade sobre segurança cibernética.

Construindo uma visão para a segurança cibernética no Brasil: a E-Ciber

As **estratégias nacionais de segurança cibernética** são planos de ação desenhados para melhorar a resiliência e a segurança de infraestruturas, serviços e cidadãos. Elas apresentam os principais objetivos, prioridades e princípios a serem alcançados pelo país nos anos seguintes.[32] Mais de 100 países já publicaram suas estratégias nacionais.[33] Na região da América Latina e Caribe, 12 países possuem estratégias nacionais de segurança cibernética e seis estão em fase de elaboração. O Brasil é o 12º país a publicar sua estratégia.[34] Outros países como a Colômbia acabaram de publicar sua terceira edição da estratégia. Já o Uruguai – um dos países com mais alta taxa de acesso à Internet na região – não possui uma estratégia específica para a segurança cibernética, mas incorpora a pauta dentro de sua Agenda Digital, elaborada pela Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), deixando temas relacionados à ciberdefesa para serem incluídos na política de defesa

32 ENISA. National Cybersecurity Strategies. **ENISA**. s.d. Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies.

33 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.

34 OAS. Cybersecurity: Risks, Progress, and the way forward in Latin America and the Caribbean. **OAS**. 2020.

nacional. Tais diferenças reforçam o fato de que as estratégias de cibersegurança devem ser compreendidas em seus respectivos contextos de governança, e que, apesar de serem importantes indicadores de maturidade e capacidade de um país, não podem ser reduzidas a uma "checklist". Faz-se necessário, portanto, compreender como que cooperação, coordenação, comunicação e fortalecimento do conhecimento sobre o tema são operacionalizados dentro das estratégias.

"apesar de serem importantes indicadores de maturidade e capacidade de um país, [as estratégias] não podem ser reduzidas a uma "checklist"

O contexto

No dia 5 de fevereiro de 2020, o Brasil aprovou sua primeira Estratégia de Segurança Cibernética (E-Ciber). O documento estabelece as principais ações do governo (nacional e internacionalmente) na área de segurança cibernética entre os anos 2020-2023.

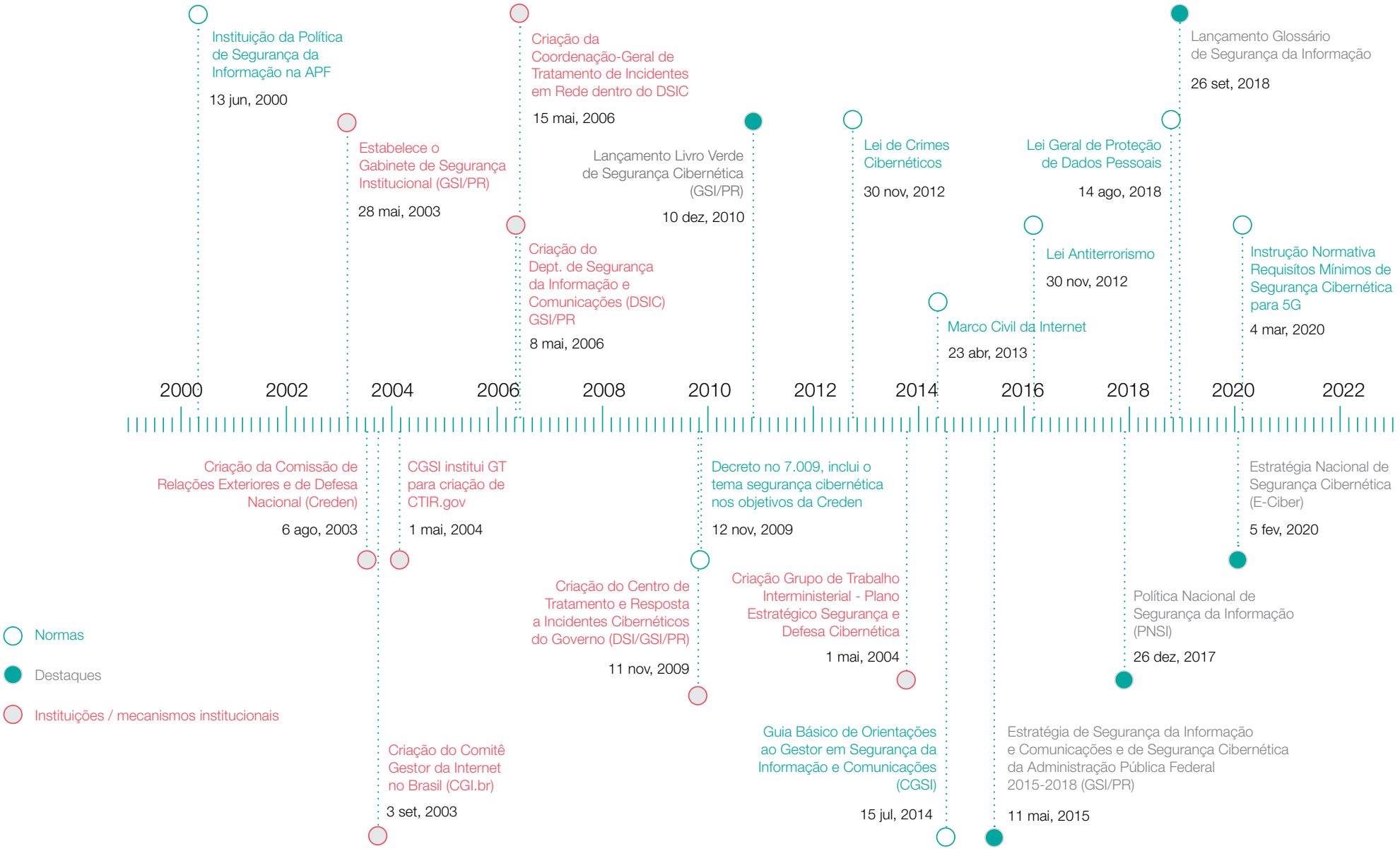
Contudo, este não é o primeiro esforço do governo em estabelecer competências, princípios e objetivos norteadores para a segurança cibernética. Desde meados dos anos 2000, o Brasil tem gradualmente introduzido o termo dentro de seu vocabulário político-estratégico por meio da publicação de inúmeros documentos (White Papers) tais como o Livro Verde da Segurança Cibernética (2010) e a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018. Diferentes órgãos da Administração Pública Federal também buscaram inserir as preocupações com a segurança em seus respectivos planejamentos. Esse é o caso da E-Digital, desenvolvida pelo Ministério da Ciência e Tecnologia e o Ministério das Comunicações, que incluiu a segurança e defesa cibernética, bem como crimes cibernéticos, dentro de um de seus eixos temáticos de confiança no ambiente digital.

Mas as ações relacionadas à segurança cibernética, apesar de crescentes, são pouco disseminadas entre os diferentes setores da sociedade. Com isso em mente, apresentamos abaixo duas linhas do tempo com os principais desenvolvimentos institucionais e políticos para a cibersegurança e defesa cibernética no Brasil.

Desde 2000, o governo tem desenvolvido instituições, políticas e diretrizes sobre segurança cibernética.[35] Começando com o conceito de segurança da informação e comunicações e gradualmente inserindo o conceito de segurança cibernética dentro da sua agenda de atuação.

35 Ver também: BRASIL. Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018. **Gabinete de Segurança Institucional da Presidência de República**. 2015.

Linha do Tempo: Segurança Cibernética no Brasil (Administração Pública Federal)



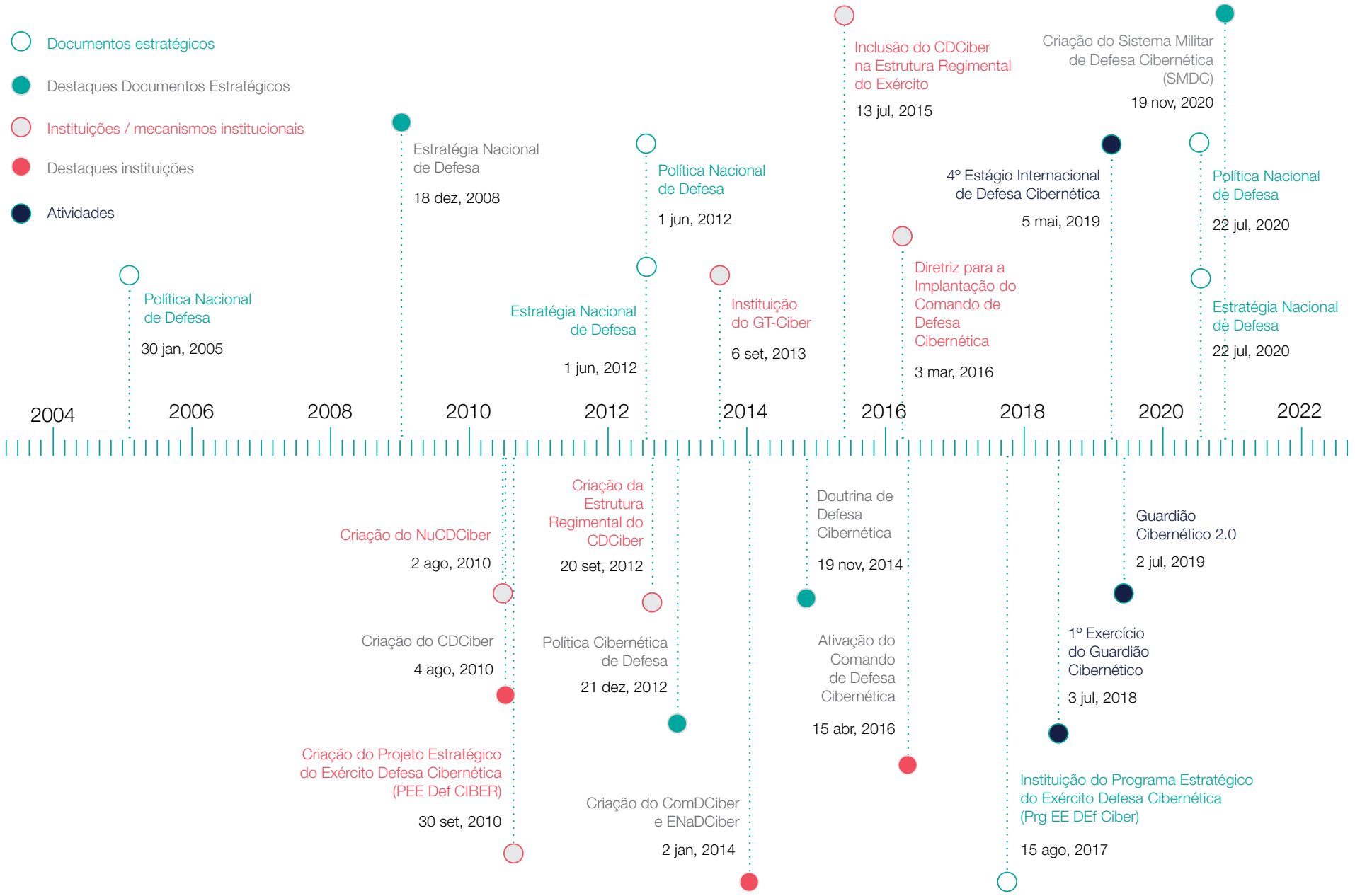
Ao passo que a linha do tempo retrata mais de duas décadas de trabalhos, na prática, o desenvolvimento de um arcabouço legislativo e normativo sobre segurança ganhou maior visibilidade e tração a partir de 2012/2013 com a Lei de Crimes Cibernéticos e as revelações do Edward Snowden — as quais contribuíram para a aprovação do Marco Civil da Internet. Desde então, observa-se uma transição dentro do panorama normativo/regulatório: um aprofundamento do vocabulário sobre segurança, no qual leis como a LGPD, por exemplo, trazem uma perspectiva de proteção de dados e segurança de dados; também observa-se um gradual avanço na consolidação de políticas setoriais, como a resolução do Banco Central sobre segurança cibernética para o mercado financeiro.[36]

