GUERRA CIBERNÉTICA
A PREMENTE RELEVÂNCIA PARA CONFLITOS FUTUROS

Capitão-Tenente GABRIEL **BOEHMER** LEITE

Encarregado da Divisão de Armamento - EsqdHS-1
Graduação em Ciências Navais na Escola Naval

FOTO: @aleksandarlittlewolf - www.freepik.com
Composição Fotográfica: 1ºSG Severiano

INTRODUÇÃO

Este artigo tem como propósito ressaltar a importância do conhecimento do ambiente cibernético, apresentando um baseamento conceitual e princípios, bem como marcos da Guerra Cibernética e aspectos disruptivos desta, de modo a arrazoar sua premência em conflitos modernos.

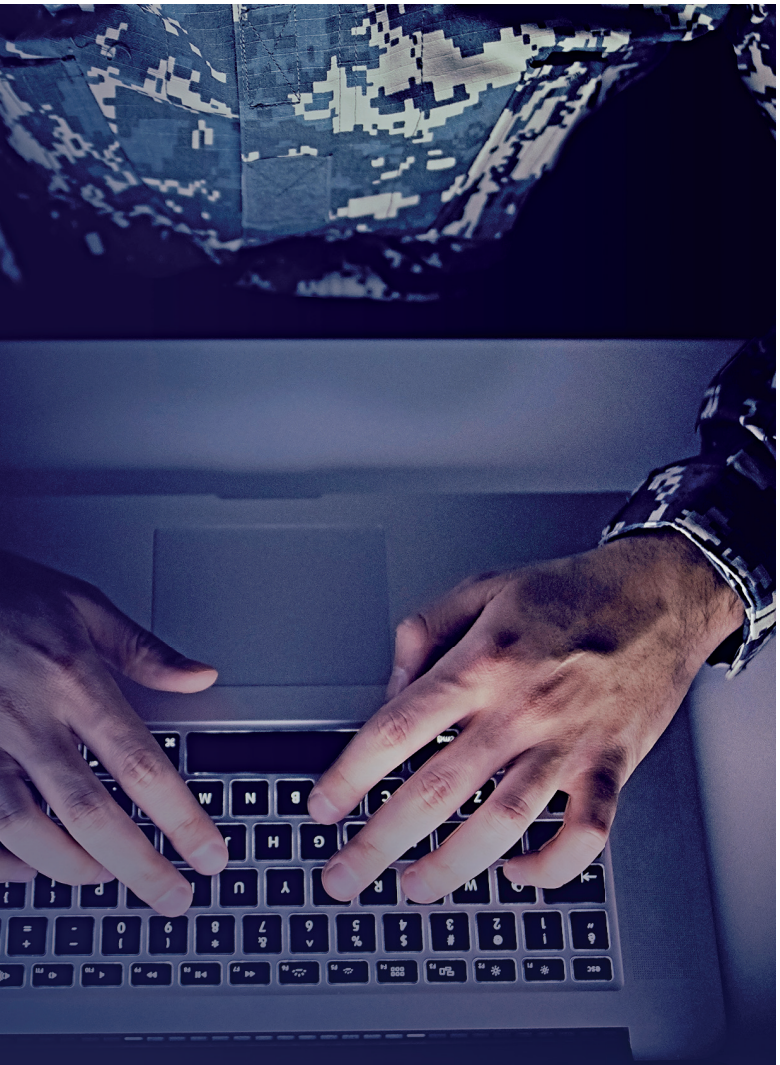
ASPECTOS INTRODUTÓRIOS E BREVE HISTÓRICO

Em virtude de uma latente demanda de gestão da informação disposta em locais fisicamente afastados, conduzida por uma economia dinâmica, competitiva e globalizada, desponta, no final do século XX, a Era da Tecnologia da Informação (TI).[1] A aplicação dos conceitos da TI fez que novo tipo de corpo social se consubstanciasse, recebendo a alcunha de "sociedade da informação". A TI, então, configurou-se alicerce da grande maioria dos ramos do conhecimento, estabelecendo uma espécie de sujeição paulatina de seus usuários.

No entanto, as vulnerabilidades[2] colaterais mostram-se proporcionais à sua extensão de atuação e, assim como em qualquer outro ambiente, são exploradas de forma ignominiosa, apoiando-se no anonimato e, principalmente, nas fracas barreiras de defesa, sobretudo devido à falta de conhecimento específico do assunto.

Por cúmulo, depreendeu-se a viabilidade de exploração de vulnerabilidades que compõe a rede de infraestruturas críticas de um Estado, a fim de se obterem informações confidenciais, realizarem-se sabotagens ou mesmo ter-se vantagem durante a ocorrência de conflitos, independentemente dos atores envolvidos (MENDONÇA, 2014).

