A atuação do Exército Brasileiro para o domínio do espaço cibernético

*Joffre Ferreira Abdalla**

Introdução

Com a evolução constante dos meios de Tecnologia da Informação e Comunicação (TIC), a sociedade alterou rapidamente seus hábitos, migrando muitas de suas atividades do mundo físico para um ambiente virtual, no qual é possível, com alcance global e instantâneo, comunicar-se, comercializar, estudar e descansar. Assim surgiu o espaço cibernético.

Com a mesma intensidade, observa-se que o setor militar também incluiu as TIC em materiais bélicos, que, agora modernizados, ampliaram o poder de combate das nações, principalmente no que diz respeito ao processo de *comando e controle* (C^2).

Nesse escopo, diante da dependência das esferas sociais, governamentais e militares para com o espaço cibernético, as nações se viram obrigadas a proteger o principal ativo que nele circula, a informação.

No Brasil, o Ministério da Defesa (MD) ficou responsável pela defesa cibernética, que abrange ações para garantir a normalidade no espaço cibernético militar e de interesse. Para tal, delegou ao Exército Brasileiro (EB) a coordenação desse sistema e a integração entre as três Forças Singulares.

Dessa forma, este artigo de opinião visa esclarecer a atuação do Exército Brasileiro no domínio do espaço cibernético à luz de sua estrutura organizacional, legislação e doutrina. Tal objetivo se justifica devido à importância do setor cibernético para a Estratégia Nacional de Defesa (END) e pela crescente exposição do país como sede de eventos internacionais. Factualmente, esses eventos têm a organização dependente do espaço cibernético.

Desenvolvimento

Para esclarecimento do tema, serão abordados os seguintes tópicos: amparo legal para atuação do Exército Brasileiro no espaço cibernético; organização e estrutura do setor cibernético no EB; domínio do espaço cibernético; e a atuação da defesa cibernética em um grande evento nacional.

Amparo legal

Quanto ao amparo legal para atuação do Exército Brasileiro no espaço cibernético, cabe destacar que o setor cibernético nacional foi dividido em dois campos distintos: a *segurança cibernética*, a cargo da Presidência da República, e a *defesa cibernética*, a cargo do MD, por intermédio da atuação das Forças Armadas (BRASIL, 2014).

Nesse escopo, a presença do Ministério da Defesa no espaço cibernético foi prevista na Estratégia Nacional de Defesa (END) publicada em 2008. Como consequência, no ano seguinte, a Diretriz Ministerial/MD nº 14 estabeleceu providências para o cumprimento das estratégias relativas aos setores ditos essenciais, delegando as responsabilidades às suas Forças Armadas. Assim, a coordenação e a integração do setor espacial ficaram a cargo da Força Aérea Brasileira (FAB). À Marinha do Brasil (MB) coube a responsabilidade sobre o setor nuclear e ao Exército Brasileiro (EB) as atividades do setor cibernético.

Desse modo, pode-se dividir a atuação no espaço cibernético em três níveis no tocante à defesa cibernética: estratégico, operacional e tático.

* Cap Art (AMAN 2010, EsAO 2020). Atualmente, serve no 19º GAC, em Santiago-RS.

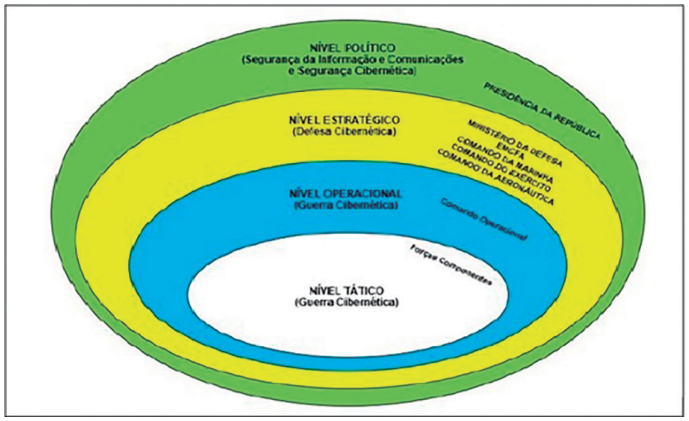

Figura 1 – Níveis de organização do setor cibernético brasileiro
Fonte: BRASIL, 2014, p. 17/36

Dessa forma, em nível estratégico, o MD executa a defesa cibernética, uma atividade integrada das Forças Armadas e liderada pelo EB. Essa atividade adota uma abordagem de cunho militar, composta por ações realizadas no espaço cibernético com o intuito de proteger os sistemas de informação de interesse da Defesa Nacional. Visa, ainda, obter dados para a produção de conhecimento de inteligência e comprometer os sistemas de informação do oponente (BRASIL, 2017, p. 2-2). Quando o nível de decisão for o operacional ou o tático, as ações cibernéticas são definidas como *guerra cibernética* (BRASIL, 2014, p. 26/36).

