O Sistema Militar de Defesa Cibernética e seus reflexos para a Defesa Nacional

Alan Denilson Lima Costa[1]

Introdução

A Política Cibernética de Defesa estabelece, como um de seus pressupostos básicos, que as atividades de Defesa Cibernética no Ministério da Defesa são orientadas para atender às necessidades da Defesa Nacional.

Para que esse pressuposto seja observado, é importante identificar claramente quais são as necessidades da Defesa Nacional que estão relacionadas a esse novo setor estratégico da Defesa — o Setor Cibernético —, de forma a definir acertadamente as atitudes, medidas e ações que devem ser tomadas pelo Estado brasileiro para neutralizar as potenciais ameaças cibernéticas que possam afetar a consecução ou a manutenção dos Objetivos Fundamentais[1] da nação.

Os agentes de tais ameaças podem ser atores estatais ou não estatais (pessoas, grupos ou organizações) com motivação e capacidade técnica para, por meio do espaço cibernético, explorar vulnerabilidades encontradas nos ativos de informação de interesse. Realizam, sem autorização legal, ações orientadas a acessar, extrair, danificar ou destruir dados ou informações sensíveis em trânsito nas redes ou armazenados em sistemas de informação utilizados por órgãos governamentais, empresas, ou indivíduos.

Esse mesmo espaço cibernético que é utilizado pelos agentes da ameaça para realizar suas ações, é o pilar que sustenta e dinamiza a grande engrenagem de interdependência global existente em nossos dias, quando a agenda política internacional tem uma grande amplitude e é influenciada por um grande número de atores estatais e não estatais.

Nesse cenário contemporâneo, os estados soberanos se encontram em uma situação em que não têm o controle absoluto sobre o fluxo de informação de natureza transnacional que atravessa as suas fronteiras físicas. Essa fragilidade gera, naturalmente, uma sensação de insegurança, por não conseguirem exercer, de forma efetiva, a soberania westfaliana clássica.

Da análise da **Figura 1**, verifica-se que, dependendo do objeto referente da ameaça cibernética, que pode ser externa ou inter-

---

[1] Cel Com (AMAN/87), mestre em Segurança e Defesa (ECEME), mestre em Segurança, Defesa e Integração pelo Instituto de Altos Estudos da Defesa Nacional da Venezuela. Foi comandante do Centro de Instrução de Guerra Eletrônica. Atualmente exerce a função de chefe do Estado-Maior Conjunto do Centro de Defesa Cibernética (CDCiber).

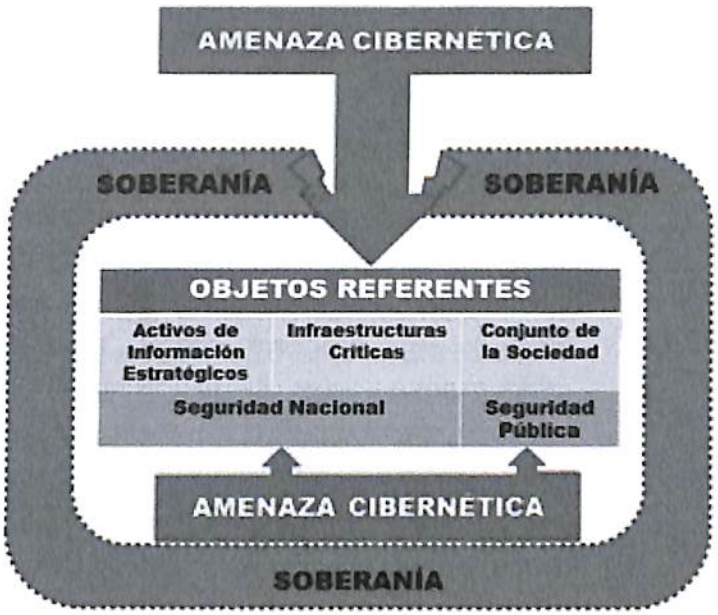


Figura 1 – A ameaça cibernética

Fonte: elaborado pelo autor e publicado em dissertação no Instituto de Altos Estudios de la Defensa Nacional de Venezuela[2]

na, as ações preventivas e/ou reativas a serem adotadas pelo Estado estarão enquadradas no âmbito da segurança pública ou da Defesa Nacional.