Isso posto, podemos inferir que tais conceitos combinados atuam para alterar o formato da guerra como a conhecíamos. Na era da globalização, o advento da Guerra Cibernética apresenta nova lógica a geopolítica dos conflitos. A utilização do ciberespaço como ambiente de guerra influencia na natureza da guerra, nas funções a serem exercidas por combatentes e na própria eficiência das ações no teatro de operações.



O CONCEITO DE GUERRA CIBERNÉTICA

Guerra Cibernética (GC) ou ciberguerra pode ser definida como o uso de ataques cibernéticos (digitais) por um país ou nação para dissolver os sistemas de computadores de outro país ou nação, com o objetivo de gerar danos significativos e "comparáveis à guerra real" (SINGER e FRIEDMAN, 2014). Devido à sua contemporaneidade e fluidez de caracterização, neste artigo, será mostrado o conceito apresentado na publicação Doutrina Militar de Defesa Cibernética do Ministério da Defesa:

> Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de Comando e Controle (C2) do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC. (BRASIL, 2014).

De todo modo, orótulo "Guerra Cibernética" passou a ser comumente utilizado, devido ao fato de que ataques cibernéticos causam danos físicos e psicológicos a pessoas e objetos no mundo real e podem desestruturar tão ou mais dramaticamente os alicerces de uma nação quanto a um ataque "real", isto é, a invasão literal de países.

Com relação às Ações Cibernéticas a serem abrangidas pela GC, a referida Doutrina estabelece a seguinte divisão:

> Ataque Cibernético: compreende ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente.
> Proteção Cibernética: abrange as ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais e redes de computadores e de comunicações, incrementando as ações de Segurança, Defesa e Guerra Cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente.
> Exploração Cibernética: consiste em ações de busca ou coleta, nos Sistemas de Tecnologia da Informação de interesse, a fim de obter a consciência situacional do ambiente cibernético. Essas ações devem preferencialmente evitar o rastreamento e servir para a produção de conhecimento ou identificar as vulnerabilidades desses sistemas. (BRASIL, 2014)[3].

PRINCÍPIOS DA GUERRA CIBERNÉTICA

Em um Seminário apresentado em West Point, Parks e Duggan (2001) compararam, pioneiramente, princípios da guerra clássica com princípios que seriam utilizados na GC. Adicionalmente, concluíram que os princípios do ciberespaço diferiam e, então, elencaram novos princípios.

A Arte da Guerra de Sun Tzu, a exemplo, é frequentemente citada em publicações sobre operações de informação. Ao recomendar a manipulação da tomada de decisão do adversário, podemos estabelecer uma conexão com o princípio da GC de que esta deve ter um efeito no mundo real, a ser posteriormente exposto.

Clausewitz (1832), particularmente ao argumentar sobre a vontade, a névoa da guerra e o atrito da guerra descrevem possibilidades da GC, que podem objetivar a criação de uma névoa em um conflito, instaurar atrito, presente em um ciberespaço não confiável e, em casos mais sérios, minar a vontade combativa do adversário. A estratégia de Liddel-Hart (1954), por outro lado, encontra aplicabilidade à GC

por meio do princípio da aproximação indireta[4], contornando a defesa inimiga ou explorando seus elos mais fracos.

Isso posto, os princípios apontados na ocasião resumiam-se a: a GC só faz sentido se produzir algum efeito no mundo real, com obtenção de vantagens; toda ação no mundo virtual é visível, mesmo que medidas para dissimular sejam realizadas; não existem leis imutáveis de comportamento no mundo cibernético, exceto aquelas que possuem limitações do mundo físico; alguma entidade dentro do mundo cibernético tem autoridade, acesso ou capacidade de realizar qualquer ação que um invasor deseja realizar; as ferramentas de GC são de uso dual; quem controlar a parte do ciberespaço que o oponente utiliza pode controlar o oponente; o mundo virtual não é confiável nem consistente; e as limitações físicas de distância e espaço não se aplicam ao mundo cibernético.

Esses princípios prestam-se como base para um entendimento mais familiar do ciberespaço. A Doutrina Militar de Defesa Cibernética do Ministério da Defesa engloba, de forma pragmática e atualizada, os princípios anteriormente citados e complementam as peculiaridades do ambiente cibernético. São eles:

- Princípio do Efeito, em que as ações no Espaço Cibernético devem produzir efeitos que se traduzam em vantagem estratégica, operacional ou tática que afetem o mundo real;

- Princípio da Dissimulação, que pressupõe dificultar a rastreabilidade das ações cibernéticas ofensivas e explorat;

- Princípio da Rastreabilidade, cuja definição é detectar ações cibernéticas ofensivas e exploratórias contra os sistemas de TI e de comunicações amigos; e

- Princípio da Adaptabilidade, o qual assevera a adaptação à característica de mutabilidade do ciberespaço, mantendo a proatividade diante de mudanças súbitas e imprevisíveis.