Organização e estrutura do setor cibernético no EB

O setor cibernético foi inserido na estrutura do Exército Brasileiro em 2010, por meio da criação do Centro de Defesa Cibernética (CDCiber), órgão que ficou encarregado de coordenar e de integrar as ações no espaço cibernético em proveito das operações militares com intuito de colocar em prática a END.

O CDCiber estava diretamente subordinado ao Departamento de Ciência e Tecnologia (DCT), Orgão de Direção Setorial (ODS), que tem a finalidade de orientar, normatizar e supervisionar a pesquisa, o desenvolvimento e a implementação das bases física e lógica da defesa cibernética do Exército, dentre outras missões relacionadas aos meios de Tecnologia da Informação e Comunicações (TIC).

Entretanto, para atuar no espaço cibernético, o CDCiber não se ateve apenas a atividades operacionais no ciberespaço. Houve também a necessidade de executar a capacitação de recursos humanos, além do desenvolvimento de doutrina para orientar as ações cibernéticas de ataque e de exploração da rede oponente, bem como da proteção de seus ativos informacionais.

Diante desse amplo escopo de atividades, em 2014 o MD decidiu implantar o Comando de Defesa Cibernética (ComDCiber) como elemento central e integrador das Forças Armadas, e a Escola Nacional de Defesa Cibernética (ENaDCiber) como elemento de capacitação dos recursos humanos, para integrar os militares das Forças Armadas e, assim, ampliar as capacidades de defesa cibernética nacionais.

Em 2017, diante da crescente importância do setor cibernético e visando a ampliar suas estruturas e capacidades, o Exército decidiu transformar o Projeto de Defesa Cibernética em Programa Estratégico do Exército, o que aumentou a prioridade de desenvolvimento desse setor militar.

Figura 2 – Organização do Exército Brasileiro no setor cibernético nacional
Fonte: Palestra do Comando de Defesa Cibernética, 2018

Domínio do espaço cibernético

Atualmente, o ambiente cibernético das redes de transmissão de dados é o principal vetor de circulação de informações governamentais ostensivas ou sigilosas. É por meio dessas redes que circulam as decisões políticas e estratégicas, bem como as ordens das operações militares.

Consequentemente, a segurança do espaço cibernético nacional tornou-se fundamental para a soberania das nações. Dentre outras garantias, visa à circulação das informações sem interceptação ou interferência de

outros atores, o que afiança a privacidade das informações de seus cidadãos e de empresas, a continuidade da prestação de serviços, além do sigilo das políticas e estratégias governamentais.

Diante de um cenário de conflito, a força cibernética de um país deve ter condições de realizar ações de ataque e de exploração a redes de sistemas informacionais de um espaço cibernético alvo, além de ações de proteção de seus próprios ativos de informação contra investidas oponentes.

Conforme consta em manual doutrinário, as ações de ataque compreendem a interrupção, a negação e a degradação de informações ou de sistemas computacionais ligados em redes de dados (BRASIL, 2014). Um exemplo dessas ações poderia ser a interrupção de serviços de infraestruturas críticas automatizadas, que são altamente dependentes das redes para circulação de comandos de funcionamento.

Em uma situação hipotética de conflito, Clarke (2015) menciona o sistema elétrico norte-americano como um alvo compensador, pois sua degradação iria comprometer muitos outros sistemas das Forças Armadas e da sociedade estadunidense.

As ações de exploração cibernética consistem na busca e na coleta de conhecimento sobre o sistema informacional alvo do oponente no que diz respeito ao seu funcionamento, à proteção e às vulnerabilidades, de modo que possa assegurar uma correta consciência situacional durante o planejamento e a execução do ataque a esse alvo (BRASIL, 2014). Nessa fase, é fundamental a observação do princípio da dissimulação a fim de evitar o rastreamento e a identificação do invasor no sistema, pois, do contrário, as vulnerabilidades levantadas serão corrigidas e os mandantes da ação serão sancionados. Clarke (2015) aborda que o ataque pode ser preparado durante a fase de exploração, com a adição de bombas lógicas e de códigos maliciosos de *backdoors* (facilitadores de invasão).

