

# Proposta de metodologia para avaliação da capacidade cibernética

Thiago Itamar Plum\*

## Introdução

A Estratégia Nacional de Defesa (END), publicada originalmente em 2008, atribuiu ao Exército Brasileiro a responsabilidade de coordenar as atividades de Defesa Cibernética no âmbito das Forças Armadas. Desde então, o Sistema Militar de Defesa Cibernética (SMDC) vem conquistando o seu espaço nas atividades conjuntas coordenadas pelo Ministério da Defesa. Como maior exemplo disso, temos a participação do Comando de Defesa Cibernética em todas as operações conjuntas das Forças Armadas, compondo a Força Conjunta de Guerra Cibernética (F Cj G Ciber) ou o Destacamento Conjunto de Guerra Cibernética (Dst Cj G Ciber). Por serem ainda incipientes, esses setores carecem de estrutura, de processos bem definidos e de um melhor estudo do inimigo para prestar um assessoramento mais efetivo aos comandantes.

A atividade cibernética, atualmente, faz parte das tarefas desempenhadas pelas Forças Armadas desde os tempos de paz. De fato, a cibernética possui uma característica transversal única, permeando outras capacidades, como a Inteligência e as Operações de Informação<sup>1</sup>, por exemplo.

A evolução do conhecimento cibernético e o dinamismo do ambiente virtual pressupõem uma constante e crescente necessidade de capacitação e aperfeiçoamento na área, visando a auxiliar o processo decisório em todos os níveis. Nesse contexto, é possível visualizar uma das grandes carências da cibernética: a inexistência de uma metodologia capaz de prover aos

comandantes a consciência situacional adequada das capacidades cibernéticas dos diversos atores e ameaças presentes no domínio cibernético.

Por essa razão, o principal objetivo da metodologia proposta é o assessoramento objetivo, preciso e conciso ao chefe militar, que, mesmo não possuindo conhecimento específico na área de cibernética, travará contato com as capacidades cibernéticas do inimigo.

O tema está inserido no contexto de uma linha extremamente relevante nos tempos atuais, que ganhou especial vigência no âmbito do Exército Brasileiro em 2008, com a publicação da END. Nela, ficou atribuída ao Exército a responsabilidade da coordenação desse setor estratégico.

Desde então, o setor cibernético vem crescendo em ritmo acelerado, com destaque para eventos como a participação nos Grandes Eventos no Brasil na última década; a ativação do Comando de Defesa Cibernética, em 2016; e a ativação da Escola Nacional de Defesa Cibernética, em 2019. Esses exemplos são permeados, ainda, por uma diversa gama de intercâmbios, como o Exercício Ibero-Americano; a participação na Operação *Locked Shields*<sup>2</sup>, da OTAN; e a integração com as infraestruturas críticas da nação, exemplificada no *Exercício Guardião Cibernético*.

Atualmente, o setor cibernético brasileiro passa por um momento de consolidação. Com isso, cresce de importância a definição de processos, metodologias e doutrina capazes de melhor auxiliar o chefe militar, em consonância com as idiosincrasias atinentes às nossas Forças Armadas.

\* Maj Cav (AMAN/2005, EsAO/2015, ECEME/2021). Atualmente, integra o Centro de Defesa Cibernética.

## Alguns conceitos básicos

Com o objetivo de alcançar um nível mínimo de compreensão acerca do tema a ser abordado, serão definidos alguns conceitos básicos. Nesse escopo, serão apresentadas algumas ideias-força sobre os *atores cibernéticos*; as *ameaças cibernéticas* e, mais especificamente, como elas são capazes de influir em um conflito militar; e as *capacidades cibernéticas* ofensivas dos países.

O estudo de *ameaças cibernéticas* é uma atividade para a qual se dedicam cada vez mais recursos humanos e materiais. Diferentes conceitos e nomenclaturas são aplicados. O presente trabalho empregará a expressão *inteligência de ameaças*, assim definida como “o processo de aquisição, via múltiplas fontes, de conhecimento sobre ameaças a um ambiente” (BROMILEY, 2016, p. 4, tradução nossa). Um ponto fundamental para o entendimento do conceito citado é que a inteligência, caso não seja “acionável”, isto é, não tenha aplicação na prática, que não permita que se faça algo ou se tome uma decisão a partir dela, tem pouco ou nenhum valor.

Faz-se mister caracterizar, primeiramente, quem são os atores capazes de influir no domínio cibernético. Alguns documentos sobre cibernética dividem os atores em grupos, como a Estratégia Nacional de Segurança Cibernética do Reino Unido, que cita, entre os principais atores, os criminosos cibernéticos, Estados-Nação ou atores patrocinados por Estados-Nação, terroristas, *hacktivistas*<sup>3</sup> e *script kiddies*<sup>4</sup> (GRÃ-BRETANHA, 2016).

Os criminosos cibernéticos são definidos como aqueles que se utilizam de meios cibernéticos para perpetrar ou potencializar seus crimes, notadamente a fraude, extorsão e roubo de dados. A Estratégia Nacional britânica, de maneira bastante incisiva, atribui a grupos criminosos de origem russa (GRÃ-BRETANHA, 2016) a maioria dos crimes cibernéticos ocorridos no país.

Os Estados, ou atores patrocinados por Estados, podem ser considerados outro grupo relevante. Para a metodologia que este trabalho propõe, esses atores são, sem dúvida, os mais importantes. Normalmente, eles atingem efeitos mais danosos, por terem como alvos sistemas críticos do oponente, tais como os energéticos, financeiros, governamentais e de Defesa (GRÃ-BRETANHA, 2016). Cabe ressaltar, ainda, que, mesmo

que um determinado país não possua capacidades cibernéticas ofensivas próprias, atualmente é muito fácil adquiri-las junto a países mais desenvolvidos na área cibernética.

