OBSERVATÓRIO MILITAR
da Praia Vermelha
http://ompv.eceme.eb.mil.br/

Os desafios da capacitação de recursos humanos para a Defesa Cibernética

Henrique de Queiroz Henriques
Mestrando em Ciências Militares pelo Instituto Meira Mattos da ECEME

A partir do século XXI, o ciberespaço tem se configurado como um novo domínio de interação da humanidade ao passo que elementos básicos do dia a dia, assim como estruturas da sociedade passam a ser dependentes do uso do espaço cibernético, elevando este ambiente a um nível estratégico e demandando transformações no comportamento humano para lidar com as novas possibilidades, assim como despertando o interesse do Estado em controlar e defender esse domínio (MEDEIROS, 2019, p. 91).

O caráter anônimo e sem fronteiras que caracteriza o ciberespaço torna esse ambiente em um palco de assimetrias que suscita conflitos impensáveis há pouco tempo atrás, praticamente impossível de se identificar a origem dos atacantes ou mesmo se o vetor de um ataque cibernético é estatal, criminosos ou por um simples indivíduo (SOUZA, 2020, n. p.).

Dessa forma, a cibernética passou a ganhar espaço no pensamento e comportamento dos indivíduos, seja pra se inserir nesse novo mundo de tecnologias ou mesmo ter condições de atuar no espaço cibernético, como um agente de estado ou com objetivos escusos.

Para enfrentar esse ambiente operacional, marcado pela difusão de poder, incertezas, flexibilização de fronteiras e territórios, multiplicidade e anonimato de atores é necessário que a formação seja eficaz no desenvolvimento de capacidades que possibilitem o enfrentamento de toda sorte de atores e ameaças, principalmente por ser notório o crescimento de ocorrências cibernéticas no cenário internacional (BETZ, 2017, n.p.).

Nesse sentido, o Estado deve buscar formas de capacitar seus recursos humanos para fazer frente às novas demandas advindas do ciberespaço. O desafio inicial é a identificação do ponto de partida, pois como dito acima, a ameaça cibernética pode advir de um simples indivíduo, os chamados hackers. A partir dessa afirmação surgem novas perguntas: A partir de que idade um indivíduo se torna um hacker? Quais as capacidades que este indivíduo deve desenvolver para estar apto a explorar as possibilidades do mundo virtual? Se o Estado não se apropriar das capacidades desse indivíduo, empresas ou o crime organizado podem se aproveitar desse conhecimento? O Estado é capaz de formar seus quadros para Defesa Cibernética?

Ao nos debruçarmos nestes questionamentos chegamos a conclusão que a formação em cibernética pode se dar de diversas formas, seja individualmente ou mesmo começando por cursos na área da Tecnologia da Informação, no entanto, a "administração da violência" é de competência própria da profissão militar, o que os distingue de quase todos os civis, seja em sua formação básica ou mesmo nos cursos de especialização e extensão, sendo seu dever aprender a administrar a violência em diversos setores e ambientes operacionais (NETO, 2012, n.p.).

A capacitação militar voltada para a cibernética é de certa forma complexa, pois exige domínio de uma área nova do conhecimento e que demanda constante atualização requerendo altos níveis intelectuais, treinamento constante e certo pendor para a atividade, somados a responsabilidade de promover a segurança e a defesa da sociedade.

De acordo com a Estratégia Nacional de Defesa – END (Decreto 6.703/2008), o setor cibernético é essencial para a defesa nacional. Dessa forma, a END determina a constituição de uma organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar. Neste contexto, busca-se a formação de recursos humanos capazes de atuar em rede de computadores, auxiliando o aperfeiçoamento de procedimentos de segurança que reduzam as vulnerabilidades dos sistemas de Defesa Nacional (BACH DA GRAÇA, 2014, p.71).

Para enfrentar esses desafios, o Ministério da Defesa editou diversas diretrizes e portarias como a Portaria 3.028/2012, a DIRETRIZ MINISTERIAL N° 14/2009 e editou a Política Cibernética de Defesa (MD31-P-02), por meio da Portaria Normativa nº 3.389/MD, delegando ao Exército Brasileiro a responsabilidade de coordenar e integrar o setor cibernético, definindo providencias para que seja cumprida a Estratégia nacional de Defesa em setores estratégicos (BACH DA GRAÇA, 2014, p.72).

Os desafios da formação em cibernética não se resumem ao indivíduo. Cada vez mais a Defesa Cibernética tem sido prioridade de governos mundo a fora, principalmente pela crescente dos ataques cibernéticos em diversos setores, seja estatal ou empresarial. Esses investimentos contínuos buscam assegurar capacidades cibernéticas em todo espectro das operações militares, identificando e responsabilizando os atores estatais ou não, como o realizado pelos Estados Unidos da América em sua estratégia Nacional de Defesa, investindo bilhões de dólares no setor, custo esse pago pela sociedade. (SOUZA, 2020, n. p.).