Observa-se também que entre 2010 e 2020, o GSI apresentou uma série de documentos que gradualmente inseriram o conceito de segurança cibernética dentro de seu escopo de atuação. Isso inclui: a construção de uma proposta de visão estratégica (Livro Verde de Segurança Cibernética), uma reflexão sobre a relação entre segurança da informação e cibernética na Administração Pública Federal, um glossário de termos e, mais recentemente, a Política Nacional de Segurança da Informação (PNSI) e a E-Ciber.

Há mais de 10 anos, o Brasil investe no desenvolvimento de suas capacidades cibernéticas para defesa, tendo como marco inicial o reconhecimento do setor cibernético como um dos pilares estratégicos para a defesa nacional em 2008. De acordo com a Doutrina de Defesa Cibernética o termo se refere ao "conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de inteligência e comprometer os sistemas de informação do oponente".

36 Resolução 4.658, Banco Central do Brasil.

Linha do Tempo: Defesa Cibernética no Brasil



Conforme a linha do tempo acima retrata, observa-se uma concentração de esforços no período de 2010 à 2016 — momento de preparo para o ciclo de megaeventos sediados no país (Rio+20 sendo o primeiro e as Olimpíadas de 2016, o último). Outra tendência nesse período foi o desenvolvimento de documentos basilares para auxiliar e guiar a atuação estratégica do Brasil em operações cibernéticas (tal como a Política Cibernética de Defesa e a Doutrina de Defesa Cibernética) de instituições dedicadas à operacionalização e implementação de atividades de defesa cibernética (o Centro de Defesa Cibernética e o Comando de Defesa Cibernética).[37]

Por um lado, os megaeventos foram um importante propulsor para o investimento em segurança e defesa cibernética, resultando em maior capacitação de atores estratégicos. Para responder e se preparar para esses eventos, as Forças Armadas (e o Exército em especial) precisaram pensar em estruturas de coordenação em conjunto para a proteção de sistemas e redes durante os eventos. Isso resultou no estabelecimento de canais com órgãos com a Polícia Federal, CERT.br, CTIR.gov e entre outros.

Após os megaeventos, observa-se duas dinâmicas: (i) consolidação de programas e orçamentos para defesa cibernética e (ii) foco em coordenação intra-Ministério da Defesa — um exemplo sendo a aprovação do Sistema Militar de Defesa Cibernética em novembro de 2020 — e interagências, por meio de espaços e exercícios — um exemplo sendo o exercício do Guardião Cibernético.[38]

Contudo, apesar desse período ter resultado em maior coordenação e cooperação operacional, também deixou o legado de uma segurança cibernética militarizada, recebendo críticas tanto de grupos da sociedade civil quanto da academia.[39]

Próximos Passos

Com a E-Ciber publicada no início de 2020 e uma Política ou Lei Nacional de Segurança Cibernética (a ser lançada),[40] o Brasil tem a oportunidade de integrar a experiência desses órgãos e suas boas práticas de coordenação dentro de um panorama de conhecimentos e mecanismos de coordenação de outros setores.

Ao passo que essas diferentes iniciativas criam um ecossistema de abordagens para fortalecer a resiliência e segurança cibernética no país, pouco se fala sobre as sinergias ou lacunas existentes entre esses esforços. Conforme o ataque ao STJ em novembro de 2020 mostrou, a falta de preparo e cuidados básicos de atualização de sistemas podem gerar um impacto sem precedentes para o funcionamento de órgãos críticos para a democracia brasileira. É imprescindível, portanto, que a atenção advinda desses ataques sirva como um importante sinalizador não só da necessidade de se aprimorar os canais de respostas a incidentes, mas da necessidade de coordenação e alinhamento entre diferentes setores.

---

37 DINIZ, G.; MUGGAH, R.; GLENNY, M. Deconstructing cyber security in Brazil: Threats and responses. Rio de Janeiro: **Instituto Igarapé**, p. 3-32. (Strategic Paper 11). 2014;
HUREL, L. M. "Securitização e governança da Segurança Cibernética no Brasil". Em REIA, J.; FRANCISCO, P.A.P.; BARROS, M.; MAGRANI, E. (org.). **Horizonte presente: tecnologia e sociedade em Debate.** Belo Horizonte: Letramento. 2018.

38 https://www.eb.mil.br/web/imprensa/aviso-de-pauta/-/asset publisher/0004ie79MBVM/content/exercicio-guardiao-cibernetico-2-0.

39 Nota técnica da Sociedade Civil para a CPI de Crimes Cibernéticos. **Coding Rights e Instituto Beta para Internet e Democracia.** 2016. Disponível em: https://cpiciber.codingrights.org/crimes-ciberneticos/; ARTIGO 19. Da Cibersegurança à Ciberguerra - do desenvolvimento de políticas de vigilância no Brasil. **Artigo 19.** 2016. Disponível em: https://artigo19.org/blog/2016/03/10/da-ciberseguranca-a-ciberguerra-o-desenvolvimento-de-politicas-de-vigilancia-no-brasil/.

40 DE LUCA, C. "Após estratégia, GSI elabora a Política Nacional de Segurança Cibernética". **Tilt UOL**. 2020. Disponível em: https://porta23.blogosfera.uol.com.br/2020/02/09/apos-estrategia-gsi-elabora-a-politica-nacional-de-seguranca-cibernetica/.

A Lei Geral de Proteção de Dados (LGPD), representa um importante avanço na consolidação de provisões específicas sobre a segurança dos dados a empresas e às organizações do Estado. **A LGPD, no Art. 6, destaca *segurança* como um dos princípios essenciais para o tratamento de dados pessoais e a define como a** "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão". **Também exige que empresas adotem medidas de segurança técnicas e administrativas para a proteção contra incidentes (Art. 46), e determina que incidentes sejam comunicados à Autoridade Nacional de Proteção de Dados** e ao titular dos dados (Art. 48). Apesar das tentativas de se postergar a aplicabilidade da LGPD no contexto da pandemia, sua entrada em vigor em agosto de 2020 contribui para a consolidação de boas práticas para a segurança no tratamento, processamento, armazenamento e transmissão de dados pessoais.

No entanto, novos desafios se colocam para a segurança de dados. Esses desafios estão diretamente ligados ao amadurecimento do país em segurança cibernética, o qual inclui, por exemplo, o desenvolvimento de uma política para o compartilhamento de vulnerabilidades e incidentes dentro do setor público com prazos para a comunicação de incidentes e divulgação das vulnerabilidades.[41] O Reino Unido, por exemplo, publicou uma nota pública sobre suas ações para administração de vulnerabilidades. garantindo maior transparência e previsibilidade sobre a governança da segurança cibernética no país.[42]

A E-Ciber é o primeiro documento dedicado a desenvolver objetivos e ações para a consolidação da segurança cibernética no país e abre o caminho para uma reflexão sobre como integrar não só setores, mas harmonizar as diferentes legislações existentes por meio da consolidação de uma visão macropolítica para o país.

A estratégia

Seis dias antes do fim do governo do presidente Michel Temer, foi publicado o decreto aprovando a **Política Nacional de Segurança da Informação (PNSI) em dezembro de 2018.**[43] Após uma década de desenvolvimentos *ad hoc* e propostas para a consolidação de uma política nacional dedicada ao tema, a PNSI, traz consigo uma proposta de horizonte de desenvolvimento de estratégias para abordar temas específicos da Segurança da Informação. Desenvolvida pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR) — principal órgão designado para o desenvolvimento de políticas e diretrizes sobre o tema — **a PNSI prevê o estabelecimento de cinco estratégias: (i) segurança cibernética; (ii) defesa cibernética; (iii) segurança das infraestruturas críticas; (iv) segurança da informação sigilosa; e (v) proteção contra o vazamento de dados.**

A PNSI estabelece um horizonte estratégico para a segurança cibernética, garantindo positivamente algum grau de previsibilidade da atuação de órgãos como o GSI e outros nessa matéria em momento de instabilidade política e incerteza econômica. Mais do que isso, a PNSI prevê não só a **elaboração de estratégias, mas de planos nacionais para guiar a implementação de ações**

41 Atualmente, o Art.48 §1 afirma que a "comunicação [do incidente] será feita em prazo razoável, conforme definido pela autoridade nacional".