Os terroristas utilizam o domínio cibernético como meio de propagação de suas ações, com o intuito de atrair atenção da mídia e intimidar a população (GRÃ-BRETANHA, 2016), além de tentar reforçar seu processo de recrutamento. A capacidade ofensiva de terroristas pode ser considerada baixa, porém o impacto de suas ações é desproporcionalmente alto.

Os grupos *hacktivistas* são marcados por sua ideologia, atuando sempre contra a sua percepção de injustiças cometidas por governos ou entidades públicas ou privadas. A maioria das ações *hacktivistas* é direcionada a ataques de negação de serviços ou desfigurações de páginas. Algumas ações isoladas, entretanto, podem causar danos maiores e mais duráveis às suas vítimas (GRÃ-BRETANHA, 2016).

Os *script kiddies* não são considerados como ameaças cibernéticas nas doutrinas de defesa cibernética de alguns países, justamente por se tratar de indivíduos com baixa capacidade técnica para executar ataques de maiores consequências ou mesmo duração. Há que se levar em conta, entretanto, que a falta de segurança de muitos sistemas poderia permitir-lhes causar transtornos desproporcionais, afetando negativamente sistemas de informação de organizações ou entidades (GRÃ-BRETANHA, 2016).

Além dos atores citados, a doutrina canadense elenca o *insider*, ou seja, o ator que pertence ao órgão atacado, utilizando-se de sua posição interna para facilitar o acesso ao sistema a ser comprometido (CANADÁ, 2018). Os atores que constituem ameaças cibernéticas, portanto, podem ser enquadrados em uma ou mais categorias.

Da análise de todos os atores até o momento elencados, poder-se-ia atribuir apenas aos atores estatais a influência direta sobre um teatro de operações ou sobre um conflito militar. Não será essa, porém, uma visão algo limitada? O modelo a seguir ensina que a capacidade cibernética ofensiva pode ser construída de três maneiras: com as próprias forças, com voluntários e com mercenários, conforme demonstrado na **figura 1**.

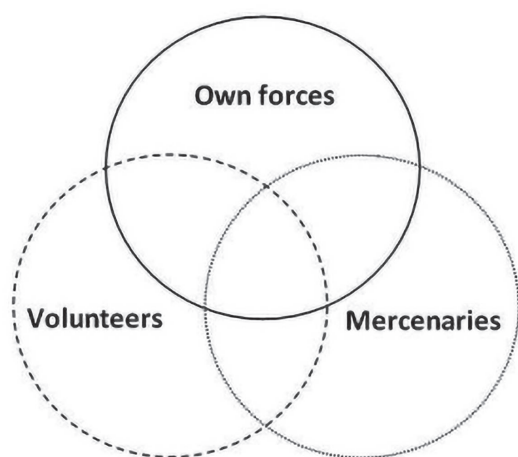


Figura 1 – A construção da capacidade cibernética ofensiva  
Fonte: OTTIS, 2009

Na primeira abordagem, Ottis (2009) observa que um Estado irá empregar a sua própria estrutura na construção de capacidades cibernéticas ofensivas. A principal vantagem desse método é a ligação direta com os recursos humanos e materiais da nação – que serão tão abundantes quanto a prosperidade dessa nação –, além da sinergia de esforços na implementação da capacidade ofensiva, provida pela unidade de comando inerente ao aparelho estatal, seja ele pertencente ao estamento militar ou não. Por outro lado, essa abordagem traz como principais desvantagens o alto custo de manutenção de uma força, que pode não vir a ser empregada, e a facilidade de atribuição de ataques cibernéticos ao Estado que se utilizar de suas próprias forças.

Ottis (2009) enumera, a seguir, a formação de forças voluntárias na construção de capacidades cibernéticas ofensivas. Esse método traz consigo vantagens significativas, especialmente a dificuldade na atribuição do ataque. A diversidade de talentos, localizações e técnicas, táticas e procedimentos (TTPs) pode gerar grande confusão no defensor, dificultando assim sobremaneira a sua resposta. Ainda como vantagem, é possível verificar o baixo custo de uma força voluntária, já que o Estado não assumiria as despesas de manutenção diretamente. Como principais desvantagens, o autor observa a necessidade de treinamento contínuo dessa “reserva” e a dificuldade em orquestrar um esforço cibernético ofensivo adequado.

Por fim, Ottis (2009) estuda a terceira abordagem: a força mercenária. Reconhecendo a complexidade, e mesmo a relutância das Forças Armadas de muitos países na contratação de mercenários, o autor considera esta a menos provável das três formas de construção da capacidade cibernética ofensiva. Ainda assim, destaca-se o anonimato desse tipo de operação, o que dificulta a atribuição e rastreabilidade do ataque. A utilização de mercenários pode ser demandada, ademais, por uma necessidade específica de capacidade não desenvolvida na própria força. A utilização de mercenários, porém, pode ser facilmente considerada a menos confiável de todas as abordagens descritas, tendo em vista a falta de compromisso com disponibilidade e qualidade dos mercenários a serem empregados.

Após o estudo dos atores, é importante verificar o que os transforma em ameaças. Para Ablon (2018), há necessidade de agrupar os atores por objetivos – algo muito semelhante ao que acaba de ser descrito –, por motivações e por capacidades. Esses dois últimos fatores são os verdadeiros vetores de transformação de simples atores em ameaças cibernéticas totalmente desenvolvidas.