Por fim, as ações de proteção, que têm caráter permanente, devem neutralizar ataques e explorações oponentes contra sistemas cibernéticos amigos, a fim de garantir a plena utilização do espaço cibernético, em especial do sistema de comando e controle das operações militares (BRASIL, 2014).

Cabe adicionar que, segundo Clarke (2015), para o domínio de um espaço cibernético, é preferível um sistema de proteção permanente e altamente capacitado a um sistema de ataque cibernético sofisticado, pois um país pode ser surpreendido por um ataque inicial e ter essa capacidade ofensiva anulada. Como exemplo, menciona que China e Coreia do Norte são capazes de lançar ataques cibernéticos e, se necessário, limitar suas conexões na internet, o que minimizaria a eficácia de um ataque de retaliação.

Um caso de atuação da defesa cibernética em grandes eventos

A defesa cibernética é uma atividade diária em operações militares ou em situação de normalidade institucional. No âmbito da Defesa Nacional, visa garantir a capacidade de atuação em rede, a interoperabilidade e a proteção dos sistemas e ativos de informação relativos ao Ministério da Defesa.

Consequentemente, para garantir a integridade de sua rede, o MD adota níveis de alerta relativos à possibilidade de ameaças no espaço cibernético de seu interesse. Esses níveis estão associados às lições aprendidas em exercícios simulados ou ataques cibernéticos reais, conforme o **quadro 1**:

Nível de Alerta		Significado / Interpretação (*)
Cor	Nome	
Branco	Baixo	– Aplicável quando as ameaças cibernéticas percebidas não afetam o Espaço Cibernético de interesse do MD e das FA. – Situação normal ou rotineira, considerando o histórico. – Probabilidade de concretização de ameaças cibernéticas baixa, considerando o histórico.
Azul	Moderado	– Aplicável quando as ameaças cibernéticas percebidas afetam o Espaço Cibernético de interesse do MD e das FA, sem comprometer as infraestruturas críticas da Informação. – Probabilidade de concretização de ameaças cibernéticas entre baixa e média, considerando o histórico.
Amarelo	Médio	– Aplicável quando ações cibernéticas hostis afetam o Espaço Cibernético de interesse, sem comprometer as infraestruturas críticas da informação. – Aplicável quando houver a percepção de ameaças cibernéticas contra as infraestruturas críticas da informação. – Probabilidade da concretização de ameaças cibernéticas entre média e alta, considerando o histórico.
Laranja	Alto	– Aplicável quando as ações cibernéticas hostis degradam alguma Infraestrutura Crítica da Informação. – Probabilidade de concretização de ameaças cibernéticas entre média e alta, considerando o histórico. – Infraestrutura Crítica da Informação atingida, porém com possibilidade de restabelecimento das condições de segurança ou dos serviços em tempos aceitáveis para o cumprimento da missão. – Infraestrutura Crítica da Informação atingida com impacto entre médio e alto, considerando o histórico.
Vermelho	Muito Alto	– Aplicável quando ações cibernéticas hostis exploram ou negam a disponibilidade das infraestruturas críticas da informação. – Probabilidade de concretização de ameaças cibernéticas muito alta, considerando o histórico. – Infraestrutura Crítica da Informação atingida com impacto alto ou superior, considerando o histórico. – Infraestrutura Crítica da Informação atingida, com possibilidade de restabelecimento da condição de segurança ou dos serviços em tempos além dos aceitáveis para o cumprimento da missão.

Quadro 1 – Quadro dos níveis de alerta adotados pelo Ministério da Defesa
Fonte: BRASIL, 2014, p. 27-28

Dentre os diversos grandes eventos dos quais o CD-Ciber participou na segurança do espaço cibernético nos últimos anos (**figura 3**), pode-se mencionar os Jogos Olímpicos do Rio 2016 como uma ocasião em que o nível de alerta cibernético poderia ter evoluído momentaneamente, embora não tenha ocorrido nenhum pronunciamento oficial a respeito,

Por se tratar de um evento de dimensões internacionais, incidentes cibernéticos praticados por *hacktivistas* e terroristas eram iminentes. Diante disso, foi desencadeada a Operação JO, na qual o sistema de defesa cibernética atuou de modo conjunto com outros órgãos nacionais para garantir a integridade das informações da competição que circulavam no espaço cibernético.

