

ASSESPRO

PODER LEGISLATIVO
CÂMARA DOS DEPUTADOS
COMISSÃO DE RELAÇÕES EXTERIORES E DEFESA NACIONAL (CRE)
SUBCOMISSÃO DE DEFESA CIBERNÉTICA (CREDC)

Audiência Pública: riscos à segurança digital do país.

A Subcomissão Permanente de Defesa Cibernética (CREDC) do Senado Federal, realizou, na quarta-feira (30), audiência pública para debater os riscos à segurança digital do país com a participação do General de Divisão **Alan Denilson Lima Costa**, Comandante de Defesa Cibernética do Exército Brasileiro e foi conduzida pelo senador Esperidião Amin (PP/SC), presidente da Subcomissão.

O debate estava previsto na proposta do plano de trabalho da comissão, que sugeria audiência pública com órgãos públicos: Ministério da Defesa (MD); Gabinete de Segurança Institucional da Presidência da República (GSI/PR); Comandos do Exército, da Marinha e da Força Aérea para debater os temas de (i) Política Nacional de Cibersegurança: Estratégia Nacional de Segurança Cibernética e Plano Nacional de Cibersegurança, (ii) Relações entre Segurança e Defesa Cibernética; (iii) anteprojeto de lei sobre Política Nacional de Cibersegurança (PNCiber) e o Sistema Nacional de Cibersegurança (SNCiber).

O general **Alan Denilson** apresentou uma exposição histórica e técnica sobre a implantação do setor cibernético na Defesa Nacional, destacando que o Brasil reconheceu as ameaças cibernéticas como um risco à segurança nacional desde 2008, quando a temática foi incluída na Estratégia Nacional de Defesa, posicionando-a ao lado de áreas como nuclear e espacial. O Comando de Defesa Cibernética foi efetivamente estabelecido em 2016, intensificando a cooperação internacional. Projetando os desafios vindouros, enfatizou a importância da preparação para as transformações que a Inteligência Artificial e as tecnologias quânticas trarão até 2040, mencionando a necessidade de implementar algoritmos criptográficos pós-quânticos.

Destacou que as capacidades desenvolvidas estão prontas não só para operações militares, mas também disponíveis para apoiar a segurança cibernética do país, e delineou os níveis de atuação na segurança cibernética, tendo a responsabilidade política recaindo sobre o GSI, enquanto a Defesa Cibernética atua como um comando estratégico operacional, responsável por entregar capacidades ao nível tático.

Reiterou que o Comando é um órgão central do Sistema Militar de Defesa Cibernética (SMDC), cuja missão é desenvolver e aplicar capacidades cibernéticas em favor da defesa nacional, e que entre suas principais competências estão: (i) desenvolver e aplicar – *capacitação dos recursos humanos*; (ii) colaborar com o GSI em incidentes cibernéticos; (iii) propor e executar a cooperação internacional que, por sua relevância, possui uma estratégia própria de ampliar as capacidades cibernéticas e tem por objetivo posicionar o Comando de Defesa Cibernética e o Brasil como um parceiro confiável e dotado de elevada capacidade técnica e organizacional para conduzir ações cibernéticas; (iv) assessorar o Ministério da Defesa e os Comandos das Forças no emprego da capacidade cibernética; e (v) fomentar o desenvolvimento de soluções tecnológicas.

Seguiu exemplificando ações do Comando, como a participação em fóruns internacionais – *por vezes, como o único representante da América Latina* –; a organização de um estágio internacional, realizado em Brasília, para receber oficiais de nações amigas visando a troca de experiências; capacitações e exercícios de jogo de guerra com situações fictícias de simulação construtiva com resolução de questões de cibersegurança. Enfatizou que essas simulações, como o Exercício Guardiã Cibernético realizado pelo Exército – *que em 2024 contou com mais 140 organizações e 600 profissionais* –, visam o adestramento da equipe dedicada na perspectiva da ampliação da capacidade militar cibernética.

Abordou ainda, no âmbito das interações institucionais, a participação do Comando no Comitê Nacional de Cibersegurança, liderado pelo GSI. O colegiado, composto por três grupos de trabalho, tem trabalhado na revisão da Estratégia Nacional de Cibersegurança; no desenvolvimento de um anteprojeto de lei para criação um órgão de governança que coordene as ações dessa temática em âmbito nacional. O terceiro concluiu suas atividades abordando a cooperação internacional.

O senador **Fernando Dueire** (MDB/PE) elogiou a apresentação e a organização estatal para tratar da temática, e nesse contexto levantou duas questões: i) a disponibilidade de orçamento para execução das atividades previstas; e ii) a necessidade de um órgão de governança ou comitê para coordenar o trabalho de segurança cibernética, dado a complexidade e a transversalidade do tema.

Em resposta, o general **Alan Denilson** explicou que a construção de uma organização robusta é essencial para atender aos desafios da Defesa e Segurança Cibernética. Afirmou que são diversas frentes que precisam ser muito bem guarnecidas com estratégias próprias, com um planejamento estratégico claro e ferramentas para medir o progresso, e com pessoas vocacionadas para que avance e reconheceu que a estrutura atual no GSI é pequena.

Quanto à questão orçamentária, o general enfatizou que é difícil quantificar valores, pois as ameaças exploram vulnerabilidades, mas destacou que é crucial o investimento em infraestrutura e sistemas operacionais para a modernização e prevenção. Além disso, investir na qualificação da força de trabalho e no desenvolvimento de soluções nacionais para órgãos públicos também são questões que merecem atenção e investimento.