O Departamento de Comércio dos Estados Unidos da América (EUA) define como ameaça cibernética “qualquer circunstância ou evento com potencial de impactar negativamente as operações de uma organização” (BADGER *et al.*, 2016). A definição não é ampla por acidente. As ameaças cibernéticas evoluem de maneira muito rápida, sendo cada vez mais contundentes e imprevisíveis.

Dessa forma, infere-se que os atores, munidos de uma ou mais motivações, procurarão realizar atividades no domínio cibernético, com vistas a causar efeitos diversos sobre seus alvos. O Centro de Segurança Cibernética do Canadá trata de efeitos cibernéticos específicos sobre os atributos de um sistema de informação, ou seja, disponibilidade, integridade e confidencialidade (CANADÁ, 2018). Já o manual de campanha *EB70-MC-10.232* (Guerra Cibernética) enumera, como efeitos de ataques cibernéticos, os de

interromper, negar o uso, degradar, corromper ou destruir sistemas computacionais ou informações armazenadas em dispositivos e redes computacionais e de comunicações de interesse. (BRASIL, 2017, p. 4-1)

A citada definição de ataque cibernético não esgota, contudo, o rol das capacidades cibernéticas de um oponente. Isso ocorre porque ela não considera diversas atividades que projetam poder de combate sem exercer um ou mais dos efeitos elencados. Ou seja, são atividades que moldam o ambiente e manipulam as ações inimigas, mas não têm, como resultado imediato, um efeito militar que consta da doutrina. Em que pese esse fato, é correto afirmar que tais ações exploratórias ou de manipulação do domínio cibernético conferem, sim, melhores capacidades aos seus atores.

Como exemplo do exposto, é possível citar a recente pesquisa sobre uma ameaça atribuída ao governo chinês, denominada *Naikon*. O grupo concentra suas atividades na implantação de *malware* em terminais da infraestrutura governamental de outros países, com o único intuito de extrair inteligência. As atividades do *Naikon* foram inicialmente reportadas por pesquisadores de segurança em 2015, porém eles se mantiveram ativos e seguiram espionando outros governos asiáticos. Recentemente, foram “redescobertos” pela empresa *Checkpoint* (2020), devido à reutilização de TTPs anteriormente vistas.

Nesse caso, não havia um efeito militar claro constante da doutrina brasileira. Ainda assim, não se pode descartar a grande capacidade dessa ameaça de operar no quinto domínio<sup>5</sup>, ainda mais se levado em conta o período de cinco anos (no mínimo) em que ela atuou despercebida. Esse tipo de ameaça, altamente dotada de motivação e paciência, veio a ser denominada *ameaça persistente avançada* (*advanced persistent threat*, ou *APT*).

Esse termo ganhou destaque com a evolução do cenário cibernético e da guerra cibernética nos últimos anos. A APT foi definida formalmente como um adversário que possui níveis sofisticados de habilidade e recursos significativos, utilizando-se de vetores de ataque diversos para atingir seu objetivo, e atuando em sua consecução por períodos prolongados (NIST, 2011).

Muitos dos principais ataques cibernéticos da história são atribuídos a APTs. É possível citar o exemplo da *GhostNet*, que foi descoberta em 2009 (CITIZEN LAB, 2009). A campanha, também com origem atribuída à China, atingiu quase 1.300 ativos de computação, em mais de 100 países. Um terço das máquinas infectadas eram consideradas de alto valor, localizadas em embaixadas, ministérios, órgãos da mídia e outros.

Outro caso relevante na história é o do *Deep Panda*. O grupo, de origem atribuída à China, comprometeu bases de dados para obter informações de cerca de quatro milhões de cidadãos americanos do *Office of Personnel Management*, ou OPM, algo como Escritório de Gerenciamento de Pessoal. Esse órgão possui dados de todos os servidores públicos dos Estados Unidos. Segundo pesquisadores de segurança, o objetivo do *Deep Panda* era montar uma base de dados para obter possíveis alvos de recrutamento (WAGSTAFF, 2015).

Faz-se mister conhecer, ainda, o grupo conhecido como APT28, também conhecido como *Fancy Bear*<sup>6</sup>. Trata-se de uma ameaça atribuída à Federação Russa, à qual se reputam ataques marcantes, destacando-se aqueles à Agência Mundial Antidoping (WADA), à Geórgia – durante o conflito entre os dois países –, e ao Comitê Nacional Democrata dos Estados Unidos. Esse último ataque é considerado como influência direta sobre o resultado da eleição de Donald Trump ao cargo de presidente dos EUA (MWIKI *et al.*, 2019).

Por fim, mas certamente não menos importante, cabe ressaltar a importância do *Stuxnet*<sup>7</sup> como talvez a primeira arma cibernética moderna. Não há, até hoje, um consenso acerca do Estado responsável pelo *Stuxnet*, ainda que EUA e Israel sejam amplamente considerados como os grandes suspeitos (KUSHNER, 2013). O ataque teve como principal objetivo comprometer as usinas de enriquecimento de urânio iranianas, e chegou inclusive a destruir<sup>8</sup> algumas turbinas.

O *malware* encerra em si a concepção mais didática de ameaça persistente avançada, já que possui características como a autoduplicação, por exemplo, passando de computador para computador de maneira não detectada. Outro controle que caracteriza a especialização do artefato é a capacidade de verificar automaticamente se o seu hospedeiro é um sistema *Windows*. Caso positivo, ele segue a sua implementação; caso negativo, torna-se dormente.

Esses são apenas alguns dos exemplos de APTs que demonstram grande capacidade no domínio cibernético. Seria possível citar, ainda, outros países proeminentes na área, como Irã, Grã-Bretanha e Coreia do Norte. O advento das APTs, a proeminência do domínio cibernético e o avanço tecnológico criaram um

novo paradigma de relações de poder, influenciando diretamente nas relações internacionais nos dias atuais.