42 LEVY, I. Equities Process: Publication of the UK's process for how we handle vulnerabilities. **NCSC**. 2018. Disponível em: https://www.ncsc.gov.uk/blog-post/equities-process

43 Decreto n.9.637 de 26 de dezembro de 2018.

para a cibersegurança no país. No entanto, isso não é algo novo. A PNSI reflete recomendações previamente ressaltadas em outros documentos, mais especificamente, no Livro Verde de Segurança Cibernética de 2010. O Livro foi desenvolvido visando providenciar subsídios para a elaboração do que poderia vir a ser uma Política Nacional de Segurança Cibernética em um futuro próximo. Naquela época, o documento já notava que uma Política Nacional deveria "na medida do possível, ser precedida de análises e consensos construídos com a participação de *stakeholders* para a viabilização e otimização do processo como um todo, criando uma Agenda de Estado político-estratégica e técnica".[44] Apesar do hiato de dez anos entre o Livro Verde e a E-Ciber, pouco tempo após o lançamento da Estratégia, representantes do GSI já mencionavam que uma política estaria sendo desenvolvida.[45]

Em consonância com a PNSI, a E-Ciber foi o primeiro módulo a ser desenvolvido por ser considerada carro-chefe da abordagem do país em temas relacionados à segurança da informação. A Estratégia é o resultado de sete meses de trabalho, três grupos temáticos, 30 dias de reuniões fechadas e 20 dias de consultas públicas (166 contribuições). A E-Ciber adota uma metodologia similar à Estratégia Brasileira de Transformação Digital lançada, em 2018, desenhando eixos temáticos e transformadores para o diagnóstico do panorama nacional. O documento estabelece três objetivos estratégicos e dez ações estratégicas (Figura 1). Também inclui recomendações dentro do escopo das ações estratégicas com o objetivo de propor ações mais específicas.

Vale ressaltar que o processo de consulta pública é um importante passo para um órgão como o GSI e sinaliza uma abertura para incorporação de recomendações da sociedade, por meio de mecanismos transparentes e acessíveis de participação. Contudo, **esse é apenas um passo:** a consulta ficou aberta de 10 de setembro a 01 de outubro de 2019, proporcionando menos de 30 dias para que a sociedade pudesse contribuir com comentários. Como em outros casos de consulta pública, outra questão que se apresenta é a falta de transparência sobre como os comentários e contribuições foram incorporados no texto final. As consultas são um dentre diversos mecanismos disponíveis para processos de elaboração de políticas e diretrizes e o Brasil precisa garantir que a operacionalização e revisão das provisões da estratégia também proporcionem efetiva integração de diferentes setores.

44 MANDARINO, R. & CANONGIA, C. **Livro Verde de Segurança Cibernética**. GSI/DSI. 2010. (Página 25).

45 DE LUCA, C. "Após estratégia, GSI elabora a Política Nacional de Segurança Cibernética". **Tilt UOL**. 2020. Disponível em: https://porta23.blogosfera.uol.com.br/2020/02/09/apos-estrategia-gsi-elabora-a-politica-nacional-de-seguranca-cibernetica/.

Figura 1: Objetivos e Ações da E-Ciber

Objetivos Estratégicos	Eixos Temáticos	Ações Estratégicas[46]
1. Tornar o Brasil mais próspero e confiável no ambiente digital 2. Aumentar a resiliência brasileira às ameaças cibernéticas 3. Fortalecer a atuação brasileira em segurança cibernética no cenário internacional	**Proteção e Segurança** • Governança da Segurança Cibernética Nacional (1.1)[47] • Proteção e mitigação de ameaças cibernéticas (1.2) • Proteção estratégica (1.3) **Transformadores** • Dimensão Normativa (2.1) • Pesquisa, Desenvolvimento e Inovação (2.2) • Internacional (2.3) • Educação (2.4)	1. Fortalecer as ações de governança cibernética 2. Estabelecer um modelo centralizado de governança no âmbito nacional 3. Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade 4. Elevar o nível de proteção do governo 5. Elevar o nível de proteção das Infraestruturas Críticas Nacionais 6. Aprimorar o arcabouço legal sobre segurança cibernética 7. Incentivar a concepção de soluções inovadoras em segurança cibernética 8. Ampliar a cooperação internacional do Brasil em Segurança cibernética 9. Ampliar parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade 10. Elevar nível de maturidade em segurança cibernética

46 Numeração incluída nas Ações Estratégicas para fins da análise e referência. No texto original, as ações estratégicas foram numeradas de forma diferente. Aqui adotamos uma numeração simplificada para facilitar o acesso. Para uma visão mais detalhada das ações estratégicas e suas respectivas recomendações, ver Anexo 1.

47 Numeração de acordo com o texto da E-Ciber.

O Gabinete de Segurança Institucional, responsável pelo desenvolvimento da E-Ciber e da política nacional de segurança cibernética, também foi destacado no texto da E-Ciber como o facilitador da coordenação entre diferentes setores e dentro da Administração Pública Federal (APF). Nesse sentido, consideráveis desafios permanecem tanto para o papel do GSI quanto para a implementação da E-Ciber. Por mais que o GSI já desempenhe a função de coordenação e facilitação na APF, sua relação com a sociedade civil permanece frágil, com grupos frequentemente apontando para a falta de transparência e militarização da agenda do Departamento de Segurança da Informação do GSI. Este é um obstáculo considerável para o desenvolvimento de uma visão sobre segurança que precisa englobar toda a sociedade.[48] Novos canais formais e informais poderão auxiliar na construção de confiança entre as diferentes partes, mas a implementação das ações e alcance dos objetivos, como por exemplo, o estabelecimento de um Conselho Nacional com diferentes setores (previsto na E-Ciber), é marcada por grande ceticismo. A efetivação da E-ciber requererá um esforço contínuo de todas as partes.

A Estratégia também recebeu críticas por ser mais um diagnóstico do cenário da cibersegurança no país ou até "uma carta de boas intenções" — algo que o Livro Verde de Segurança Cibernética já teria realizado em 2010 — do que um documento operacional com direcionamento e metas claras de implementação.

Apesar da E-Ciber buscar "representar o pensamento do governo federal sobre" essa área temática,[49] permanecem indefinidos os horizontes de implementação e acompanhamento da Estratégia. A Estratégia do Reino Unido, por exemplo, apesar de também apresentar um diagnóstico do estado da arte e do ambiente estratégico, o documento inclui claras indicações sobre "planos de implementação", "avaliação de resultados" e "objetivos e princípios" norteadores que informam a relação do governo com outros setores.[50]

48 Também chamado de "whole-of-society" ou "whole of nation approach" em Inglês. Klimburg (2011) argumenta que o poder cibernético de uma nação é composto por três dimensões: coordenação de aspectos políticos-normativos e operacionais entre agências governamentais, coerência de políticas por meio de alianças internacionais e "frameworks" legais e cooperação com atores não estatais. Esses atores não estatais (setor privado e sociedade civil) possuem grande parte das capacidades e a proximidade com as diferentes realidades e riscos de diferentes partes da sociedade. Reunir esses diferentes setores não é simplesmente uma medida de inclusão, mas, conforme aponta Klimburg (2011), é o fundamento de uma "whole of nation approach" e esse é, por conseguinte, um elemento central para a definição do poder cibernético de um país. Dessa forma, para além de capacidades operacionais e normativas, "poder" é determinado pela capacidade do Estado de interagir, integrar e aprender com esses setores para formar seu posicionamento.
KLIMBURG, A. Mobilising Cyber Power. **Survival**. v.53, n.1, p.41-60. DOI: 10.1080/00396338.2011.555595.

49 Cyber Security Summit Brasil. Disponível em: https://www.youtube.com/watch?v=TUv4wcfb-AY

50 UK. National Cyber Security Strategy 2016-2021. P. 9 (versão em português). Disponível em: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

Dimensões da Governança da Cibersegurança[51, 52]

Nessa seção, apresentamos uma análise da E-Ciber (ações estratégicas e recomendações) de acordo com as cinco dimensões da governança da cibersegurança: **cooperação, capacitação, coordenação, integração de conhecimentos e sustentabilidade de esforços**. A partir de uma análise temática do documento, observa-se que que grande parte das ações estratégicas e recomendações dialogam com diferentes dimensões da governança da cibersegurança. A ***cooperação*** e a ***sustentabilidade de esforços*** se destacam como os elementos transversais da Estratégia. A dimensão de ***coordenação***, no entanto, destaca-se por apresentar ações mais concretas, apontando para os possíveis desdobramentos práticos da E-Ciber no âmbito legislativo e reforçando o papel do GSI e outras instituições na atuação em temas associados à cibersegurança. Por fim, as recomendações associadas à ***capacitação*** e à ***integração de conhecimentos*** introduzem sugestões principiológicas associadas à adoção de padrões tecnológicos, bem como à proposição de espaços e modelos para facilitar a integração de outros setores no debate sobre cibersegurança.

Cooperação

Se refere à troca ou trabalho entre diferentes partes com uma finalidade comum. Neste caso, remete, por exemplo, tanto a acordos, planos, cooperação operacional, como ao desenvolvimento de mecanismos para aprimoramento do trabalho entre setores, ministérios e agências dentro e fora da administração pública federal, bem como práticas (formais e informais) de colaboração entre atores.

Cooperação Nacional

A Estratégia apresenta duas dimensões da cooperação na área de segurança cibernética: nacional e internacional. No *âmbito nacional*, o documento ressalta a necessidade de se estabelecer canais de **compartilhamento de informações,** tanto dentro da APF quanto entre o setor público e privado, sobre incidentes, vulnerabilidades cibernéticas e riscos cibernéticos.[53] No que diz respeito à APF, o compartilhamento de dados está regulado pelo Decreto 10.046 de 2019, que dispõe sobre a governança no compartilhamento de dados. Mais especificamente, o Decreto estabelece níveis de compartilhamento de dados (amplo, restrito e específico), de acordo com a sua confidencialidade. Parâmetros como estes podem e devem informar o desenvolvimento de práticas específicas sobre incidentes e vulnerabilidades identificadas em diferentes órgãos da APF. Apesar do caráter sensível de informações como essas, isso não pode ser um empecilho para que as recomendações estabelecidas pela E-Ciber sejam alcançadas.

51 As ações estratégicas foram alocadas para cada dimensão de acordo com dois critérios: menção explícita dos elementos previstos na definição da dimensão na descrição da ação estratégica e/ou nas iniciativas sugeridas e identificadas em cada uma das ações estratégicas.

52 Os eixos temáticos foram alocados para cada dimensão, de acordo com a sua relação com as definições das dimensões. Nem todos os elementos incluídos em "eixos temáticos" são recomendações explícitas, mas são sugestões para o desenvolvimento de cada eixo.