A figura nos mostra ainda que, quando o agente da ameaça cibernética orienta suas ações para os ativos de informação estratégicos ou para as infraestruturas críticas do país, configura uma ameaça à Segurança Nacional que deve ser combatida pelos meios de defesa do Estado.

Portanto, a ameaça cibernética que tenha como objeto referente um determinado ativo de informação estratégico para o país ou uma infraestrutura crítica de interesse da Defesa Nacional, com potencial para afetar um ou mais Objetivos Fundamentais (soberania, progresso etc.), deve ser percebida, identificada e combatida com os meios de Defesa Cibernética da nação.

Nesses casos, a eficácia das ações preventivas e reativas de Defesa Cibernética a serem conduzidas pelo Estado brasileiro por meio da aplicação efetiva do Poder Nacional dependerá, fundamentalmente, da atuação colaborativa de toda a sociedade brasileira, incluindo não apenas o Ministério da Defesa e as Forças Armadas, mas também outros órgãos e agências governamentais, a comunidade acadêmica, os setores público e privado e a base industrial de defesa.

A fim de colaborar com esse esforço nacional, as Forças Armadas brasileiras vêm desenvolvendo novas capacidades para atuar nesse novo domínio operativo — o domínio cibernético.

O espaço cibernético como um novo domínio operativo

Fruto dos avanços tecnológicos trazidos pela revolução industrial, máquinas de guerra nunca antes vistas foram empregadas, de forma inovadora, nos campos de batalha da Segunda Guerra Mundial.

Aquelas novas tecnologias aplicadas ao material de emprego militar permitiram o nascimento da Guerra Relâmpago (*Blitzkrieg*) e o emprego de porta-aviões, submarinos, modernos caças bombardeiros etc., transformando a arte da guerra e consolidando os três domínios operacionais clássicos: terrestre, naval e aéreo.

Durante o período da Guerra Fria, o mundo presenciou o lançamento da *Strategic Defense Initiative*, também conhecida como "Guerra nas Estrelas", por parte do governo dos Estados Unidos da América, que tinha como objetivo desarticular qualquer tipo de ameaça nuclear contra os interesses norte-americanos, consolidando uma nova dimensão operacional, a espacial.

Todos esses fatos sumariamente descritos acima atestam que a transformação da guerra se dá pela integração de dois elementos: a nova tecnologia disponível e o cenário operativo onde a empregamos.

O mundo assistiu, ainda, durante a segunda metade do século XX, a uma extraordinária revolução tecnológica, que se caracterizou pelo desenvolvimento de uma crescente capacidade de processamento e de transferência de dados a distância, consolidando as bases da atual rede mundial de computadores, a Internet.

O século XXI, que alberga a sociedade da informação, é marcado pelo uso intensivo das Tecnologias da Informação e Comunicações (TIC) que implementaram profundas transformações no modo como os estados e seus sistemas de defesa operam.

Nos dias atuais, governos e empresas, públicas e privadas, empregam uma intrincada e complexa rede de computadores e sistemas de informação para gerenciar instalações, serviços, bens e sistemas essenciais para o funcionamento da sociedade. Esses ativos, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, com reflexos diretos na segurança do Estado e da sociedade.

Essa crescente utilização das TIC, não só por parte dos Estados, mas também pelos indivíduos, cria novos riscos para todas as atividades realizadas através do espaço cibernético.

Como consequência desse fenômeno, quanto maior a utilização de sistemas de informação por parte de um Estado para gerir os seus processos críticos, mais ele estará exposto a ações cibernéticas hostis, que buscarão explorar falhas de segurança nas redes e sistemas de informação utilizados pelos órgãos escolhidos como alvo, com o objetivo de extrair informações estratégicas ou sabotar processos vitais para a nação.