ATAQUES CIBERNÉTICOS: MARCOS EVOLUTIVOS DA GUERRA CIBERNÉTICA

O ciberespaço é utilizado há muitos anos. Podemos, no entanto, estabelecer dois marcos iniciais na Guerra Cibernética, representados por dois casos de relevância. O primeiro, na Estônia, em 2007, evidencioua capacidade de um ataque cibernético em escala nacional, protagonizando o que podemos chamar de primeira guerra virtual (CLARK e KNAKE, 2010). O segundo, em 2010, é conhecido como o caso "Stuxnet", sendo considerado o primeiro ataque cibernético engendrado para neutralizar diretamente equipamentos físicos, ocorrido no Irã.

A série de ciberataques à Estônia em 2007 deixou diversos sites do governo fora do ar. A motivação teria sido a remoção da estátua do Soldado de Bronze de Tallinn, que homenageava a vitória russa contra o nazismo. À época, a Rússia foi acusada pelo governo estoniano, entretanto nada foi comprovado e a origem dos ataques é ainda desconhecida. É interessante pontuar que a Estônia é um país de infraestrutura amplamente informatizada e possui os serviços essenciais virtualizados, o que tornou o país alvo mais fácil desses ataques.

No caso Stuxnet, uma empresa de segurança digital da Bielorrússia, encontrou um *malware*[5] recôndito, que ocasionava uma falha de sistema (*crash*) em computadores com antivírus da empresa. Após análise por especialistas em segurança cibernética, o *malware*, chamado de Stuxnet, foi denominado com um sofisticado código, projetado exclusivamente para neutralizar as centrífugas das instalações nucleares de enriquecimento de urano iranianas. Além de um ataque cibernético com consequências inéditas a estruturas físicas, esse caso se tornaria, adicionalmente, o estopim de uma subsequente corrida global por armas cibernéticas.

FOTO: @rawpixel-com - www.freepik.com
Composição Fotográfica: 1ºSG Severiano

ASPECTOS DISRUPTIVOS SOB O REFERENCIAL DA GUERRA CIBERNÉTICA

A Guerra Cibernética apresenta possibilidades disruptivas com relação ao *modus operandi* da capacitação militar. Ataques com resultados catastróficos podem ser realizados a partir de estruturas

com baixo investimento de capital e poucas pessoas. Os pesados investimentos normalmente necessários para prontificação de contingentes militares massivos a longo prazo não se comparam ao estilo *asset light*[6] de unidades especializadas em exploração do ciberespaço, as quais podem ser rapidamente mobilizadas e adaptadas às rápidas mudanças tecnológicas. É claro que, para isso, faz-se necessário investimento base em TI. Este tipo de investimento, embora crescente no mundo todo, ainda é um desafio a países menos avançados.

Entretanto, não seria, paradoxalmente, uma opção para Estados com poder bélico inferior, aos moldes da concepção estratégica da *Jeune École*[7]? Guardadas as devidas proporções e adaptando-se aos tempos atuais, o propósito de utilizar unidades pequenas e poderosamente equipadas para combater uma frota maior de navios de guerra e minar o comércio naval da nação rival guarda interessante semelhança com as possibilidades do uso do ambiente cibernético em conflitos.

Podemos observar, adicionalmente, curioso aspecto no âmbito da seleção e gestão de pessoal a ser utilizada por Forças Armadas nesta empreitada. Combatentes vigorosos e disciplinados não seriam, exatamente, o produto esperado nesse caso. O ponto crítico passa a ser a necessidade de pessoal ultraespecializado, incluindo, talvez, indivíduos que não cumpram determinados requisitos médicos e físicos, exigidos ao serviço militar.

CONSIDERAÇÕES FINAIS

Assim sendo, podemos asseverar que, hodiernamente, o poder bélico assume, cada vez mais, dimensões ocultas e de difícil mensuração objetiva. A capacidade pugnaz em termos de quantidade de meios e combatentes já não seria a única forma de assegurar a inviolabilidade de um país, adaptando, inclusive, o conceito de dissuasão. A internet não possui fronteiras físicas, o inimigo permanece oculto e o ataque pode escalar as consequências de formas inesperadas, afetando o Estado tanto na esfera militar ou conflituosa, quanto na econômica e social.