53 Ações estratégicas que incluem recomendações explícitas sobre o compartilhamento de informações: AE3 (estimular o compartilhamento de informações sobre incidentes e vulnerabilidades cibernéticas; estabelecer mecanismos que permitam a interação e o compartilhamento de informações em diferentes níveis) e AE9 (incentivar a criação de mecanismos de compartilhamento de informações sobre riscos cibernéticos).

No entanto, dois desafios se apresentam para a concretização dos objetivos associados ao compartilhamento de informações. O primeiro se refere ao fato de que o compartilhamento de vulnerabilidades e informações relacionadas a incidentes não é uma prática consolidada na APF. Pode-se apontar diversas razões para isso: ausência de redes de confiança, falta de claros mecanismos para compartilhamento, inexistência de pontos de contato designados para o recebimento e interlocução com diferentes órgãos e de recursos para se estabelecer equipes específicas para lidar com segurança cibernética e informação. Porém, conforme os ataques ao STJ em novembro de 2020 mostram, os custos e impactos **da falta de protocolos nacionais para compartilhamento de informações sobre incidentes pode ferir o próprio funcionamento das instituições democráticas do país.**

O segundo desafio é que ainda **não existem normas amplamente adotadas sobre o compartilhamento de informações sobre incidentes e vulnerabilidades entre o setor público e o setor privado**. Isso é preocupante, pois muitas empresas não só possuem conhecimento e capacidades para detectarem ameaças (threat landscape), mas muitas das infraestruturas críticas do país dependem de tecnologias dessas empresas. A não inclusão do setor privado contribui para o aumento da lacuna de conhecimento sobre ameaças por parte do setor público, diminuindo sua capacidade de responder adequadamente a incidentes.

O compartilhamento de informações pode ser fortalecido tanto por meio do estabelecimento de políticas específicas, como por protocolos setoriais. No setor financeiro, por exemplo, a Resolução do Banco Central (BACEN) 4.658 de 2018 determina que as instituições financeiras devem desenvolver iniciativas para o compartilhamento de informações sobre incidentes — considerando o dever de sigilo e a livre concorrência. No âmbito internacional, o *Financial Services Information Sharing and Analysis Center* (FS-ISAC) é um exemplo de uma organização dedicada ao compartilhamento de informação para redução de riscos cibernéticos dentro do setor.

No caso de incidentes cibernéticos e identificação de vulnerabilidades, a designação de níveis para o compartilhamento pode ser algo a se considerar para criar confiança entre órgãos e setores. Essa é uma prática já estabelecida em organizações internacionalmente reconhecidas, como o FS-ISAC ou o Fórum de Respostas a Incidentes Cibernéticos (FIRST Org). Em ambos os casos, os membros das organizações utilizam o *Traffic Light Protocol* para sinalizar o grau de compartilhamento de uma determinada informação por meio de cores (vermelho, amarelo, verde e branco).[54]

O estabelecimento de políticas específicas sobre publicação de vulnerabilidades ("vulnerability disclosure")[55] também pode contribuir não só para o fortalecimento de resiliência dos serviços e atividades do governo, mas incentivar a colaboração entre órgãos da APF com o intuito de monitorar e consolidar informações sobre o panorama de ameaças na APF**. Boas práticas de compartilhamento de informações aliadas à publicação de vulnerabilidades, também podem ser um instrumento importante para garantir maior transparência sobre os processos associados à segurança cibernética**, bem como construir confiança com a sociedade ao estabelecer canais constantes de prestação de contas[56]

54 No caso do FIRST, a página com a descrição detalhada do TLP pode ser encontrada aqui: https://www.first.org/tlp/ ; Já o FS-ISAC inclui o TLP como elemento fundacional para o seu "modelo de confiança" e pode ser acessado aqui: https://www.fsisac.com/tlp . Organizações como o CTIR Gov e o CERT.br utilizam o TLP como protocolo para classificação de informações.

55 O ato de providenciar informações sobre vulnerabilidades a uma terceira parte que não estava previamente ciente do fato. O indivíduo ou organização que conduz esse ato é chamado de *relator* (tradução livre extraída do: https://cyber.dhs.gov/bod/20-01/. A definição foi retirada da ISO/IEC 29147:2018).

56 Alguns exemplos de práticas instituídas por governos sobre "vulnerability disclosure" são o *Vulnerability Disclosure Toolkit* lançado pelo National Cybersecurity Centre (NCSC) do Reino Unido e as recomendações da Cybersecurity and Infrastructure Security Agency (CISA) dos EUA sobre a publicação e desenvolvimento de uma política de "vulnerability disclosure."

Cooperação internacional

A E-Ciber avança ao trazer uma ação estratégica específica sobre a **cooperação e atuação internacional do Brasil em segurança cibernética**. Pouco se discute sobre a ciberdiplomacia no país, em grande parte por ser recente (tanto em termos de campo prática). Países têm adotado estratégias diferentes para consolidar suas políticas externas nessa área, com a publicação de documentos destacando seu posicionamento internacionalmente.[57] A E-Ciber abre espaço para uma visão mais robusta sobre o futuro da ciberdiplomacia ao reconhecer a cooperação internacional nessa área e destacar recomendações específicas para o tema.

No âmbito da cooperação internacional, a E-Ciber ressalta atividades que incluem exercícios internacionais, colaboração em crimes cibernéticos e consolidação de uma política externa do país sobre o tema. No caso dos exercícios, o ComDCiber participou em 2019 do 4º Estágio Internacional de Defesa Cibernética que reuniu militares de dez países.[58] O Brasil tem atuado de diferentes formas no campo do combate a crimes cibernéticos, por exemplo, participando de grupos especializados em crimes cibernéticos em instâncias como a Organização dos Estados Americanos (OAS) e na Europol, Ameripol e Interpol.[59]

Um importante avanço para a cooperação internacional é a adesão do Brasil à Convenção de Budapeste. O processo ganhou tração em julho de 2019 e, em dezembro do mesmo ano, o Ministério das Relações Exteriores (MRE) e o Ministério da Justiça e Segurança Pública publicaram uma nota anunciando seu início. Em julho de 2020, o texto foi finalmente encaminhado para o Senado.[60] O avanço do processo de adesão vai ao encontro das medidas recomendadas pela E-Ciber de "ampliar o uso de mecanismos internacionais de combate aos crimes cibernéticos".

O MRE tem aumentado gradualmente seu envolvimento em temas relacionados à cibersegurança. Em 2020, o Brasil destacou seu primeiro ciberdiplomata, encarregado de acompanhar pautas nacionais e internacionais associadas ao tema. Atualmente, diversos países já designaram diplomatas e destacaram grupos dentro dos ministérios para representarem os interesses nacionais na governança global da segurança cibernética. Alguns desses espaços incluem: o United Nations Group of Governmental Experts (UNGGE) e o Open-Ended Working Group on the Developments in the Field of ICTs in the Context of International Security. Outros países, como a Dinamarca, apontaram o primeiro diplomata para grandes empresas de tecnologia.

No ambiente multilateral, **o Brasil foi o segundo país a servir como moderador do UNGGE mais de uma vez**. Estabelecido em 1999, o UNGGE é um dos principais espaços

57 A Austrália, por exemplo, destacou seu primeiro ciberdiplomata em 2017 e publicou, no mesmo ano, uma estratégia específica para a atuação do país internacionalmente intitulada "Australia's International Cyber Engagement Strategy". O documento cobre áreas como cibersegurança, crimes cibernéticos, comércio digital, governança da internet, entre outros em 2019, o país não só publicou um relatório de acompanhamento da implementação da estratégia, bem como seu posicionamento sobre a aplicabilidade do direito internacional no ciberespaço.

58 ASCOM. Competição virtual envolve militares de dez países durante Estágio Internacional de Defesa Cibernética. **Ministério da Defesa**. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/noticias/ultimas-noticias/competicao-virtual-envolve-militares-de-dez-paises-durante-estagio-internacional-de-defesa-cibernetica.

59 OAS/GCSCC. **Cybersecurity Capacity Review**: Federative Republic of Brazil. Organization of the American States. 2020. Disponível em: http://www.oas.org/en/sms/cicte/docs/ENG-CYBERSECURITY-CAPACITY-REVIEW-BRAZIL.pdf.

60 https://www.in.gov.br/en/web/dou/-/despachos-do-presidente-da-republica-268441788.

internacionais para o debate sobre a paz e segurança no ciberespaço – com ênfase no comportamento responsável de Estados. No nível regional[61], o país participa do grupo de trabalho para Medidas de Construção de Confiança (CBMs)[62] em cibersegurança, estabelecido em 2017 no âmbito do Comitê Interamericano contra o Terrorismo da Organização dos Estados Americanos.[63] Em 2018 e 2019, o grupo acordou que Estados-membro designariam um ponto de contato para discutir as implicações de ameaças cibernéticas hemisféricas e para facilitar o trabalho em cooperação internacional nessa área.[64]

Apesar da crescente inserção do Brasil em fóruns de diálogos internacionais, existem outras dimensões desse objetivo estratégico que merecem maior atenção e acompanhamento, tal **como "ampliar acordos de cooperação em segurança cibernética" e "promover eventos e exercícios internacionais sobre segurança cibernética"**[65]. Desde 2013, diversas declarações conjuntas e planos de ações do Brasil têm incluído segurança, defesa cibernética, crimes cibernéticos e preservação dos direitos humanos como pilares importantes para a cooperação bilateral. Contudo, pouco se sabe sobre o andamento dessas colaborações.

Conforme o país expanda sua atuação em espaços sobre cibersegurança, outros setores poderão auxiliar na consolidação da política externa nesse tema. O Reino Unido, por exemplo, estabeleceu um Comitê Multissetorial Consultivo para informar a ciberdiplomacia do país. No Brasil, a Anatel, possui Comissões Brasileiras de Comunicação (CBC)[66] que estão "encarregadas de organizar os trabalhos nos foros internacionais de telecomunicações" — uma delas dedica-se à Governança e Regimes Internacionais. Ações como essas podem aprimorar a integração de conhecimentos, reunir especialistas e ampliar a colaboração na construção de uma política externa sobre o tema, fortalecer canais para a cooperação internacional.