Observando esse cenário pelo prisma da estratégia militar e assumindo que as forças militares também dependem, em maior ou menor grau, do espaço cibernético para comandar e controlar as suas ações, empregar seus sistemas de armas e de vigilância, controlar o espaço aéreo, entre outras atividades operativas, constata-se que o espaço cibernético entrou sem ser convidado no tabuleiro multidimensional da guerra, tornando-se um novo domínio operacional a ser considerado nos planejamentos militares — o domínio cibernético.

O domínio cibernético permeia todos os demais, e as ações realizadas no espaço cibernético, sejam elas de caráter defensivo ou ofensivo, contribuem para a obtenção ou para a manutenção da liberdade de ação necessária ao desencadeamento de ações em outros domínios. O contrário também é verdadeiro, visto que os cinco domínios operacionais estão integrados.

O objetivo central da integração dos domínios é potencializar a sinergia entre as capacidades inerentes a cada um deles, de forma a gerar um efeito único e, frequentemente, decisivo no espaço de batalha.

Para combater nessa nova dimensão, as forças militares devem dispor de novas capacidades e estar em condições de empregá-las em todo o espectro dos conflitos.

O Sistema Militar de Defesa Cibernética

A Teoria Geral de Sistemas, formulada pelo biólogo alemão Ludwig von Bertalanffy em seus trabalhos publicados entre 1950 e 1968, estabelece que todo sistema deve constituir um todo harmônico e coerente, integrado por um conjunto de subsistemas interdependentes, que, dentro de um conceito de divisão do trabalho, realizam funções especializadas que se complementam e, de forma sinérgica, geram o produto do sistema.[3]

Concebido a partir dessa visão sistêmica clássica, o Sistema Militar de Defesa Cibernética (SMDC) é definido como um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal, essenciais para realizar as atividades de defesa no espaço cibernético.

O SMDC tem por finalidade assegurar, de forma conjunta, o uso efetivo do espaço cibernético pelas Forças Armadas bem como impedir ou dificultar a sua utilização contra interesses da Defesa Nacional. Além disso, cabe ao SMDC assegurar a proteção cibernética do Sistema Militar de Comando e Controle (SISMC²), garantindo às Forças Armadas a capacidade de atuar em rede com segurança bem como coordenar e integrar a proteção das infraestruturas críticas da informação de interesse da Defesa Nacional, definidas pelo Ministério da Defesa.

Uma importante característica dos sistemas é a subsidiariedade, pois nenhum sistema é completo em si mesmo. Segundo a Teoria Geral de Sistemas, todo sistema é um subsidiário em sua delimitação e nos insumos que recebe ou fornece a outros sistemas que compõem o seu entorno e em virtude dos quais atua.[4]

Essa característica está presente no SMDC na medida em que ele interage intensamente com outros sistemas e órgãos que também estão inseridos no ambiente da Defesa Nacional.

Entre os principais sistemas relacionados à Defesa Nacional, destacam-se o SISMC2, o Sistema de Inteligência de Defesa (SINDE), o Sistema Nacional de Mobilização (SINAMOB), o Sistema de Mobilização Militar (SISMOMIL), o Sistema de Defesa Aeroespacial Brasileiro (SISDABRA), o Sistema de Controle do Espaço Aéreo Brasileiro (SISCEAB) e o Sistema de Ciência, Tecnologia e Inovação de Interesse da Defesa Nacional (SisCTID).

O Centro de Defesa Cibernética (CDCiber), órgão central do Sistema, é a organização militar responsável pela orientação, supervisão e condução das atividades do SMDC. Sua organização interna viabiliza o funcionamento dos subsistemas, verdadeiras engrenagens que movimentam os processos internos e geram o produto do SMDC: Forças Armadas capazes de atuar no domínio cibernético, com efetividade operativa.