No fim do século passado, quando o mundo conhecia uma ordem mundial bipolar, Estados Unidos e a então União Soviética chegaram a um impasse: ambos possuidores de armamento nuclear, viram-se confinados ao conceito de *destruição mútua assegurada*, ou MAD, no acrônimo em inglês<sup>9</sup>. Muitos autores estudaram a fundo esse conceito, com destaque para Thomas Schelling (1980), que conclui sobre as relações internacionais como essencialmente a manipulação compartilhada do risco da guerra, coagindo os outros países com ameaças veladas, assim garantindo um certo grau de segurança internacional. Esse foi, de fato, o paradigma das relações internacionais do período, ao qual Buchanan (2020) se refere como *signaling*.

O *signaling*, algo como  *sinalização* em português, servia justamente para demonstrar aos países estrangeiros as suas capacidades militares. Assim, buscava-se um fator dissuasório nas ações nacionais, especialmente nas expressões política e militar. De fato, o poder de convencimento não provinha apenas da posse de armas nucleares, mas também de exercícios no terreno, modernização do exército e outras práticas. Essas ações eram ostensivas, justamente por buscarem sinalizar aos possíveis adversários de um país que qualquer ataque seria prontamente rechaçado.

Paralelamente, atividades de espionagem e manipulação ocorriam, ainda que em menor escala. Com isso, os Estados tinham o fito de moldar o ambiente internacional e as relações bi e multilaterais. A essa doutrina, Buchanan (2020) deu o nome de *shaping*. O *shaping* pode ser utilizado tanto para avançar os interesses de um país amigo como para deter ou mitigar os interesses de países antagonistas.

É difícil imaginar um pareamento mais adequado do que o existente entre o cânone do *shaping* e o *hacktivismo*, assim compreendido como as atividades de *hackers* em favor dos interesses de um Estado. As atividades cibernéticas de espionagem, sabotagem e manipulação servem perfeitamente ao propósito da moldagem da geopolítica internacional, uma vez que se caracterizam pelo anonimato e obtenção de inteligência. Os benefícios da atividade no domínio ciber-

nético para a consecução de objetivos de moldagem do ambiente são incomparáveis.

Atualmente, “uma das principais maneiras como os governos moldam a geopolítica é *hackeando* outros países” (BUCHANAN, 2020, p. 17, tradução nossa). Essa assertiva fornece uma ideia da relevância do domínio do ambiente operacional cibernético em face dos desafios do mundo atual. De fato, as grandes potências atuais possuem um nível de maturidade avançado em suas estruturas e atividades cibernéticas. Em alguns casos, atuam diretamente no tecido social do oponente com o único intuito de causar dissenso, como no caso da já citada interferência russa nas eleições presidenciais dos EUA em 2016. As possibilidades são limitadas apenas pela capacidade dos atores de traduzir os planejamentos em ações.

Além disso, a guerra cibernética passou também a ser percebida como um fator de nivelamento de forças, por assim dizer. Isso veio inclusive a constar da doutrina militar americana, que afirma que

atores estatais e não estatais utilizam uma ampla gama de tecnologia avançada, que representa um meio barato para que adversários em piores situações materiais posem como ameaças significativas para os EUA. A aplicação de capacidades cibernéticas de baixo custo pode prover uma vantagem contra uma nação ou organização dependente de tecnologia. Isso pode provocar uma vantagem assimétrica para aqueles que, em outras situações, jamais se oporiam às forças militares dos EUA. (EUA, 2018, p. 26, tradução nossa)

## **Crítérios utilizados na proposta de metodologia**

Definidas as ameaças cibernéticas, é possível estabelecer quais critérios serão utilizados na avaliação de suas capacidades cibernéticas. O objetivo maior é, conforme exposto, focar no assessoramento ao chefe militar. Nesse escopo, cresce de relevância a utilização de um processo militar, ou pelo menos que se assemelhe a um.

A avaliação da capacidade cibernética de uma ameaça não é tarefa simples. Ela tampouco é estanque, devendo ser constantemente revisada e atualizada, da mesma maneira que o estudo do inimigo é realizado de maneira cíclica. A metodologia proposta tem por objetivo a atribuição de um valor quantitativo às capacidades cibernéticas ofensivas de uma ameaça. Por isso

será estabelecida uma escala de 0 a 10 pontos, onde “0” significa pouca ou nenhuma capacidade, e “10” capacidade extremamente desenvolvida.

O manual de *Doutrina Militar Terrestre* (BRASIL, 2019) consubstanciou o Planejamento Baseado em Capacidades no âmbito do Exército Brasileiro. Essas, por sua vez, possuem fatores determinantes, a saber: doutrina, organização, adestramento, material, ensino, pessoal e infraestrutura (DOAMEPI). Com o incremento desses fatores, portanto, a capacidade será gerada ou melhorada conforme o caso. É prudente, então, utilizar esses fatores na proposta de metodologia que será empregada.

Cabe ressaltar que não há um valor fixo para cada aspecto dentro dos parâmetros do DOAMEPI, permitindo que o analista tenha maior flexibilidade na atribuição da nota. Em que pese tornar o processo mais subjetivo, entende-se que essa maneira permite uma melhor adaptação a novas situações ou exceções às regras elencadas.