Capacitação

Inclui elementos como a formação e treinamento em segurança cibernética e as ações destacadas para elevar o grau de capacidades em responder a ameaças cibernéticas. O estabelecimento de protocolos de compartilhamento de informação e de vulnerabilidade, entre agências do governo e com outros setores, são alguns exemplos de boas práticas adotadas por diferentes países, que viabilizam a circulação e comunicação de conhecimentos para o desenvolvimento informado de respostas a ameaças.

As ***ações estratégicas***[67] da E-Ciber destacam três prioridades para a **capacitação** da sociedade em cibersegurança: (i) a adesão a padrões tecnológicos (AE1); (ii) o desenvolvimento e atualização de normas para facilitar respostas a incidentes e crimes cibernéticos (AE6); (iii) o investimento no conhecimento e preparo de equipes e setores frente a riscos cibernéticos (AE7).

---

61 OAS/IDB. Cybersecurity: Risks, Progress, and the way forward in Latin America and the Caribbean. Organization of the American States. 2020. Report.

62 Confidence-Building Measures, em Inglês.

63 http://www.oas.org/en/sms/cicte/Documents/Sessions/2018/FINAL/RES%201%20Resolución%20Medidas%20Regionales%20de%20Fomento%20CICTE01217E.doc.

64 CICTE/RES.1/18 e CICTE/RES.1/19

65 Trecho retirado da E-Ciber.

66 https://antigo.anatel.gov.br/institucional/comissoes-brasileiras-de-comunicacao-cbcs

67 Em especial, a AE1 (Fortalecer as ações de governança cibernética), AE6 (Aprimorar o arcabouço legal sobre segurança cibernética) e AE7 (Incentivar a concepção de soluções inovadoras em segurança cibernética).

Padrões

Padrões tecnológicos são elementos fundamentais para a interoperabilidade e segurança de sistemas e redes. Mais do que isso, padrões em geral moldam não só o mundo físico e virtual, mas também as nossas relações sociais e a nossa forma de ver o mundo e a segurança de tecnologias.[68] Esse é o caso da criptografia. A ampla adoção de padrões criptográficos pelos setores público e privado é capaz de promover maior confiabilidade da população e dos gestores sobre a segurança de um sistema. De acordo com o *Cybersecurity Capacity Review,* lançado pela Universidade de Oxford, diferentes setores no Brasil já adotam diferentes padrões de segurança da informação e cibersegurança — sendo os setores financeiro e de comunicações eletrônicas os pioneiros.

A Estratégia destaca **três pontos** que devem compor o horizonte de prioridades para a inserção, investimento e adesão do Brasil a padrões que elevem o nível de cibersegurança do país.

O primeiro se refere ***à necessidade de se estabelecer* requisitos mínimos de segurança cibernética no contexto de contratações**. Ao longo dos últimos anos, o Brasil tem desenvolvido políticas e diretrizes setoriais que, apesar de cada vez mais frequentes, ainda precisam ser melhor integradas com uma visão estratégica. Esse é o caso da resolução 4.658 do Banco Central, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem que devem ser observadas pelas instituições financeiras. A resolução foi um importante passo para o estabelecimento de um critério mínimo de segurança no setor financeiro, mas foi criticada pelo desafio que apresentaria para organizações menores que não possuem recursos, capacidades ou expertise para atender à demandas específicas, como o estabelecimento de planos de resposta a incidentes (Art. 6) ou a garantia da confidencialidade, integridade e disponibilidade dos dados e informações processados ou armazenados pelo prestador de serviços (Art. 12). Apesar dos desafios, o governo publicou em dezembro de 2020 o "Guia de Boas Práticas para Especificação de Requisitos de Segurança da Informação e Privacidade em Contratações de Tecnologia da Informação", para auxiliar instituições públicas na especificação de requisitos mínimos em soluções tecnológicas e a incorporação de segurança cibernética, segurança da informação e proteção de dados em processos de contratação de produtos e serviços.

O segundo, e talvez o principal avanço da E-Ciber, foi o **reconhecimento da criptografia como um elemento central para a realização de diversas ações estratégicas**. Mais especificamente, ela ressalta a necessidade de se incentivar o desenvolvimento de competências e soluções em criptografia e estimular o uso da criptografia no âmbito da sociedade em geral e para a comunicação de assuntos considerados sensíveis. Contudo, grandes desafios permanecem para tornar isso uma prática. O histórico conturbado do debate público sobre criptografia no país é marcado pelos "bloqueios do WhatsApp" de 2014[69] e uma tensão constante entre o acesso a dados por forças policiais e de investigação e o fortalecimento da segurança da informação por meio da implementação da criptografia.[70] Ao passo que países como o Reino Unido, EUA e Austrália

68 BUSCH, L. **Standards**: Recipes for Reality. Cambridge: MIT Press. 2011.

69 O aplicativo de mensageria privada, WhatsApp foi alvo de quatro decisões judiciais que pediam o bloqueio do aplicativo por se recusar a entregar conteúdo de comunicações que faziam parte de inquéritos e processos penais. Conforme apontado por Jacqueline Abreu (2017:27), "Trata-se de um conflito entre poderes tradicionais do Estado, de investigar e punir por meio do processo penal, e os crescentes poderes informacionais, de criar e facilitar espaços de comunicação e exercício de liberdades, de grandes corporações."; ABREU, J. **Passado, presente e futuro da criptografia forte**: desenvolvimento tecnológico e a regulação. Revista Brasileira de Políticas Públicas. v. 7, n.3. 2017.

70 ABDELSON, H; ANDERSON, R.; BELLOVIN, S.M.; BENALOH, J.; BLAZE, M.; DIFFIE, W.; GILMORE, J.; GREEN, M.; LANDAU, S.; NEUMANN, P.G.; RIVEST, R.L.; SCHILLER, J.I.; SCHNEIER, B.; SPECTER, M.; WEITZNER, D.J. (2015**). Keys Under Doormats**: Mandating insecurity

se posicionam a favor do acesso excepcional para fins de persecução criminal, o Brasil não impôs restrições normativas ou regulações para o desenvolvimento da criptografia no país. Pelo contrário, conforme o relatório do IP.rec (Instituto de Pesquisa em Direito e Tecnologia de Recife) aponta, "a Infraestrutura Brasileira de Chaves Públicas (ICP-Brasil), órgão público instituído pela Medida Provisória nº 2.200-2/2001, estabelece quais são os algoritmos e padrões mínimos de segurança recomendados para o emprego de tecnologias de criptografia em território nacional. Se não há regulação, há uma agenda que promove o emprego de técnicas progressistas e cada vez mais avançadas".[71] Apesar disso, em 2020, pesquisadores descobriram que durante 60 anos o Exército, o Itamaraty e a Marinha utilizavam equipamentos e serviços fornecidos pela empresa Crypto AG, ligada à agência de inteligência estadunidense (CIA), que inseriram falhas nos códigos para acessar mensagens por meio de um *backdoor*[72] o que ressalta o desnível entre o comprometimento com altos padrões de segurança cibernética e da informação vis à vis as práticas de implementação de padrões criptográficos.

Por fim, a terceira e última dimensão de capacitação ressaltada pela Estratégia foi a **importância da interoperabilidade internacional**. O esforço de se elevar o nível de maturidade do Brasil depende da adesão a padrões internacionais que permitam maior interoperabilidade não só no âmbito técnico, mas no compartilhamento de metodologias para análises de riscos digitais. Conforme o diagnóstico da E-Ciber, "verificou-se que a adoção de padrões únicos e excludentes de governança não produziriam necessariamente resultados positivos, ao considerar a transversalidade e a capilaridade das ações de segurança cibernética nas instituições públicas e privadas e na sociedade em geral." A Estratégia avança nesse aspecto ao apresentar uma gama de padrões que vão desde mais técnicos (criptografia e *common vulnerabilities exposure*) até principiológicos (*privacy by design* e *privacy by default*), profissionais (capacitação por meio de certificações internacionais em cibersegurança) e metodológicos (*frameworks* para avaliação de riscos). No entanto, apesar de trazer exemplos de padrões internacionais e experiências nacionais, não apresenta de forma clara e objetiva as diferentes ações para se atingir esses objetivos. Por meio das recomendações, retorna a um modelo de "lista de intenções" e falha em comunicar efetivamente como o governo irá apoiar esses processos. Apesar dos objetivos estarem mais direcionados à APF, eles só poderão ser atingidos por meio do estabelecimento de diálogo e confiança interagências e multissetorial.

Como há diferentes níveis de maturidade e recursos, é importante que a visão estratégica de adesão à padrões seja acompanhada de investimentos em programas educacionais e planos de investimento tanto para o nível federal como para o estadual — tal como o estabelecimento de metas claras para a implementação de padrões (critérios mínimos de segurança), em um determinado período de tempo.

---

by requiring government access to all data and communications. Cambridge, 2015. Disponível em https://dspace.mit.edu/handle/1721.1/97690.

71 RAMIRO, A.; CANTO, M.; LIMA, J.P. & AGUIAR, T. **O Mosaico Legislativo da Criptografia no Brasil:** uma análise de projetos de lei**.** Instituto de Pesquisa em Direito e Tecnologia do Recife. 2020. Disponível em: https://ip.rec.br/publicacao/o-mosaico-legislativo-da-criptografia-no-brasil-uma-analise-de-projetos-de-lei/.

72 BRUSTOLIN, V.; DE OLIVEIRA, D. & PERON A.E.R. Exploring the relationship between crypto AG and the CIA in the use of rigged encryption machines for espionage in Brazil, **Cambridge Review of International Affairs.** 2020**.** DOI: 10.1080/09557571.2020.1842328.

Para elaborar esse plano, ***é importante estabelecer os padrões mínimos, com as adaptações necessárias para as realidades de diferentes órgãos, realizar um diagnóstico que mostre a atual*** situação dos órgãos e estados e desenvolver um plano de implementação com definição de prioridades para curto, médio, e longo prazo.

Outras possibilidades imediatas incluem a definição de métricas de adesão a padrões entre os órgãos da APF, por exemplo. Medidas como essas poderiam trazer maior concretude para processos de acompanhamento e avaliação de progresso em relação aos objetivos estratégicos traçados. Caso contrário, em 2023 (o último ano da E-Ciber), o governo não terá métricas específicas para avaliar o avanço real em relação aos objetivos e ações estratégicas.