Para alcançar o objetivo de formar seus recursos humanos em cibernética o Exército precisou definir qual o universo a capacitar, bem como quais as capacidades necessárias para desempenhar as diversas atividades ligadas a Defesa Cibernética. Dentro desse contexto, definiu-se que o devemos entender que a capacitação em cibernética se desenvolve em 5 (cinco) níveis, quais sejam: USUÁRIO (Utiliza os sistemas de TI), TÉCNICO (Implementa sistemas de TI), ACADÊMICO (Programador, desenvolvedor de redes), PENTESTER (Aplica técnicas de defesa ativa), DESENVOLVEDOR 1 (Cria

programas e técnicas de defesa), DESENVOLVEDOR 2 (Cria técnicas e programas contra sistemas operacionais).

Entende-se que o caminho para que tenhamos um profissional em Cibernética é longo e complexo, demandando disponibilidade e auto-aperfeiçoamento contínuo, o que nos evoca a necessidade de mesmo após os diversos cursos de especialização, este profissional necessitará permanecer ativo no campo, de forma a participar de eventos de atualização como **LAAD** Defense & Security - Feira Internacional de Segurança Pública e Corporativa, eventos da BLACKHAT (Empresa especializada em treinamentos e eventos em segurança da informação).

Outro desafio enfrentado pela formação de guerreiros cibernéticos é assegurar privacidade e outros direitos fundamentais. Proteger o Estado de ataques cibernéticos é a essência a ser buscada, porém não basta investir em tecnologias e capacitação técnica de pessoal, mas também em regulação jurídica de defesa cibernética, devendo ser específica para as situações de amplo espectro do combate virtual, já que institutos como o Marco Civil da Internet possui posição diversa relativa da guerra cibernética, colocando barreiras a atuação e limitando o alcance do Estado (BACH DA GRAÇA, 2014, p.77).

Nesse sentido, a capacitação em cibernética é permeada de desafios e se caracteria por uma formação precoce e de aperfeiçoamento continuado, já que o ambiente virtual é volátil e incerto, multifacetado e em constante evolução. A Tecnologia da Informação e suas ramificações estão altamente presentes no conflito de 4ª Geração e a cibernética ganha papel relevante nesse contexto, o que nos leva a reflexão de como o Estado deve encarar essa capacitação.

Devemos definir se formamos os recursos humanos desde o início da carreira militar, capacitamos àqueles que se voluntariam para o trabalho na área ou até mesmo recrutar aqueles que despontam como ícones no setor privado, ou mesmo com histórico duvidoso para que possamos construir uma rede capaz de identificar e proteger as infra-instrutoras estratégicas e garantir o funcionamento dos sistemas operacionais essenciais para a nação brasileira.

Rio de Janeiro - RJ, 27 de abril de 2021.

Como citar este documento:

HENRIQUES, Henrique de Queiroz. Os desafios da capacitação de recursos humanos para a Defesa Cibernética. **Observatório Militar da Praia Vermelha**. ECEME: Rio de Janeiro. 2021.

Referência:

BACH DA GRAÇA, Ronaldo. Regulação da Guerra Cibernética e o Estado Democrático de Direito no Brasil. **Revista de Direito, Estado e Telecomunicações**, v. 6, n. 1, 2014.

BETZ, David J. **Cyberspace and the State: Towards a Strategy for Cyber-power.** Routledge, 2017.

GOMES, Ulisses de Mesquita et al. Desafios estratégicos para segurança e defesa cibernética. 2011.

NETO, Jacintho Maia. Os desafios do ensino militar: transformando a pós-graduação stricto sensu em Ciências Militares. **Coleção Meira Mattos: revista das ciências militares**, n. 26, 2012.

MEDEIROS, Breno Pauli. Ciberespaço e relações internacionais: rumo a construção de um novo paradigma?. 2019.

SOUZA, Marcos Luiz da Cunha, GOLDONI, Luiz Rogério Franco. Custos econômicos da Guerra Cibernética. **Observatório Militar da Praia Vermelha**. Rio de Janeiro: ECEME. 2020

SOUZA, Marcos Luiz da Cunha, MEDEIROS, Breno Pauli, GOLDONI, Luiz Rogério Franco. Infraestrutura básica e vulnerabilidades cibernéticas. **Observatório Militar da Praia Vermelha**. Rio de Janeiro: ECEME. 2020