A *doutrina* pode ser considerada um fator ligeiramente mais preponderante do que os demais em razão de a base doutrinária de uma organização ser a responsável por ditar a sua geração de capacidades. Ou seja, uma organização – força armada ou não – não irá, pelo menos em tese, buscar desenvolver uma capacidade que não esteja em sua base doutrinária. Da análise da base doutrinária, destacam-se três componentes, que vêm a ser os parâmetros a serem estudados. Eles dizem respeito sobretudo à maturidade da doutrina, sua flexibilidade e a liberdade de ação por ela provida. Assim, foram considerados, no **quadro 1**, os seguintes parâmetros:

| Parâmetro         | Indicador   |
|-------------------|---|
| Maturidade        | Há quanto tempo a ameaça possui documentos que tratem sobre cibernética?                      |
|                   | Existe documentação destinada aos níveis político, estratégico, operacional e tático?         |
|                   | Há quanto tempo foi a última revisão doutrinária?   |
| Flexibilidade     | A doutrina em vigor garante flexibilidade no domínio cibernético?                             |
| Liberdade de ação | Quais as retaliações ou sanções passíveis de serem sofridas mediante um ataque cibernético?   |
|                   | O ataque cibernético é previsto explicitamente na doutrina?                                   |
|                   | Existe histórico de ações cibernéticas ofensivas?   |
| Emprego sistêmico | As ações cibernéticas são vislumbradas como modeladoras do ambiente operacional?              |
|                   | A doutrina vigente prevê o emprego de ações cibernéticas em todas as operações?               |
|                   | A doutrina vigente prevê o emprego de ações cibernéticas nas Operações de Apoio à Informação? |

Quadro 1 – Doutrina  
Fonte: O autor

Esses parâmetros são, portanto, os aspectos a serem examinados para que se chegue a um valor quantitativo do fator doutrina.

A *organização* de uma entidade é definida pelo manual de *Doutrina Militar Terrestre* como “a Estrutura Organizacional dos elementos de emprego”. A principal característica da *organização* na geração de capacidades é evitar a redundância de competências. Desse conceito, compreende-se como fundamental a definição de estruturas de direção, gestão e planejamento, conforme parâmetros no **quadro 2**:

| Parâmetro                       | Indicador   |
|---------------------------------|---|
| Articulação nos níveis do poder | Existem organizações que tratam sobre cibernética nos níveis político, estratégico, operacional e tático? |
|                                 | As organizações existentes possuem estrutura adequada para cumprir sua missão?                            |
|                                 | Há sinergia e cooperação entre organizações militares e civis, como indústria e academia?                 |
| Direção e gestão                | A estrutura organizacional está organizada de maneira a facilitar a orientação de esforços?               |
|                                 | Os processos estão bem definidos?   |
| Planejamento                    | Existem estruturas responsáveis pelo planejamento?  |
| Resiliência                     | A estrutura é resiliente?   |

Quadro 2 – Organização  
Fonte: O autor

O estudo da organização de uma ameaça é fundamental, conforme se pode perceber, para o assessoramento preciso ao chefe militar. A compreensão específica dessa idiosincrasia poderá não apenas auxiliar na defesa contra uma ameaça, mas também permitirá revelar possíveis pontos fracos.

O *adestramento* corresponde às atividades de preparo, utilizando as três formas de simulação: virtual, construtiva e viva (BRASIL, 2019). Mas o que seria cada uma dessas formas no domínio cibernético? O *Exercício Guardião Cibernético 2.0*, realizado em 2019, utilizou duas dessas formas de simulação: a virtual e a construtiva (DEFESANET, 2019). Naquela oportunidade, foram utilizadas mesas de discussão com grupos de trabalho (a simulação construtiva) e um Simulador de Operações Cibernéticas (a simulação virtual). Mas o que seria uma simulação viva? Ora, é possível citar um exercício de *Red Teaming* como um exemplo de simulação viva, em que atores reais utilizam sistemas reais para atacar ativos reais, simulando o comportamento de um atacante. Os parâmetros observados no aspecto adestramento são os seguintes, conforme o **quadro 3**:

| Parâmetro       | Indicador   |
|-----------------|---|
| Simulações      | São realizados exercícios dos três tipos existentes de simulação? |
|                 | Os exercícios são realizados periodicamente?                      |
|                 | Os exercícios são realizados de forma conjunta?                   |
|                 | Há exercícios combinados?   |
| Preparo cíclico | Existe um ciclo previsto de adestramento?                         |
| Experiência     | A ameaça é experiente na atuação no domínio cibernético?          |

Quadro 3 – Adestramento

Fonte: O autor

O adestramento reflete diretamente no desenvolvimento das capacidades ofensivas de uma ameaça cibernética, já que muitas das simulações possuem também um efeito dissuasório, muito relevante nos tempos atuais. Se um grupo ou país demonstra possuir uma certa capacidade ofensiva, muito provavelmente isso será notado por outros países.

O fator *material* engloba todos os materiais e sistemas disponíveis para uso por um ator, com ênfase no desenvolvimento e prospecção tecnológica. Dessa forma, os meios que um ator cibernético utiliza irão, sem dúvida, influenciar sua capacidade de atuação.

Esse fator gera ampla discussão entre especialistas. De um lado, existe uma corrente de pensamento que defende a ideia de que a capacidade cibernética é barata, e contribui para a diminuição da assimetria em um conflito. Ross Rustici (2011) considera que a capacidade destrutiva de Estados pobres ou fracos é sem precedentes nos dias atuais, devido ao baixo custo de um arsenal cibernético.

Por outro lado, alguns estudiosos do assunto defendem um ponto de vista um pouco diferente. Ainda que haja um consenso sobre o baixo custo da aquisição de capacidade cibernética limitada, o verdadeiro poder cibernético demanda alto custo de investimento. Armas cibernéticas elaboradas, como o Stuxnet, já estudado neste trabalho, tiveram seu custo projetado em cerca de 3 milhões de dólares (STIMPSON, 2015).