Normas

A Estratégia dedica uma ação inteira ao aprimoramento do arcabouço legal vigente sobre segurança cibernética (AE6)[73]. Das seis recomendações elencadas na ação estratégica, três estão diretamente relacionadas ao desenvolvimento de capacidades: **a identificação de lacunas na legislação vigente, realização de esforços para incluir novas tipificações de crimes cibernéticos e elaboração de normativos sobre tecnologias emergentes.** Ao mesmo tempo em que o interesse e atenção a temas relacionados a crimes cibernéticos, segurança da informação e cibersegurança ganham notoriedade, pouco se discute a capacitação de formuladores de políticas públicas e legisladores para atuar nos temas.

Conhecimento e preparo de equipes e setores

Além da capacitação de formuladores de políticas e tomadores de decisão, a Estratégia também apresentou, no contexto de uma de suas ações estratégicas[74], recomendações para o setor privado e para a sociedade. Para os setores público e privado, destacou a necessidade de atividades como a organização de campanhas de conscientização internas e profissionalização de funcionários para atuarem no combate aos crimes cibernéticos. Grande parte das recomendações direcionadas à sociedade se concentram no fortalecimento da educação e formação em segurança cibernética, desde a educação infantil até a pós-graduação.

Dois pontos merecem atenção: a inclusão de uma visão interdisciplinar da segurança cibernética, inclusive nas ciências humanas, nos programas educacionais e profissionalizantes, e o papel nos programas educacionais e profissionalizantes e o papel da sociedade civil no processo de capacitação em segurança cibernética. No primeiro caso, maior clareza sobre a integração de conhecimentos no processo de capacitação é fundamental para que atores do setor público, setor privado, academia e sociedade civil estejam preparados para compreender as dinâmicas geopolíticas, sociais, econômicas e legislativas, nas quais tecnologias e práticas de segurança (nacional, individual, social) se desenvolvem. No segundo caso, a E-ciber não se refere à "sociedade civil", somente à "sociedade" ou "sociedade em geral". ***É importante ressaltar que*** grupos da sociedade civil têm desempenhado um importante papel de organizadores de programas, cursos e campanhas de conscientização em segurança digital para grupos de risco, comunidades vulneráveis, jornalistas investigativos, entre outras parcelas da população.[75] O reconhecimento desse papel pode fortalecer a dimensão de capacitação.

73 Ação estratégica 6: Aprimorar o arcabouço legal sobre segurança cibernética.

74 Ação estratégica 10: Elevar o nível de maturidade da sociedade em segurança cibernética; Ação estratégica 9: Ampliar a parceria em segurança cibernética entre o setor público, setor privado, academia e sociedade.

75 https://www.codingrights.org/safermanas-dicas-de-seguranca-digital-em-gifs/. https://festival3i.org/mesa/seguranca-digital-para-jornalistas/. https://new.safernet.org.br/content/seguran%C3%A7a-digital#. Para exemplos internacionais, a Access Now desenvolveu uma linha de ajuda em segurança digital disponível em nove idiomas: https://www.accessnow.org/help-pt/.

Coordenação

Estabelecimento de canais, pontos de contato, boas práticas, protocolos e/ou outros mecanismos para coordenação de atividades ligadas à segurança cibernética. Tal coordenação é potencializada em contextos institucionais com responsabilidades e papéis claros, bem como mecanismos específicos intra e interagências e multissetoriais.

A visão de **coordenação** desenvolvida pela E-Ciber concentra-se no **estabelecimento de um modelo centralizado de governança nacional** (AE2). O modelo de governança terá por objetivo promover a coordenação de atores para além da APF; promover análise conjunta de desafios; auxiliar na formulação de políticas públicas; criar grupos de debate, entre outras competências.

A Ação Estratégica apresenta recomendações concretas e mais detalhadas sobre as mudanças necessárias para que o governo possa consolidar um modelo nacional para abordar o tema. Entre elas, está a **legitimação do GSI como o principal ator responsável pela "coordenação da segurança cibernética em âmbito nacional, que possibilite a atuação de modo amplo, cooperativo, participativo, e alinhado com as ações de defesa cibernética, a cargo do Ministério da Defesa".** Conforme apontado anteriormente, o GSI já desempenha uma função de facilitador e coordenador entre órgãos da APF em pautas relacionadas à cibersegurança.

No entanto, a E-Ciber traz novos objetivos e escopo para a atuação do órgão, ao recomendar que o mesmo crie e coordene grupos de debate em diferentes setores com o objetivo de fomentar discussões "por meio de mecanismos informais de participação". Também recomenda o **estabelecimento de um Conselho Nacional de Segurança Cibernética** "que congregue diversos atores estatais e não estatais, com o objetivo de pensar a segurança cibernética sob um prisma abrangente, inclusivo, moderno e com ênfase nas reais necessidades nacionais". **De acordo com o documento, sua criação deverá ser incluída em um anteprojeto de lei sobre o tema**. A redação da lei ficará à cargo do GSI e deverá estabelecer diretrizes para o alinhamento macroestratégico e "contribuir de forma decisiva para elevar a segurança das organizações e dos cidadãos". A expectativa é que órgãos públicos e privados possam participar — uma vez aderindo a certos critérios a serem definidos.[76] Contudo, **muitas incertezas permanecem sobre a funcionalidade e o impacto desses mecanismos** — ainda que em formato de propostas. Ainda maiores são as incertezas sobre a contribuição da sociedade civil e da academia nesses processos.

A lei poderá introduzir incentivos para a consolidação de uma cultura de segurança que alcance toda a sociedade. Isso inclui protocolos de compartilhamento de informações, princípios para a cibersegurança no país, entre outros pontos. Contudo, a E-Ciber pré-anuncia uma lei que poderá estabelecer um Sistema Nacional de Segurança Cibernética, um Conselho Nacional e confirmar o papel do GSI enquanto o principal ator responsável pela coordenação de esforços e elaboração de políticas nessa área.

Por mais bem intencionada que seja a tentativa de se estabelecer uma lei de segurança cibernética, um contexto de polarização, desinformação e instabilidade política pode colocar em xeque essas tentativas. A confusão de conceitos associados a crimes cibernéticos e desinformação podem levar a uma reconfiguração de um projeto de lei. Isso se torna mais preocupante quando considera-se o que poderia ser enquadrado dentro da regulação de "ações de segurança cibernética" e especificação de

76 Cyber Security Summit Brasil. Disponível em: https://www.youtube.com/watch?v=TUv4wcfb-AY.

"atribuições".[77] **É importante que políticos compreendam, mais do que nunca, as distinções entre segurança cibernética, crimes cibernéticos, defesa cibernética e outros termos associados.** A ausência de um diálogo acessível à sociedade sobre segurança cibernética é capaz de amplificar os desentendimentos sobre quais "ações" e "atribuições" deveriam ou não estar no escopo da lei, por exemplo. Percebe-se, mais uma vez, a centralidade de um debate público sobre o tema como um dos passos para o estabelecimento de uma cultura de segurança cibernética que integre tanto as preocupações operacionais quanto o desenvolvimento de políticas — um alinhamento estratégico.

Outros desafios se apresentam para as ambições estratégicas de coordenação centralizada não só em sua forma, mas também em seu âmbito institucional. Não é incomum para países destacarem um órgão central para lidar com certas pautas relacionadas à segurança cibernética. No entanto, a característica do GSI e a concentração de militares é preocupante, pois reforça a já existente militarização da cibersegurança, além de congregar pouca diversidade na construção e implementação das atividades de coordenação. Diversas perguntas permanecem sobre como os mecanismos de consulta e aconselhamento trarão essa diversidade — setorial, de gênero, de raça, de disciplina — de visões para o processo de consolidação da governança nacional e se essa inclusão e coordenação com diferentes setores, previstas na E-Ciber, se traduzirá no processo de decisões. Será essencial estabelecer claros mecanismos de transparência com a sociedade para o acompanhamento desses processos de governança (no primeiro momento) e de ações específicas (futuramente).

Ao passo que o documento apresenta o estabelecimento do modelo centralizado como uma das ações estratégicas, também não discorre sobre possíveis modelos e boas práticas em outros países que serviram de inspiração para a inclusão desse ponto. Países como a Austrália, Cingapura e Reino Unido, por exemplo, optaram por um modelo centralizado de Centros Nacionais de Segurança Cibernética. No caso da Austrália[78] e do Reino Unido,[79] os Centros estão integrados ao sistema de inteligência e também incorporam funções de respostas a incidentes. Já Cingapura possui uma Agência dedicada à segurança cibernética, a qual faz parte do Ministério da Comunicação e Informação e incorpora funções que vão desde respostas a incidentes até o desenvolvimento de políticas, operações e representações em fóruns internacionais.[80]

Já no âmbito operacional, a Estratégia foca em recomendações mais específicas, atentando para a necessidade de aprimoramento em torno de respostas a incidentes, proteção de infraestruturas críticas e compartilhamento de informações. Entre os principais pontos, o documento ressalta ações que visam a facilitação dos processos e desenvolvimento de mecanismos de compartilhamento de informações sobre incidentes e vulnerabilidades. Também recomenda a promoção de maior interação entre agências reguladoras de infraestruturas críticas para tratarem sobre segurança cibernética.

77 "[U]rge a necessidade de uma lei que regule as ações de segurança cibernética, que especifique atribuições, que aponte mecanismos de diálogo com a sociedade e que torne possível, ao Gabinete de Segurança Institucional da Presidência da República, com a participação de representantes de todos os entes nacionais, exercer o papel de macro coordenador estratégico, ao proporcionar alinhamento às ações de segurança cibernética e ao contribuir para a evolução de todo o País nesse campo, de forma convergente e estruturada" – extraído da E-Ciber.

78 https://www.cyber.gov.au/acsc.

79 https://www.ncsc.gov.uk/section/about-ncsc/what-we-do.

80 TER, K.L. Singapore's Cybersecurity Strategy. Computer Law & Security Review, v. 34, p 924-927. 2018.

Integração de Conhecimentos

Desde atividades de resposta e tratamento de incidentes à proteção de dados e preservação de direitos humanos, a segurança não só depende da articulação entre diferentes grupos, mas de diferentes conhecimentos e expertise.

