Avaliação de Políticas Públicas
(Resolução nº 44, de 2013)

Proposta de Plano de Trabalho

Avaliação do Programa de Defesa Cibernética

Presidente: Senador **NELSINHO TRAD**

Vice-Presidente: Senador **MARCOS DO VAL**

Relator: Senador **ESPERIDIÃO AMIN**

1. APRESENTAÇÃO

A avaliação de políticas públicas tem como objetivo principal aprimorar a gestão do Estado, por meio da mensuração de sua eficiência, eficácia e efetividade. O resultado da avaliação é fundamental para orientar as ações do Poder Público.

A Resolução do Senado Federal n° 44, de 2013, prevê que a Casa Legislativa realize a avaliação de políticas públicas, que buscará, entre outras medidas, adequar os dispositivos normativos às necessidades sociais.

Nos termos do art. 1º dessa normativa, "as comissões permanentes selecionarão, na área de sua competência, políticas públicas desenvolvidas no âmbito do Poder Executivo, para serem avaliadas".

Mediante a aprovação, no dia 9 de maio, do Requerimento nº 24, de 2019, a Comissão de Relações Exteriores e Defesa Nacional (CRE) decidiu avaliar a Política de Defesa Cibernética, setor estratégico do Estado Brasileiro, que, segundo a Estratégia Nacional de Defesa, é delegada ao Exército Brasileiro.

No Brasil, os assuntos relacionados às vulnerabilidades digitais foram tratados, inicialmente, sob a égide da Segurança da Informação pelo Decreto nº 3.505/2000, que instituiu a Política de Segurança da Informação.

No âmbito da Defesa, o denominado Setor Cibernético foi destacado pela Estratégia Nacional de Defesa (END), aprovada pelo Decreto nº 6.703/2008, ao lado do setor espacial e do setor nuclear, como um dos três setores considerados estratégicos e essenciais para a Defesa Nacional.

A Diretriz Ministerial nº 014/2009, do Ministério da Defesa, definiu as responsabilidades relativas a cada um desses três setores estratégicos: nuclear, a cargo da Marinha; cibernético, a cargo do Exército; e espacial, a cargo da Aeronáutica. Adicionalmente, determinou providências relativas a objetivos e estratégias setoriais correspondentes a cada Força. Reforçou, ainda, que esses três setores "transcendem, por sua natureza, a divisão entre desenvolvimento e defesa, entre o civil e o militar".

O interesse da Casa por esse tema não é novo. Em 2013, um episódio mundial de grande repercussão — a suposta espionagem de agência dos Estado Unidos em vários países — resultou em denúncias de intromissão em assuntos oficiais brasileiros. Como consequência, em 3 de setembro daquele ano, o Senado Federal instaurou uma Comissão Parlamentar de Inquérito (CPI) destinada a "investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar e-mails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal".

Os trabalhos da CPI duraram até abril de 2014, incluindo depoimentos de vários especialistas e de representantes de órgãos públicos ligados às áreas de inteligência e cibernética, tais como o Ministério da Defesa, a Anatel e a Polícia Federal, bem como aqueles supostos alvos da espionagem norte-americana, a exemplo da Petrobras.

Ainda no contexto do episódio acima apresentado, o Ministério da Defesa criou um Grupo de Trabalho (GT-Ciber), instituído pela Portaria Ministerial nº 2.569-EMCFA/MD, de 6 de setembro de 2013, para elaborar propostas mais imediatas para o campo da Defesa Cibernética.

No relatório apresentado pelo GT-Ciber, que foi aprovado pelo Ministro da Defesa em 13 de março de 2014, constaram medidas para mitigar as vulnerabilidades do ambiente cibernético, incluindo a criação do

Comando de Defesa Cibernética (ComDCiber) e da Escola Nacional de Defesa Cibernética (ENaDCiber).

Em 27 de outubro de 2014, a Portaria Normativa nº 2.777/MD definiu a "Diretriz de Implantação de Medidas Visando à Potencialização da Defesa Cibernética Nacional". Coube ao Exército, em articulação com o Estado-Maior Conjunto das Forças Armadas (EMCFA), a Secretaria Geral do Ministério da Defesa (SG/MD) e as demais Forças Armadas, os seguintes encargos, entre outros:

- Imediata ativação do Núcleo do Comando de Defesa Cibernética (NuComDCiber) e coordenação da criação e implantação do ComDCiber;

- Imediata ativação do Núcleo da Escola Nacional de Defesa Cibernética (NuENaDCiber) e coordenação da criação e implantação da ENaDCiber; e

- Organização e execução de projetos relacionados ao Setor de Defesa Cibernética.

O tema "defesa cibernética" vem sendo tratado pelas Forças Armadas, sob a coordenação do Exército, desde 2010. Nesse período, esforços vêm sendo realizados para incorporar e aplicar capacidades.