No presente estudo, o parâmetro material será dividido entre *hardware* e *software*, basicamente as duas ramificações de sistemas de tecnologia de informação, suficientes para uma análise bastante abrangente da geração ou aquisição de capacidades cibernéticas por parte de um Estado, conforme **quadro 4**:

| Parâmetro                                 | Indicador   |
|---|---|
| Ferramentas e soluções de <i>software</i> | A ameaça possui a capacidade de adquirir soluções cibernéticas?                   |
|   | A ameaça possui a capacidade de desenvolver soluções cibernéticas?                |
| Material e soluções de <i>hardware</i>    | A ameaça tem a capacidade de fabricar suas próprias soluções de <i>hardware</i> ? |

Quadro 4 – Material

Fonte: O autor

Como se pode observar, o grande diferencial nesse quesito é a capacidade de desenvolver tecnologia. Os Estados que possuírem essa capacidade estarão, indubitavelmente, à frente dos demais.

O fator *educação* ou *ensino* “compreende todas as atividades continuadas de capacitação e habilitação, formais e não formais”. Sob esse prisma, o fator *educação* é fundamental no desenvolvimento e aquisição de capacidades cibernéticas ofensivas, de acordo com o que prescreve o **quadro 5**:

| Parâmetro           | Indicador  |
|---------------------|--|
| Capacitação         | A capacitação de recursos é feita de maneira contínua?   |
|                     | A capacitação em cibernética no âmbito nacional é reconhecida internacionalmente?                  |
|                     | A capacitação de recursos humanos é compartilhada com outros países?                               |
| Ambiente acadêmico  | A produção acadêmica em cibernética é influente no cenário global?                                 |
| Ambiente não formal | A produção não formal (blogs, fóruns, redes sociais) em cibernética é influente no cenário global? |

Quadro 5 – Educação

Fonte: O autor

Apesar de o ensino ser amplamente globalizado no mundo atual, ainda é possível afirmar que aqueles que detêm o conhecimento irão compartilhá-lo da maneira que lhes for mais conveniente. Por essa razão, uma alta capacidade no fator *ensino* reflete em alta capacidade no domínio cibernético.

O fator *pessoal* pode ser entendido como

uma abordagem sistêmica voltada para a geração de capacidades, que considera todas as ações relacionadas com o planejamento, a organização, a direção, o controle e a coordenação das competências necessárias à dimensão humana. (BRASIL, 2019, p. 3-4)

Assim, o fator *pessoal* é imprescindível para a geração de capacidades cibernéticas por parte de qualquer Estado. Nesse contexto, a capacidade cibernética poderá ser obtida por meio da capacitação (incluindo a retenção) de recursos, bem como os aspectos qualitativos e

quantitativos desses recursos humanos. Daí, podem-se verificar no **quadro 6** os parâmetros a serem estudados:

| Parâmetro                         | Indicador   |
|-----------------------------------|---|
| Captação de recursos humanos      | O ator estudado apresenta boa capacidade de recrutamento de elementos externos às Forças Armadas? |
|                                   | O ator estudado apresenta boa capacidade de retenção de recursos humanos nas Forças Armadas?      |
| Proficiência dos recursos humanos | A organização dispõe de pessoal com reconhecido nível técnico?                                    |
|                                   | A organização dispõe de pessoal especializado nas diferentes áreas funcionais?                    |
| Aspectos quantitativos            | O efetivo empregado nas operações gera a capacidade cibernética desejada?                         |

Quadro 6 – Pessoal  
Fonte: O autor

A partir da enumeração dos parâmetros, é possível perceber o grande desequilíbrio que o fator *pessoal* pode causar na guerra cibernética.

Por fim, a *infraestrutura* é o fator que encerra todos os elementos estruturais utilizados no suporte e emprego dos elementos de combate, de acordo com a especificidade de cada um (BRASIL, 2019). No caso da guerra cibernética, o estudo da *infraestrutura* é indissolúvel do estudo de uma ameaça, devido ao seu alto valor estratégico. A *infraestrutura* possui uma característica paradoxal: o seu incremento provoca normalmente a geração de mais capacidades cibernéticas, entretanto produz também o efeito indesejado de ampliar a superfície de ataque<sup>10</sup> de determinada organização. Os parâmetros analisados encontram-se no **quadro 7**:

| Parâmetro                   | Indicador   |
|-----------------------------|---|
| Exposição                   | Qual é o nível de exposição de ativos da organização na Internet?           |
|                             | Quais sistemas legados estão expostos?                                      |
| Infraestrutura estratégica  | Como estão dispostos os cabos submarinos que chegam ao território nacional? |
|                             | Quais são as estruturas estratégicas de interesse?                          |
| Características estruturais | Os sistemas da organização podem ser considerados resilientes?              |
|                             | Os sistemas da organização podem ser considerados relativamente seguros?    |
|                             | É possível verificar redundâncias nos sistemas da organização?              |

Quadro 7 – Infraestrutura  
Fonte: O autor

O fator *infraestrutura* encerra a parametrização do presente trabalho de acordo com o DOAMEPI. Com isso, objetiva-se uma avaliação abrangente da ameaça, pautada em critérios pré-definidos, que irão padronizar e nivelar os conhecimentos acerca do tema.

Cabe destacar que este estudo não pretende esgotar o assunto ou ser a palavra final no sentido de avaliar a

capacidade cibernética de uma nação. Trata-se, isso sim, de uma base, da aplicação da metodologia de maneira até certo ponto superficial, tendo em vista que o objetivo da proposta é uma metodologia adequada, e não realizar levantamentos sobre a capacidade cibernética de diversos países do mundo. Esta última é uma tarefa mais adequada para um *analista de inteligência de ameaças*<sup>11</sup>.