A segurança cibernética depende de diferentes conhecimentos e especialidades. A falta de integração de visões no desenvolvimento de políticas e tecnologias pode resultar na consolidação de uma perspectiva míope sobre os riscos e ameaças nacionais.[81] A integração depende do mapeamento das capacidades nacionais em responder e compreender o panorama de ameaças cibernéticas e digitais, o qual passa pelo mapeamento dos conhecimentos atuais nos temas relacionados à cibersegurança. Cada setor já possui vasta experiência no desenvolvimento de iniciativas de capacitação. Organizações da sociedade civil, especializadas em direitos digitais e mídias, por exemplo, já trabalham com comunidades específicas, ajudando-as a se protegerem online.

No contexto da E-Ciber, a integração é enquadrada em recomendações voltadas para a promoção de exercícios de simulação de cenários (com múltiplos atores, como o Guardião Cibernético), o incentivo à participação em eventos nacionais e internacionais; e o aperfeiçoamento de mecanismos de integração e colaboração entre universidades, centros de pesquisa, atores do setor privado e institutos, no tema. Porém, a noção de integração de conhecimentos permanece indefinida na E-Ciber.

Sustentabilidade de Esforços

O desenho de mecanismos, parcerias e atividades que possam ter um impacto duradouro e/ou que possam perdurar e se adaptar de acordo com as mudanças no panorama de ameaças e riscos. Sendo assim, a sustentabilidade é compreendida, em lato sensu, podendo se referir à sustentabilidade financeira, de mecanismos de governança, estratégias, canais de cooperação, medidas de transparência e prestação de contas, bem como a frameworks para monitoramento e implementação de atividades/objetivos.

A sustentabilidade de esforços se refere a ações que contribuem para um impacto duradouro no desenho de mecanismos, parcerias e atividades, e que possuem flexibilidade para se adaptarem às mudanças do panorama de ameaças e riscos. Grande parte das ações[82] e recomendações previstas na E-Ciber relacionadas à essa dimensão se concentram na adoção de padrões que garantam uma continuidade e confiabilidade de sistemas, redes e infraestruturas. Outras recomendações enfatizam ações mais práticas de definição de requisitos de segurança para trabalho remoto e desenvolvimento de soluções de cibersegurança para tecnologias emergentes. Contudo, os principais requerimentos para a sustentabilidade de quase todas as ações recomendadas pela Estratégia dependem da alocação de recursos não só financeiros, mas recursos humanos que possam atender às demandas de coordenação, interlocução e inovação previstas no documento.

81 Maschmeyer, L., Deibert, R., & Lindsay, J. (2020). A Tale of two cybers – how threat reporting by cybersecurity firms systematically underrepresents threats to civil society. Journal of Information Technology & Politics, 1-19, DOI:10.1080/19331681.2020.1776658.

82 Ação estratégica 7: Incentivar a concepção de soluções inovadoras em segurança cibernética; Ação estratégica 10: Elevar o nível de maturidade da sociedade em segurança cibernética.

Pontos Fortes e Fracos da E-Ciber

FORTES

- Primeira vez que um documento do GSI sobre o tema foi encaminhado para consulta pública;
- Reconhecimento da atuação internacional do Brasil em foros especializados em segurança cibernética;
- Previsão do desenvolvimento de capacidades multissetoriais (Conselho Nacional, fóruns, mecanismos de integração entre setores);
- Ressalta a importância de se desenvolver tecnologias com padrões como privacidade e segurança por concepção e design;Visa estimular o uso de criptografia tanto no âmbito da APF quanto na sociedade em geral;
- Ressalta a necessidade de se fortalecer o papel de Centros de Tratamento e Resposta a Incidentes Cibernéticos no país.

FRACOS

- Falta de alinhamento das expectativas relacionadas à E-Ciber. Frustração de diversos setores com o formato da estratégia e a falta de clareza sobre o que quer alcançar;
- Nenhuma menção à sociedade civil (ou terceiro setor) somente à “sociedade” ou “sociedade em geral”;
- Ausência de uma visão clara para o avanço de um debate sobre o estabelecimento de protocolos para a troca de informações entre setores;
- Falta de confiança e desafiadora interlocução entre o GSI e grupos da sociedade civil;
- Incerteza sobre capacidade do GSI de coordenar uma gama tão abrangente de atividades;
- Indefinição sobre o conteúdo a ser apresentado em uma Lei de Segurança Cibernética;
- Ausência de um plano orçamentário (ou expectativa de um) para desenvolvimento de planos para a implementação de ações estratégicas.

Conclusões e Recomendações

Apesar dos desafios, a E-Ciber é um passo importante para a consolidação de um vocabulário e de uma visão estratégica para o Brasil nessa área. Diante de críticas ao caráter abrangente da Estratégia, representantes do GSI argumentaram que o objetivo da E-Ciber é o de abrir espaço para o desenvolvimento da Política Nacional de Segurança Cibernética, a qual terá como instrumento um Plano Nacional de Segurança Cibernética e planos setoriais.[83] O documento sinaliza quais podem ser os principais interesses nacionais para o avanço de uma disseminação da segurança cibernética como um tema que perpassa os setores e a sociedade.

Apesar das tensões domésticas associadas ao contínuo questionamento da credibilidade de instituições democráticas, mobilização da extrema direita e críticas ao governo por sua inação no combate ao coronavírus, essa instabilidade não interferiu diretamente na agenda de segurança cibernética. A E-Ciber é um importante passo para o Brasil, embora revele o longo caminho que temos pela frente para que objetivos e ações estratégicas sejam de fato implementadas. A segurança não deve ser vista somente como uma propriedade de sistemas, redes, máquinas e infraestruturas. A segurança cibernética é um componente fundamental para o enfrentamento de ameaças híbridas no século XXI e, como as eleições em diferentes países, os ataques ao STJ e vazamentos de dados em massa têm mostrado, essencial para a preservação da democracia e fortalecimento da resiliência multissetorial.

83 De Luca, C. (2020). "Após estratégia, GSI elabora a Política Nacional de Segurança Cibernética". Tilt UOL. Disponível em: https://porta23.blogosfera.uol.com.br/2020/02/09/apos-estrategia-gsi-elabora-a-politica-nacional-de-seguranca-cibernetica/.

Recomendações

Recomendação 1

O acompanhamento público da E-Ciber pode trazer maior transparência sobre os objetivos alcançados no meio da vigência da estratégia. Para isso, recomendamos a publicação de um relatório de monitoramento anual com detalhamento dos avanços e desafios da implementação da E-Ciber.

Recomendação 2

Estabelecer canais de diálogo com a sociedade civil e reconhecer sua atuação e papel como importantes atores com experiência em programas de capacitação. Essa interlocução será fundamental para um diálogo mais transparente e para a inclusão dos direitos humanos na agenda de segurança cibernética da APF.

Recomendação 3

Aprimorar mecanismos de compartilhamento de informações sobre incidentes e publicação de vulnerabilidades entre o setor público e o setor privado e disponibilizar diretrizes para a publicação de vulnerabilidades de forma coordenada ("coordinated vulnerability disclosure"). A publicação de guias e relatórios com as regras de compartilhamento devem estar acessíveis para toda a sociedade.

Recomendação 4

Apesar de destacar mecanismos consultivos como o Conselho, a implementação da E-Ciber depende também do aprimoramento da interlocução do GSI com grupos da sociedade e da academia (tanto ciências humanas quanto exatas). Para isso, é fundamental que o GSI construa um plano de comunicação e interlocução com diferentes setores da sociedade, capaz de promover maior interação entre esses grupos.

Recomendação 5

Avaliar capacidades internas do GSI vis à vis a expansão do seu escopo de atuação no tema. Esforços futuros devem priorizar um planejamento multissetorial da implementação da E-Ciber.

Recomendação 6

Avaliar a necessidade de uma lei e/ou o melhor momento para encaminhar ao Congresso Nacional a Lei de Segurança Cibernética, evitando que desgastes com outros assuntos, como, por exemplo, a desinformação e crimes cibernéticos, se confundam com desafios relacionados ao tema.

Anexo 1: Ações Estratégicas e Recomendações da E-Ciber

1. Fortalecer as ações de governança cibernética	(1.1) realizar fóruns de governança;
	(1.2) criar controles para o tratamento de informações com restrição de acesso;
	(1.3) estabelecer requisitos mínimos de segurança cibernética nas contratações pelos órgãos públicos;
	(1.4) implantar programas e projetos sobre governança cibernética;
	(1.5) adotar, além dos normativos de governança emitidos pelo Gabinete de Segurança Institucional da Presidência da República, normas, padrões e modelos de governança reconhecidos mundialmente;
	(1.6) adotar, a indústria, padrões internacionais no desenvolvimento de novos produtos desde sua concepção(privacy/security by design and default);
	(1.7) recomendar a adoção de soluções nacionais de criptografia, observada, para tanto, a legislação específica
	(1.8) intensificar o combate à pirataria de software
	(1.9) adotar soluções de segurança cibernética que abordem iniciativas integradoras
	(1.10) designar o gestor de segurança da informação
	(1.11) recomendar a certificação em segurança cibernética, conforme padrões internacionais
	(1.12) ampliar o uso do certificado digital
2. Estabelecer um modelo centralizado de governança no âmbito nacional	(2.1) promover a coordenação dos diversos atores relacionados com a segurança cibernética, além da esfera federal
	(2.2) promover a análise conjunta dos desafios enfrentados no combate aos crimes cibernéticos
	(2.3) auxiliar na formulação de políticas públicas
	(2.4) criar um conselho nacional de segurança cibernética
	(2.5) criar grupos de debate sobre segurança cibernética, em diferentes setores, sob coordenação do Gabinete de Segurança Institucional da Presidência da República, para fomentar discussões sobre o tema, por meio de mecanismos informais de participação
	(2.6) estabelecer rotina de verificações de conformidade em segurança cibernética, internamente, nos órgãos públicos e nas entidades privadas
	(2.7) permitir a convergência dos esforços e de iniciativas, e atuar de forma complementar para receber denúncias, apurar incidentes e promover a conscientização e a educação da sociedade quanto ao tema. Para viabilizar a sua implementação, ficará a cargo do Gabinete de Segurança Institucional da Presidência da República a coordenação da segurança cibernética em âmbito nacional, que possibilite a atuação de modo amplo, cooperativo, participativo, e alinhado com as ações de defesa cibernética, a cargo do Ministério da Defesa.