Para que o SMDC seja capaz de cumprir sua finalidade e entregar o produto que a nação

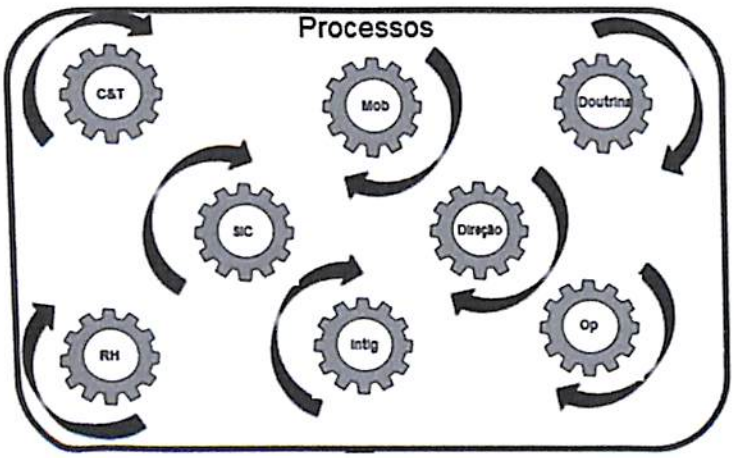


Figura 2 – Subsistemas do Sistema Militar de Defesa Cibernética
Fonte: elaborado pelo autor

brasileira espera, as Forças Armadas devem dispor de capacidades de Defesa Cibernética, ou seja, devem ser capazes de realizar, com eficácia, respeitados os limites de suas competências, todo o espectro de ações cibernéticas: proteção, exploração e ataque cibernéticos.

Dentro do conceito de geração de forças por meio do Planejamento Baseado em Capacidades (PBC), o Exército Brasileiro define capacidade como a aptidão requerida de uma força ou organização militar para que possa cumprir determinada missão ou tarefa. Uma nova capacidade é gerada a partir do desenvolvimento de um conjunto de sete fatores determinantes, inter-relacionados e indissociáveis: doutrina, organização (e processos), adestramento, material (e sistemas), educação, pessoal e infraestrutura, que formam o acrônimo DOAMEPI.

Para alcançar a efetividade operacional conjunta para combater no domínio cibernético, o primeiro passo é mapear as capacidades estruturantes e operativas que o SMDC deve possuir para cumprir missões ou tarefas relacionadas à Defesa ou Guerra Cibernéticas.

Terminada essa etapa, inicia-se a fase de desenvolvimento das capacidades, e para isso é necessário estabelecer o modelo de trabalho a ser seguido, de forma a observar todos os fatores do DOAMEPI.

Para desenvolver, integrar e preparar, de modo contínuo e permanente, as capacidades cibernéticas das Forças Armadas e do Ministério da Defesa, o órgão central do SMDC se vale do Programa da Defesa Cibernética na Defesa Nacional.

O aludido programa congrega vários projetos patrocinados pelo Ministério da Defesa, estabelecidos por meio da Portaria Normativa 2.777/MD, de 27 de outubro de 2014, que dispõe sobre a diretriz de implantação de medidas visando à potencialização da Defesa Cibernética Nacional.