Assim, essa avaliação de política proposta pela CRE constitui importante e valioso instrumento para, a partir das análises a serem realizadas, retificar ou ratificar os planejamentos para o futuro do setor cibernético da defesa, que completou uma década, conferindo o aval do Senado Federal aos avanços pretendidos pelas Forças Armadas e, em última análise, em nome da sociedade brasileira.

Diante da relevância e considerando a transversalidade do Setor Cibernético para a defesa do Estado Brasileiro, as perguntas que a presente avaliação de políticas públicas buscará responder são:

1) Como se encontra a implantação das medidas definidas pelo Ministério da Defesa?

2) Quais as transformações e os impactos, positivos e negativos, de sua implementação?

3) Esses instrumentos foram efetivamente implementados ou carecem de plena implementação? Nesse último caso, quais os gargalos a serem desobstruídos?

4) Considerando a evolução da maturidade institucional, a velocidade de eventos e alterações de cenários que caracterizam o Setor Cibernético, as medidas propostas em 2014 são suficientes? Há demandas a serem atendidas para

que se obtenha o nível de defesa compatível com os cenários de curto, médio e longo prazos?

5) O que se pretende para o futuro do setor cibernético de defesa?

2. ATIVIDADES PROPOSTAS

Para levar a contento a avaliação desses instrumentos, sugere-se que a CRE segmente suas análises em cada um deles, para os quais são previstas as seguintes ações:

- Solicitação de informações ao Comando do Exército, por intermédio do ComDCiber, acerca da implantação das medidas indicadas pelo Ministério da Defesa e dos resultados obtidos com as medidas implementadas;
- Identificação de atores sociais e agentes econômicos relacionados ao tema;
- Realização de audiências públicas;
- Considerando a sensibilidade do tema, realização de audiência reservada, a fim de identificar vulnerabilidades, e levantamento de ações, visando à mitigação de ameaças e à implementação de medidas que levem à efetividade da Defesa Cibernética;

- Realização de visitas técnicas ao ComDCiber, com vistas a identificar gargalos e oportunidades de melhoria.

Com base nessas atividades, será elaborado o relatório final para apreciação pela Comissão até novembro deste ano.

3. CRONOGRAMA

Propomos a seguinte programação para o trabalho de avaliação desses instrumentos:

Atividade	Local	Convidados	Temas
1) Reunião de instalação dos trabalhos	Brasília	- Comando de Defesa Cibernética.	Apresentação e debate do plano de trabalho
2) Reuniões técnicas	Brasília	Senadores e assessorias	Reunião interna: avaliação dos trabalhos e calibragem de cronogramas. Definição de datas para as audiências públicas.
3) Análise orçamentária	Brasília	Consultoria de Orçamentos do Senado (CONORF)	Requerimento à consultoria de orçamento para análise orçamentária do setor.
4) Audiência Reservada com Membros da CRE	Brasília	- Ministério da Defesa; - Gabinete de Segurança Institucional da Presidência da República; - Comando do Exército, da Marinha e da Força Aérea; - Ministério das Relações Exteriores; - Ministério da Justiça.	I - Diagnóstico de ameaças sensíveis do setor cibernético e gargalos do Estado para implementar uma política de Defesa Cibernética, com foco: 1) na definição de marcos legais; 2) no fortalecimento da estratégia de superação dos gargalos verificados; II – Avaliação da efetividade de colaboradores nacionais e internacionais, identificando medidas necessárias para a obtenção de resultados.

Atividade	Local	Convidados	Temas
5) Duas Audiências Públicas	Brasília	1ª) Órgãos públicos: - Ministério da Defesa; - Gabinete de Segurança Institucional da Presidência da República; - Comando do Exército, da Marinha e da Força Aérea. 2ª) Representantes da sociedade civil: - Gerente geral do CERT.BR; - Representantes da ICP-Brasil; - Outros	I – Planejamento Estratégico do Setor Cibernético; II – Avaliação do planejamento e da execução orçamentária relacionados ao Setor Cibernético; III – Necessidades e cenários orçamentários relacionados ao Setor Cibernético; IV – Debate sobre a implementação das medidas definidas em 2014 e as frentes de atuação que se delineiam a partir dos resultados já verificados; V – Apontamento das ameaças e as atualizações do cenário do ambiente cibernético.
6) Visitas Técnicas	Brasília	Membros da CRE	I – Identificação das instalações do ComDCiber e ferramentas utilizadas; II – Análise dos gargalos para a implementação das infraestruturas adequadas aos cenários de curto, médio e longo prazos.
Apresentação e Votação do Relatório Final (NOVEMBRO DE 2019)			

Sala da Comissão,

, Presidente

, Relator