continuação

3. Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade	(3.1) estimular o compartilhamento de informações sobre incidentes e vulnerabilidades cibernéticas
	(3.2) realizar exercícios cibernéticos com participação de múltiplos atores
	(3.3) estabelecer mecanismos que permitam a interação e o compartilhamento de informações em diferentes níveis
	(3.4) fortalecer o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov e mantê-lo atualizado em pessoal e material
	(3.5) ressaltar o papel dos Centros de Tratamento e Resposta a Incidentes Cibernéticos - CSIRTs nacionais
	(3.6) aperfeiçoar a infraestrutura nacional de investigação de crimes cibernéticos
	(3.7) incentivar a criação e a atuação de equipe de tratamento e resposta aos incidentes cibernéticos - ETIRs, com ênfase no uso de tecnologias emergentes
	(3.8) emitir alertas e recomendações
	(3.9) estimular o uso de recursos criptográficos, no âmbito da sociedade em geral, para comunicação de assuntos considerados sensíveis
4. Elevar o nível de proteção do Governo	(4.1) incluir requisitos de segurança cibernética nas contratações estabelecidas pelos órgãos e entidades do Governo
	(4.2) aperfeiçoar e incentivar o uso dos dispositivos de comunicação segura do Governo
	(4.3) aperfeiçoar e manter atualizados os sistemas informacionais, as infraestruturas e os sistemas de comunicação dos órgãos públicos, em relação aos requisitos de segurança cibernética
	(4.4) recomendar que os órgãos públicos possuam cópias de segurança atualizadas e segregadas de forma automática em local protegido
	(4.5) elaborar requisitos específicos de segurança cibernética relativos ao uso de endpoints nas organizações públicas, aqui entendidos, em suma, como equipamentos finais conectados a um terminal de alguma rede ou a algum sistema de comunicação
	(4.6) incluir, nas políticas de segurança cibernética, requisitos relativos à gestão da cadeia de suprimentos
	(4.7) incluir requisitos de segurança cibernética nos processos de desestatização, no que envolver serviços essenciais
	(4.8) monitorar a implementação dos requisitos mínimos de segurança cibernética pelos fornecedores que integram a cadeia de suprimentos

continuação

5. Elevar o nível de proteção das Infraestruturas Críticas Nacionais	(5.1) promover a interação entre as agências reguladoras de infraestruturas críticas para tratar de temas relativos à segurança cibernética
	(5.2) estimular a adoção de ações de segurança cibernética pelas infraestruturas críticas
	(5.3) incentivar que essas organizações implementem políticas de segurança cibernética, que contemplem, dentre outros aspectos, métricas, mecanismos de avaliação, e de revisão periódica
	(5.4) incentivar a constituição de ETIRs
	(5.5) estimular que as infraestruturas críticas notifiquem o CTIR Gov dos incidentes cibernéticos
	(5.6) incentivar a participação das infraestruturas críticas em exercícios cibernéticos
6. Aprimorar o arcabouço legal sobre segurança cibernética	(6.1) identificar e abordar temas ausentes na legislação vigente
	(6.2) realizar esforços no sentido de incluir, no Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, novas tipificações de crimes cibernéticos
	(6.3) elaborar normativos sobre tecnologias emergentes
	(6.4) criar políticas de incentivo para contratação de mão de obra especializada em segurança cibernética
	(6.5) definir requisitos de segurança cibernética nos programas de trabalho remoto
	(6.6) elaborar, sob coordenação do Gabinete de Segurança Institucional da Presidência da República, um anteprojeto de lei sobre segurança cibernética, com diretrizes que irão proporcionar alinhamento macroestratégico ao setor e contribuir de forma decisiva para elevar a segurança das organizações e dos cidadãos

continuação

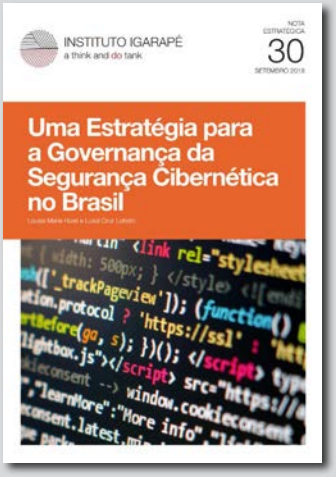
7. Incentivar a concepção de soluções inovadoras em segurança cibernética	(7.1) propor a inclusão da segurança cibernética nos programas de fomento à pesquisa
	(7.2) incentivar a criação de centros de pesquisa e desenvolvimento em segurança cibernética no âmbito do Poder Executivo federal e no setor privado
	(7.3) viabilizar investimentos em pesquisas, por meio dos fundos públicos e privados
	(7.4) criar programas de incentivo ao desenvolvimento de soluções de segurança cibernética
	(7.5) estimular a criação de startups na área de segurança cibernética
	(7.6) estimular o desenvolvimento e a inovação de soluções de segurança cibernética nas tecnologias emergentes
	(7.7) incentivar a adoção de padrões globais de tecnologia, que permitirá a interoperabilidade em escala internacional
	(7.8) incentivar o desenvolvimento de competências e de soluções em criptografia
	(7.9) estimular o prosseguimento das pesquisas sobre o uso de inteligência espectral
	(7.10) estabelecer requisitos mínimos de segurança cibernética que assegurem o uso pleno, responsável e seguro da tecnologia de quinta geração de conexão móvel - 5G
8. Ampliar a cooperação internacional do Brasil em Segurança cibernética	(8.1) estimular a cooperação internacional em segurança cibernética
	(8.2) incentivar as discussões sobre segurança cibernética nos organismos, nos fóruns e nos grupos internacionais dos quais o Brasil é membro
	(8.3) ampliar o relacionamento internacional com os países da América Latina
	(8.4) promover eventos e exercícios internacionais sobre segurança cibernética
	(8.5) participar de eventos internacionais de interesse para o País
	(8.6) ampliar os acordos de cooperação em segurança cibernética
	(8.7) ampliar o uso de mecanismos internacionais de combate aos crimes cibernéticos
	(8.8) estimular a participação do País em iniciativas futuras de estruturação normativa, como as relativas à criação de padrões de segurança em tecnologias emergentes
	(8.9) identificar, estimular e aproveitar novas oportunidades comerciais em segurança cibernética

continuação

9. Ampliar a parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade	(9.1) ampliar a cooperação entre Governo, academia e iniciativa privada para promover a implementação da E-Ciber
	(9.2) manter um ambiente colaborativo que permita o estudo e a ampla utilização das tecnologias emergentes
	(9.3) estabelecer parcerias para incentivar o setor privado a investir em medidas de segurança cibernética
	(9.4) incentivar a realização de reuniões com atores destacados em segurança cibernética
	(9.5) estimular a instituição, caso necessário, de grupos de trabalhos e fóruns sobre segurança cibernética
	(9.6) incentivar a criação de mecanismos de compartilhamento de informações sobre riscos cibernéticos
	(9.7) realizar parcerias entre a União, os Estados, o Distrito Federal, os Municípios, o Ministério Público e a academia, para a implantação de programas, projetos e ações em segurança cibernética, que alcancem a toda a sociedade
10. Elevar o nível de maturidade da sociedade em segurança cibernética	(10.1) incentivar os órgãos públicos e empresas privadas para que realizem campanhas de conscientização internas
	(10.2) realizar ações de conscientização da população
	(10.3) criar políticas públicas que promovam a conscientização da sociedade sobre segurança cibernética
	(10.4) propor a inclusão da segurança cibernética, por intermédio de suas competências básicas, e do uso ético da informação na educação básica - educação infantil, ensino fundamental e ensino médio
	(10.5) estimular a criação de cursos de nível superior em segurança cibernética
	(10.6) propor a criação de programas de incentivo para graduação e pós-graduação no Brasil e no exterior em segurança cibernética
	(10.7) fomentar a pesquisa e o desenvolvimento em segurança cibernética
	(10.8) criar programas de capacitação continuada para profissionais do setor público e do setor privado
	(10.9) incentivar a formação de profissionais para atuar no combate aos crimes cibernéticos
	(10.10) realizar eventos de capacitação em segurança cibernética
	(10.11) incentivo à participação e eventos nacionais e internacionais em segurança cibernética
	(10.12) aperfeiçoar mecanismos de integração, de colaboração e de incentivos entre universidades, institutos, centros de pesquisa e setor privado em relação à segurança cibernética
	(10.13) incentivar exercícios de simulação em segurança cibernética
	(10.14) promover a gestão de conhecimento de segurança cibernética, em articulação com os principais atores da área, a fim de otimizar a identificação, a seleção e o emprego de talentos

Leia também

PUBLICAÇÃO
REGULAÇÃO DO RECONHECIMENTO FACIAL NO SETOR PÚBLICO: avaliação de experiências internacionais
Louise Marie Hurel, Mariana Marques Rielli e Pedro Augusto P. Francisco
(Junho 2020)



NOTA ESTRATÉGICA 30
UMA ESTRATÉGIA PARA A GOVERNANÇA DA SEGURANÇA CIBERNÉTICA NO BRASIL
Louise Marie Hurel e Luisa Cruz Lobato
(Setembro 2018)

ARTIGO ESTRATÉGICO 11
DECONSTRUCTING CYBER SECURITY IN BRAZIL: Threats and Responses
Gustavo Diniz, Robert Muggah and Misha Glenny
(Dezembro 2014)

INSTITUTO IGARAPÉ
a think and do tank

O Instituto Igarapé é um think and do tank independente, dedicado à integração das agendas de segurança, clima e desenvolvimento. Nosso objetivo é propor soluções e parcerias a desafios globais por meio de pesquisas, novas tecnologias, influência em políticas públicas e comunicação. Somos uma instituição sem fins lucrativos, independente e apartidária, com sede no Rio de Janeiro, mas cuja atuação transcende fronteiras locais, nacionais e regionais. Premiada como a melhor ONG de Direitos Humanos no ano de 2018, o melhor think tank em política social pela Prospect Magazine em 2019 e considerada pelo Instituto Doar, pelo segundo ano consecutivo, como uma das 100 melhores organizações brasileiras do terceiro setor.

Apoio:

Embaixada Britânica
Brasília

Instituto Igarapé

Rio de Janeiro - RJ - Brasil
Tel/Fax: +55 (21) 3496-2114
contato@igarape.org.br
facebook.com/institutoigarape
twitter.com/igarape_org

www.igarape.org.br

Direção criativa e layout
Raphael Durão - STORMdesign.com.br

ISSN 2359-0998

www.igarape.org.br

INSTITUTO IGARAPÉ
a think and do tank