Figura 3 – Ações cibernéticas
Fonte: elaborado pelo autor

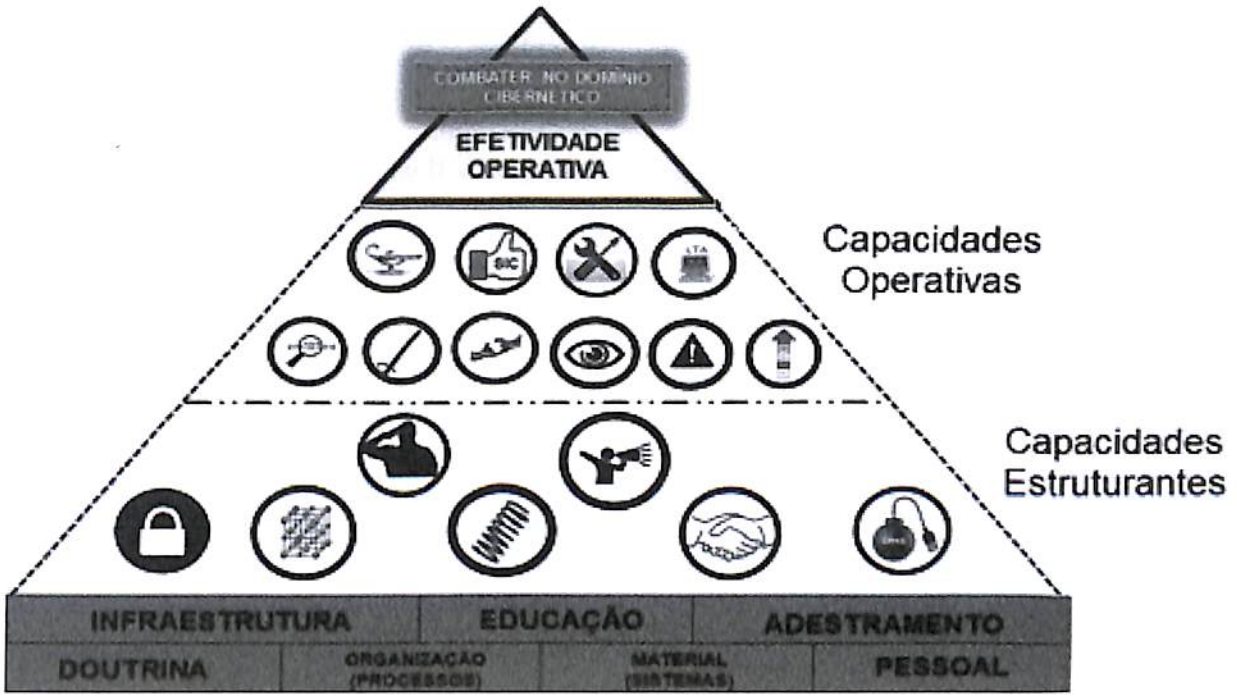


Figura 4 – Desenvolvimento das capacidades do SMDC
Fonte: elaborado pelo autor

Entre as medidas aprovadas pelo Ministério da Defesa, destacam-se: a criação do Comando de Defesa Cibernética (ComDCiber) e da Escola Nacional de Defesa Cibernética (EnaDCiber) bem como a imediata ativação dos seus núcleos de implantação (NuComDCiber e NuENaDCiber); o enquadramento das tecnologias do setor cibernético entre as prioritárias no âmbito do Ministério da Defesa; o desenvolvimento conjunto da Defesa Cibernética; a criação de um Sistema de Homologação e Certificação de Produtos de Defesa Cibernética; o apoio à pesquisa e ao desenvolvimento de produtos de Defesa Cibernética; e a criação do Observatório de Defesa Cibernética.

Uma vez desenvolvidas as capacidades estruturantes e operativas e alcançada a efetividade operativa conjunta para combater no domínio cibernético, o SMDC estará apto a:

a) gerenciar os níveis de alerta cibernético, em situação de normalidade institucional, crise ou conflito;
b) atribuir a autoria e responder a ataques cibernéticos dirigidos ao espaço cibernético de interesse do Ministério da Defesa e das Forças Armadas;
c) contribuir para a obtenção de vantagens estratégica, operacional ou tática, a partir da realização de ações no domínio cibernético, sincronizadas com a operação militar em curso;
d) efetivar a mobilização da capacidade cibernética nacional, sempre que necessário;

e) difundir oportunamente, no âmbito do SINDE, conhecimentos de Inteligência produzidos a partir de dados obtidos por meio da fonte cibernética; e
f) gerenciar e empregar pessoal qualificado nas diversas atividades do SMDC.

De forma subsidiária, o SMDC deverá ser capaz de promover a capacitação tecnológica do Setor Cibernético da Defesa em harmonia com a Política de Ciência, Tecnologia e Inovação do Ministério da Defesa; contribuir para a gestão da Segurança da Informação e Comunicações (SIC) no âmbito do Ministério da Defesa e das Forças Armadas; e contribuir para a sensibilização da sociedade brasileira acerca da relevância da Defesa Cibernética, no âmbito da Defesa Nacional.