Ressalte-se, ainda, que a aplicação da presente metodologia preconiza o estudo contínuo da ameaça, tendo em vista o dinamismo do ambiente informacional. De maneira análoga aos *levantamentos estratégicos de área* (LEA) ou às conjunturas expedidas pelo Ministério da Defesa, o estudo das capacidades operativas do inimigo é uma atividade permanente.

## Conclusão

O SMDC vive, atualmente, um momento de consolidação e amadurecimento nos campos interno e externo. A END de 2008 lançou as bases do setor e iniciou os estudos para a implantação de uma estrutura compatível com o tamanho do desafio que enfrenta o Brasil em termos de defesa cibernética. Esse não é um processo simples, e envolve comprometimento e envolvimento dos decisores em todos os níveis, que irão atribuir à cibernética o peso a ela correspondente, seja em operações de guerra ou não guerra.

Ocorre que as nuances da guerra cibernética acabam por passar despercebidas quando não se têm os insumos necessários para a sua adequada priorização. A falta de conhecimento sobre o tema ainda é um óbice – mesmo nos países mais desenvolvidos, diga-se de passagem – para o planejamento e a execução das operações no amplo espectro.

O método proposto torna possível que o comandante possa intervir de maneira adequada, apoiado em aspectos objetivos. Além disso, a avaliação da capacidade cibernética baseada nas capacidades operativas (DOAMEPI) está alinhada com a Doutrina Militar Terrestre e a Doutrina de Operações Conjuntas vigentes. Dessa forma, a cibernética será estudada em termos mais familiares para o militar.

A metodologia oriunda desta pesquisa tem como premissa a flexibilidade. Caso algum parâmetro pertinente necessite ser incluído, o operador cibernético pode fazê-lo sem prejuízo ou exclusão de outros já




elencados. A subjetividade da quantificação é, nesse caso, proposital: a imposição de muitas restrições ou “amarras” ao analista pode tornar toda a metodologia inexequível, seja em virtude da evolução tecnológica ou da obsolescência de algum conceito. Deposita-se grande responsabilidade, portanto, na capacidade do analista de aplicar a metodologia da maneira mais fidedigna e objetiva possível.

Outra vantagem do sistema proposto é a possibilidade de realização de recomendações claras e inteligência acionável, ou seja, geração de tarefas, sejam elas de *proteção*, *exploração* ou *ataque cibernético*<sup>12</sup>. Um ponto muito importante para o analista é a comunicabilidade. O elemento especialista tem muita facilidade em tirar conclusões de um determinado fato, mas nem sempre visualiza a importância de transmiti-las ao decisor. Há que se ter em mente, portanto, a necessidade de objetividade e concisão no assessoramento.

Encoraja-se, ainda, a elaboração de conceitos sintéticos quando julgado necessário ou conveniente. Isso

permitirá uma ampliação da compreensão da situação, expandindo o resultado apresentado com o resultado obtido. Os aspectos mais importantes encontrados durante o levantamento deverão ser salientados, para que se possa entender como o analista chegou até aquele parecer. Os resultados poderão, ainda, ser integrados e compartilhados com outras células do estado-maior, notadamente a célula de inteligência e a de informações.

Por fim, espera-se que o presente trabalho seja útil aos responsáveis pelo estudo da capacidade cibernética do inimigo em todos os níveis, e não somente ao Comando de Defesa Cibernética. Visualiza-se a integração dos dados como fator fundamental de sucesso da aplicação da metodologia, que servirá como um guia para o assessoramento às autoridades. Com isso, o estudo pormenorizado das capacidades cibernéticas de um Estado ou organização permitirá maior precisão na tomada de decisão, seja qual for a ameaça que se apresente. 

---

## Referências

- ABLON, L. **Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data**. 2018. Disponível em: <[https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND\\_CT490.pdf](https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf)>. Acesso em: 25 set 2019.
- BADGER, L.; JOHNSON, C.; SKORUPKA, C.; SNYDER, J.; WALTERMIRE, D. **Guide to Cyber Threat Information Sharing**. 2016. Disponível em: <<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>>. Acesso em: 28 set 2019.
- BRASIL. MINISTÉRIO DA DEFESA. **Doutrina Militar de Defesa Cibernética**. Brasília, Brasil: Governo Federal, 2014.
- BRASIL. MINISTÉRIO DA DEFESA. **Doutrina Militar Terrestre**. 2. ed. Brasília, Brasil: Governo Federal, 2019.
- BRASIL. MINISTÉRIO DA DEFESA. **Estratégia Nacional de Defesa**. Brasília, Brasil: Governo Federal, 2008.
- BRASIL. MINISTÉRIO DA DEFESA. **Guerra Cibernética**. 1. ed. Brasília, Brasil: Governo Federal, 2017.
- BROMILEY, M. **Threat Intelligence: What It Is, and How to Use It Effectively**. 2016. Disponível em: <<https://www.sans.org/reading-room/whitepapers/analyst/threat-intelligence-is-effectively-37282>>. Acesso em: 17 maio 2020.
- BUCHANAN, B. **The Hacker and the State**. 1. ed. Cambridge, Massachusetts: Harvard University Press, 2020.
- CANADÁ. **National Cyber Security Strategy**. Canada: Public Safety Canada, 2018.
- CHECKPOINT. **Naikon APT: Cyber Espionage Reloaded**. 2020. Disponível em: <<https://research.checkpoint>.

com/2020/naikon-apt-cyber-espionage-reloaded/>. Acesso em: 20 maio 2020.