A fusão de valores militares clássicos e aspectos de TI gera instabilidade entre os países, fazendo que os ataques cibernéticos se mostrem, silenciosamente, como um dos grandes desafios deste século. Em vista disso, a exemplo de países como Alemanha, Coreia do Norte, China, Estados Unidos, Irã, Israel e Rússia, e considerados potências no campo da GC, urge às Forças Armadas uma preparação eficaz e constante nesse am-biente, que pode ser utilizado para ataque e defesa, em situações de guerra ou de paz.

Visto que todos os indivíduos, empresas, instituições e governos que fazem uso do ciberespaço estão expostos a riscos e com o incremento latente da dependência destes aos sistemas digitais em combinação com a conectividade global, a informação torna-se ativo fulcral para a manutenção da segurança nacional, objeto inexorável de atenção das Forças Armadas e Estados.

NOTAS:

1- TI (Tecnologia da Informação) – Conjunto de todas as atividades e soluções providas por recursos de computação que visam permitir a produção, armazenamento, transmissão, acesso e o uso das informações. (ALECRIM, 2011).

2- Vulnerabilidade (digital) – Fraqueza apresentada por sistemas computacionais, que permitem a invasão e colocam em risco as informações e dados dos usuários. (SCHULTZ, 2020).

3- Como podemos perceber, esta segmentação assemelha-se ao que encontramos na Guerra Eletrônica, por exemplo. É interessante observar que ambas possuem pontos comuns de atuação, especialmente no âmbito das comunicações. Apresentadas as definições, traçar este paralelo auxilia a denotar a premência do estudo deste ambiente e da sua fusão com a realidade das Forças Armadas.

4- Aproximação indireta – o objetivo estratégico não é o centro de gravidade do exército inimigo, ou sua maior concentração de forças, como numa leitura errada do pensamento de Clausewitz, mas um objetivo distinto, que de forma indireta possa infligir grande dano moral, físico ou político, nas forças combatentes inimigas. (MARIMBONDO, 2019).

5- *Malware* é a abreviação de "software malicioso" (em inglês, "*malicious software*") e se refere a um tipo de programa de computador desenvolvido para infectar o computador de um usuário legítimo e prejudicá-lo de diversas formas.

6- *Asset Light* é um modelo ou estratégia de negócios utilizada por empresas na qual o objetivo fundamental é manter a menor quantidade de bens e ativos necessários, que se tornou comum com o advento de novos negócios digitais.

7- A *Jeune École* foi um conceito naval estratégico desenvolvido durante o século XIX. Ele defendia o uso de navios pequenos e fortemente armados para combater navios de guerra maiores e o uso de invasores de comércio para prejudicar o comércio da nação rival. (ROKSUND, 2007).

REFERÊNCIAS:

ALECRIM, Emerson. O que é tecnologia da informação?. **Infowester**, 2013. Disponível em: https://www.infowester.com/ti.php. Acesso em: 23 abr. 2021.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **Doutrina militar de defesa cibernética**: MD31-M-07. Brasília, DF: Ministério da Defesa, 2014. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf. Acesso em: 03 mai. 2021.

MARIMBONDO, Santiago. O desenvolvimento do pensamento estratégico: de Clausewitz às "guerras híbridas". **Blog Quilombo Spartacus**, [201-?]. Disponível em: https://quilombospartacus.wordpress.com/2019/06/30/o-desenvolvimento-do-pensamento-estrategico-de-clausewitz-as-guerras-hibridas-2/. Acesso em: 28 abr. 2021.

MENDONÇA, Cláudia da Silva. **Guerra cibernética**: desafios de uma nova fronteira. 2014. Monografia (Pós-graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet) – Instituto Tércio Pacitti, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2014. Disponível em: https://pantheon.ufrj.br/bitstream/11422/3340/1/CMendon%c3%a7a.pdf. Acesso em: 23 abr. 2021.

PARKS, Raymond C.; DUGGAN, David P. Principles of cyber-warfare. **Workshop on Information Assurance**, 2001, Nova Iorque: West Point, 2001. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?-doi=10.1.1.63.1478&rep=rep1&type=pdf. Acesso em 28 abr. 2021.

ROKSUND, Arne. **The Jeune École**: the strategy of the weak. Leiden: Brill, 2007.

SCHULTZ, Felix. Vulnerabilidade digital: como reconhecer e se proteger de ataques. **Milvus**, [s.l.], 2020. Disponível em: https://milvus.com.br/vunerabilidade-digital/. Acesso em: 23 abr. 2021.

SINGER, Peter; FRIEDMAN, Allan. **Cybersecurity and cyberwar**: what everyone needs to know?. Oxford: Oxford University Press, 2014.