O SMDC e as operações conjuntas

Para o perfeito entendimento do emprego das capacidades operativas do SMDC nas operações conjuntas, coordenadas pelo Ministério da Defesa, é necessário conhecer como os seus órgãos componentes se relacionam nos diferentes níveis de decisão.

No nível político, em que o ambiente operativo é interagências, o CDCiber, órgão central do SMDC, atua de forma colaborativa com o órgão da Presidência da República encarregado da Segurança Cibernética nacional e com o Comitê Gestor da Internet no Brasil (CGI.br).

Nesse nível, o CDCiber estabelece um canal técnico com o Centro de Tratamento de Incidentes de Redes de Computadores da Administração Pública Federal (CTIR Gov) e com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), órgão do CGI.br.

No nível estratégico, o CDCiber é a organização responsável pela coordenação e integração das ações de Defesa Cibernética no âmbito do Ministério da Defesa, cabendo-lhe: assessorar o comandante do Exército e o ministro de Estado da Defesa nas atividades do setor, formular doutrina e obter e empregar tecnologias; planejar, orientar e controlar as atividades operacionais, doutrinárias e de desenvolvimento das capacidades cibernéticas; e executar atividades de exploração cibernética, em conformidade com as políticas e diretrizes do Ministério da Defesa.

Para cumprir suas tarefas no nível estratégico, o CDCiber desenvolve continuamente as capacidades operativas necessárias à condução das ações cibernéticas no amplo espectro dos conflitos, em operações conjuntas ou singulares.

Em situação de normalidade institucional, o CDCiber coordena e integra a Defesa Cibernética com diversos órgãos do Ministério da Defesa, da Marinha do Brasil, do Exército Brasileiro e da Força Aérea Brasileira ligados ao SMDC, sendo necessário, portanto, que o desenvolvimento das capacidades estruturantes e operativas do Sistema se estenda às Forças singulares e ao Ministério da Defesa.

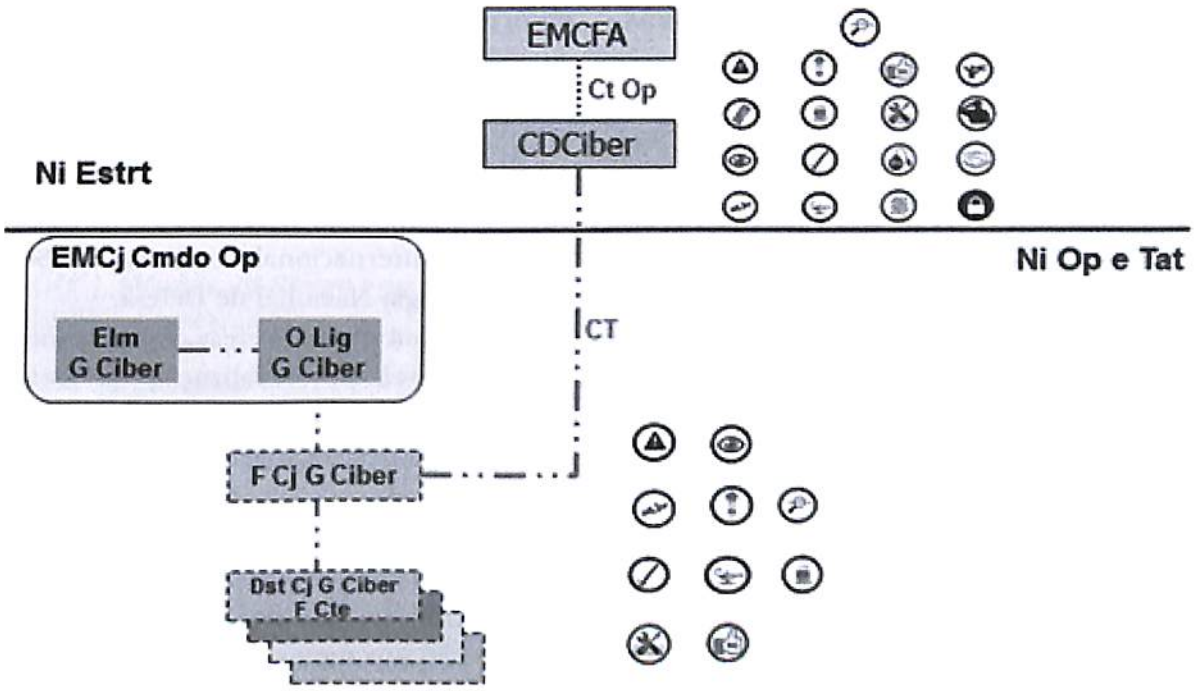
Para cumprir as tarefas acima, o CDCiber mantém canal técnico permanente com os órgãos de Defesa Cibernética dos Comandos das Forças Armadas, com as Equipes de Tratamento de Incidentes de Redes (ETIR) do Ministério da Defesa e de outras organizações parceiras e, também, com a Força Conjunta de Guerra Cibernética (F Cj G Ciber), quando constituída.