CITIZENLAB. **Tracking GhostNet: Investigating a Cyber Espionage Network**. 2009. Disponível em: <<https://citizenlab.ca/2009/03/tracking-ghostnet-investigating-a-cyber-espionage-network/>>. Acesso em: 18 maio 2009.

DEFESANET. **EGC 2.0 – Exercício Guardião Cibernético 2.0**. 2019. Disponível em: <<http://www.defesanet.com.br/cyberwar/noticia/33270/EGC-2-0---Exercicio-Guardiao-Cibernetico-2-0/>>. Acesso em: 26 maio 2020.

ESTADOS UNIDOS DA AMÉRICA. **Joint Publication 3-12: Cyberspace Operations**. [S.l.]: EUA, 2018.

GRÃ-BRETANHA. **National Cyber Security Strategy 2016-2021**. Reino Unido: Her Majesty's Government, 2016.

KUSHNER, D. **The Real Story of Stuxnet**. 2013. Disponível em: <<https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>>. Acesso em: 20 maio 2020.

MINARIK, T. **NATO Recognises Cyberspace as a “Domain of Operations” at Warsaw Summit**, 2016. Disponível em: <<https://ccdcoe.org/incyber-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/>>. Acesso em: 19 maio 2020.

MWIKI, H.; DARGAHI, T.; DEGHANTANHA, A.; CHOO, K.-K. R. **Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin: Theories, Methods, Tools and Technologies**. [S.l.: s.n.], 2019. 221-244 p. ISBN 978-3-030-00023-3.

NIST. **Managing Information Security Risk**. Estados Unidos da América: National Institute of Standards and Technology, 2011.

OTTIS, R. **Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability**. 2009. Disponível em: <[https://ccdcoe.org/uploads/2018/10/Ottis2009\\_TheoreticalModelForCreatingANation-StateLevelOffensiveCyberCapability.pdf](https://ccdcoe.org/uploads/2018/10/Ottis2009_TheoreticalModelForCreatingANation-StateLevelOffensiveCyberCapability.pdf)>. Acesso em: 24 set 2019.

RUSTICI, R. **Cyberweapons: Leveling the International Playing Field**. 2011. Disponível em: <<https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/Cyberweapons20-%20Leveling%20the%20International%20Playing%20Field.pdf>>. Acesso em: 25 maio 2020.

SCHELLING, T. **The Strategy of Conflict**. Cambridge, Massachusetts: Harvard University, 1980.

STIMPSON, R. **Cyberwarfare will not replace conventional warfare**. 2015. Disponível em: <<https://www.cfc.forces.gc.ca/259/290/317/305/stimpson.pdf>>. Acesso em: 26 maio 2020.

WAGSTAFF, J. **Hunt for Deep Panda intensifies in trenches of U.S.-China cyberwar**. 2015. Disponível em: <<https://www.reuters.com/article/us-cybersecurity-usa-deep-panda/hunt-for-deep-panda-intensifies-in-trenches-of-u-s-china-cyberwar-idUSKBN0P102320150621>>. Acesso em: 20 maio 2020. Uma proposta de aplicações de inteligência artificial ao SISFRON

---

## Notas

<sup>1</sup> A *Inteligência* é a atividade responsável pela produção de conhecimentos relativos a fatos e situações atuais ou potenciais que afetem o processo decisório. As *Operações de Informação* podem ser entendidas como ações coordenadas que concorrem para a consecução de objetivos políticos e militares. São executadas com o propósito de influenciar um oponente real ou potencial, diminuindo sua combatividade, coesão interna e externa e capacidade de tomada de decisão.

<sup>2</sup> O Brasil não compôs equipe própria, por não ser um país pertencente à organização, porém integrou a equipe espanhola.

- <sup>3</sup> Assim entendido pessoas que obtêm acesso ilegal a sistemas informacionais para avançar uma agenda política ou social.
- <sup>4</sup> Diferem dos *hackers* pela sua inexperiência e pouca idade, realizando ataques com ferramentas já prontas, já que não possuem capacidade de desenvolvimento.
- <sup>5</sup> A definição do espaço cibernético como *quinto domínio operacional* foi adotada pela OTAN em 2016, no Congresso de Varsóvia (MINARIK, 2016).
- <sup>6</sup> Os diferentes nomes atribuídos a grupos hacktivistas são produtos dos relatórios realizados por diferentes empresas de segurança. No caso específico em tela, por exemplo, *Fancy Bear* é um nome atribuído pela empresa FireEye; *APT28* é a nomenclatura adotada pela empresa Mandiant; *STRONTIUM* é o nome atribuído pela Microsoft. Entretanto todas essas empresas estão – em teoria – referindo-se à mesma ameaça.
- <sup>7</sup> *Malware* projetado especificamente para atacar sistemas operacionais que controlavam as centrífugas de enriquecimento de urânio iranianas, fabricadas pela empresa Siemens.
- <sup>8</sup> Observa-se aqui claramente, e de maneira até então inédita, o efeito militar do ataque cibernético.
- <sup>9</sup> O termo foi usado pela primeira vez nos anos 1960, por Donald Brennan, para designar o dilema: os efeitos de uma guerra nuclear serão tão devastadores que os países possuidores dessa capacidade só irão usá-la em casos extremos.
- <sup>10</sup> A superfície de ataque é o conjunto de todos os ativos que um atacante pode tentar explorar.
- <sup>11</sup> Assim entendida como o conhecimento necessário à prevenção ou mitigação de ataques cibernéticos.
- <sup>12</sup> A *proteção*, *exploração* e *ataque cibernéticos* são as três capacidades operativas da capacidade militar cibernética (BRASIL, 2017).