Figura 3 – Alguns dos grandes eventos com presença do CDCiber
Fonte: Palestra do Comando de Defesa Cibernética, 2018

Segundo consta em matéria do *site G1*, durante o evento, as redes de apoio da competição sofreram uma média de três incidentes cibernéticos por hora. Diante disso, analisando a conjuntura do grande evento e o fluxo de ameaças cibernéticas nesse ambiente, deduz-se que o estado de alerta foi elevado acima do nível baixo, denominado nível branco, que condiz com uma situação rotineira (**quadro 1**).

Dessarte, levando-se em consideração a consciência situacional, o histórico das edições anteriores, o clima de manifestações e o terrorismo internacionais contra algumas nações que participavam dessa edição, existia a probabilidade de concretização de incidentes cibernéticos nos sistemas informacionais dos Jogos Olímpicos Rio 2016.

Entretanto, diante do cenário descrito, os incidentes cibernéticos não comprometeram o funcionamento dos sistemas e, consequentemente, foi garantido o pleno funcionamento da organização dos jogos, que, factualmente, estava dependente do espaço cibernético. O êxito contra tais ameaças durante a Operação JO ocorreu devido ao trabalho do sistema de defesa cibernética do MD integrado com os demais sistemas públicos e privados envolvidos na proteção do ciberespaço do evento.

Conclusão

Neste artigo foi analisada a presença do Exército Brasileiro no espaço cibernético em tópicos que expuseram a legislação vigente para amparar a atividade militar no setor, a organização e a estrutura do EB para execução das atividades cibernéticas, bem como um caso de atuação do sistema de defesa cibernética durante um evento internacional realizado no Brasil.

Na abordagem sobre o amparo legal, foi esclarecido que a atividade de defesa cibernética possui amparo governamental para emprego a cargo das Forças Armadas, pois se enquadra como um dos componentes da Defesa Nacional e sua estratégia. Foi percebido também que o Estado valoriza a importância do setor diante da conjuntura geopolítica atual, já que constantemente fez publicações que buscaram garantir a consecução de seus interesses no ciberespaço.

Em complemento, foi analisada a organização e a estrutura do Exército Brasileiro, responsável pela coordenação da defesa cibernética. Além disso, foi identificado o esforço constante de aperfeiçoamento das estruturas do EB, de maneira que conseguisse aprimorar suas capacidades cibernéticas e, assim, proporcionar o exercício adequado no ciberespaço, sob responsabilidade do Ministério da Defesa.

O Exército Brasileiro insere-se no referido setor por intermédio da execução e da coordenação das atividades de defesa cibernética sob responsabilidade do

Ministério da Defesa. Para cumprir tal objetivo, sua organização funcional e suas infraestruturas foram ampliadas. De forma complementar, existe a previsão de aumento das capacidades mediante a implantação do setor no Programa Estratégico do Exército.

À luz da doutrina em vigor, o EB adota as ações adequadas em suas operações, além de prever a atuação conjunta com outros sistemas públicos e privados em prol da otimização do sistema de defesa cibernética.

Por fim, conclui-se que o EB está inserido no setor cibernético de modo permanente, com estruturas cada vez mais adequadas e eficientes. Essas constatações certificam-se pelo êxito das operações cibernéticas executadas durante os grandes eventos desenvolvidos no Brasil.

Referências

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. **Diário Oficial da União**, Brasília, DF, 6 fev 2020. Seção 1, p. 6.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília, DF, 2012. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/2012/mes07/end.pdf>. Acesso em: 2 maio 2020.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **MD31-M- 08: Doutrina Militar de Defesa Cibernética**. Brasília, DF, 2014.

BRASIL. Ministério da Defesa. Estado-Maior do Exército. **EB70-MC-10.232: Guerra Cibernética.** Brasília, DF, 2017.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética:** a próxima ameaça à segurança e o que fazer a respeito. Ed. Kindle. Rio de Janeiro: Brasport, 2015.

EXÉRCITO. **Liberdade de ação no espaço cibernético**. Disponível em: <http://www.epex.eb.mil.br/index.php/defesa-cibernetica>. Acesso em: 10 maio 2020.

G1, **Olimpíada Rio 2016 teve quase 3 incidentes cibernéticos por hora.** Disponível em: <https://g1.globo.com/tecnologia/noticia/olimpiada-rio-2016-teve-quase-3- incidentes-ciberneticos-por-hora.ghtml>. Acesso em: 10 set 2020.