Nas operações conjuntas, o CDCiber passa ao Controle Operacional do Estado-Maior Conjunto das Forças Armadas (EMCFA) para coordenar e executar as ações cibernéticas no nível estratégico, além de integrá-las e acompanhá-las nos níveis operacional e tático.

O Emprego no nível operacional abrange as ações cibernéticas dentro de um Teatro de Operações (TO) ou de uma Área de Operações (A Op).

Nesse nível, o Estado-Maior Conjunto (EMCj) do Comando Operacional será integrado por elementos de Guerra Cibernética das três Forças Armadas. Esses elementos de Guerra Cibernética serão oficiais superiores, com Curso de Comando e Estado-Maior, e mobiliarão as diferentes seções do EMCj, assessorando nos assuntos relativos ao emprego da Guerra Cibernética.

O comandante operacional, assessorado pelo seu EMCj, emitirá ordem de coordena-



Legenda:

------- Controle Operacional (Ct Op)

—··— Canal Técnico (CT)

Figura 5 – Emprego nos diferentes níveis de decisão
Fonte: elaborado pelo autor

ção (O Coor), estabelecendo as prioridades, a responsabilidade pela execução das ações cibernéticas, o momento do desencadeamento e as medidas de coordenação necessárias. O comandante operacional também será responsável, dentro do controle da operação planejada, pela avaliação do desempenho operacional e dos efeitos das ações cibernéticas realizadas em proveito da campanha.

No nível tático, poderá ser constituída uma F Cj G Ciber, diretamente subordinada ao comandante operacional, com a atribuição de planejar e executar as ações cibernéticas previstas no plano operacional bem como coordenar as ações cibernéticas sob a responsabilidade das demais Forças componentes (F Cte).

Cada F Cte, por sua vez, deverá constituir o seu Dst G Ciber com as capacidades visualizadas para apoiar a operação planejada, ligando-se à F Cj G Ciber por meio do canal técnico estabelecido para a operação.

Considerações finais

O processo de evolução da sociedade digital tornou estados, organizações e indivíduos irreversivelmente dependentes do espaço cibernético e vulneráveis às ameaças cibernéticas.

Nesse cenário contemporâneo, no que se refere à Defesa Nacional, o Estado brasileiro deve dispor de meios de Defesa Cibernética capazes de perceber e se contrapor às ameaças cibernéticas orientadas aos ativos de informação estratégicos do país ou às infraestruturas críticas de interesse para a Defesa Nacional.

É importante salientar que esse esforço não é responsabilidade exclusiva do Ministério da Defesa e das Forças Armadas, mas depende da ação colaborativa de toda a sociedade brasileira, representada pelos segmentos governamentais, acadêmicos e empresariais.

Para que esse esforço seja efetivo, é preciso transformar o discurso em ação e intensificar a interação e a colaboração entre o Ministério da Defesa e os demais atores envolvidos com o Setor Cibernético, nos níveis nacional e internacional, conforme estabelece a Estratégia Nacional de Defesa.

No âmbito da Defesa, ações concretas visando à potencialização da Defesa Cibernética nacional estão sendo implementadas, e novas capacidades estão sendo geradas, de forma a tornar as Forças Armadas aptas a combater no domínio cibernético, com efetividade operativa, em todo o espectro dos conflitos, agregando valor substancial aos meios de Defesa Cibernética da nação brasileira.

Referências

BETZ. David J. and Stevens, Tim. ***Cyberspace and the State**: Toward a Strategy for Cyber-power*. London, UK: IISS, Routledge, 2011.

BRASIL. Escola Superior de Guerra. ***Manual Básico:** Elementos Fundamentais*. Rio de Janeiro, 2011.

_____. Presidência da República. **Decreto nº 6.703, de 18 de dezembro de 2008**. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Brasília, 2008.

_____. **Decreto nº 8.491, de 13 de julho de 2015**. Altera a Estrutura Regimental do Comando do Exército. Brasília, 2015.

_____. Ministério da Defesa. MD31-M-07. ***Doutrina Militar de Defesa Cibernética***. 1ª Edição. Brasília, 2014.

_____. MD31-P-02. ***Política Cibernética de Defesa***. 1ª Edição. Brasília, 2012.

_____. **Portaria Normativa nº 2777/MD, de 27 de outubro de 2014**. Dispõe sobre a diretriz de implantação de medidas visando à potencialização da Defesa Cibernética Nacional. Brasília, 2014.

_____. **Portaria Normativa nº 3.405/MD, de 21 de dezembro de 2012**. Atribui ao Centro de Defesa Cibernética, do Comando do Exército, a responsabilidade pela coordenação e integração das atividades de Defesa Cibernética, no âmbito do Ministério da Defesa.

CAMAREÑA, C. Audirac, ESTAVILLO, L. Verónica, GONZÁLEZ, A. Domínguez, GARCÍA, M. López, NEGRETE, L. Puerta. ***ABC del Desarrollo Organizacional***. Ed. Trillas. México, 2002.

COSTA, Alan. ***Cooperación regional en materia de ciberdefensa***: *nuevo reto para la UNASUR*. Trabajo de Grado MSc. Instituto de Altos Estudios de la Defensa Nacional (IAEDEN). Caracas, 2013.

EXÉRCITO BRASILEIRO. EB20-MF-10.102. ***Doutrina Militar Terrestre***. 1ª Edição. Brasília, 2014.

LUGO, J. Méndez. ***El Riesgo y su Entorno***. Instituto de Altos Estudios de la Defensa Nacional (IAEDEN). Caracas, 2008.

RODRÍGUEZ, Andrés G. ***El Ciberespacio***: *un nuevo teatro de batalla para los conflictos armados del siglo XXI*. Escuela Superior de Guerra. Bogotá, 2012.

STEPHEN D. Krasner. ***Power, The State and Sovereignty***: *Essays on International Relations*. London and New York: Routledge, 2009.

---

[1] Objetivos Nacionais que, voltados para o atingimento dos mais elevados interesses da Nação e preservação de sua identidade, subsistem por longo tempo (soberania, progresso, paz social, integridade do patrimônio nacional, integração nacional e democracia).

[2] COSTA, Alan. Cooperación regional en materia de ciberdefensa: nuevo reto para la UNASUR. Trabajo de Grado MSc. Instituto de Altos Estudios de la Defensa Nacional (IAEDEN). Caracas, 2013.

[3] CAMAREÑA, C. Audirac, ESTAVILLO, L. Verónica, GONZÁLEZ, A. Domínguez, GARCÍA, M. López, NEGRETE, L. Puerta. ABC del Desarrollo Organizacional. Ed. Trillas. México, 2002.

[4] Ibidem.

NR: A adequação do texto e das referências às prescrições da Associação Brasileira de Normas Técnicas (ABNT) é de exclusiva responsabilidade dos articulistas.