DOI 10.52781/cmm.a051

# RESENHA: The fifth domain: defending our country, our companies and ourselves in the age of cyber threats.

CLARKE, Richard A.; KNAKE, Robert K. **The fifth domain**: defending our country, our companies and ourselves in the age of cyber threats. [S. l.]: Penguin Press, 2020. ISBN - 978- 0525561989.

**Resumo:** O livro enfrenta uma questão contemporânea essencial: a definição dos limites de atuação, proteção e utilização do ciberespaço como um quinto domínio operacional, bem como em as medidas a serem tomadas para tornar esse ambiente mais seguro. Utilizando o termo adotado pelo Departamento de Defesa norte-americano, os autores usam a experiência prática para indicar uma agenda que vise criar meios para aprimorar a defesa de áreas como a segurança estatal, economia, democracia e privacidade.

**Palavras-chave:** Ciberameaça. Ciberespaço. Cibersegurança. Defesa.

**Abstract:** The book faces an essential contemporary issue: the definition of the limits of action, protection and use of cyberspace as a fifth operational domain, as well as in the measures to be taken to make this environment more secure. Using the term adopted by the US Department of Defense, the authors use practical experience to indicate an agenda that aims to create means to improve the defense of areas such as state security, economics, democracy and privacy.

**Keywords:** Cyber Threats. Cyberspace. Cybersecurity. Defense.

**Rafael Gonçalves Mota**
Universidade de Fortaleza.
Faculdade Ari de Sá.
Tribunal de Justiça do Estado do Ceará.
Fortaleza, CE, Brasil.
rafaelgmota@yahoo.com.br

**Recebido: 23 abr. 2021**
**Aprovado: 28 abr. 2021**

**COLEÇÃO MEIRA MATTOS**
**ISSN on-line 2316-4891 / ISSN print 2316-4833**
http://ebrevistas.eb.mil.br/index.php/RMM/index

O livro enfrenta uma questão contemporânea essencial: a definição dos limites de atuação, proteção e utilização do ciberespaço como um quinto domínio operacional, bem como em as medidas a serem tomadas para tornar esse ambiente mais seguro. Utilizando o termo adotado pelo Departamento de Defesa norte-americano, os autores usam a experiência prática para indicar uma agenda que vise criar meios para aprimorar a defesa de áreas como a segurança estatal, economia, democracia e privacidade.

A obra é fundamental não apenas para aqueles que estudam e trabalham com segurança cibernética, mas para todos os responsáveis por pensar as questões relativas à soberania nacional, alta estratégia e políticas de defesa nacional. Compreender o alcance das ameaças concretas existentes no ciberespaço, em especial diante da imensa velocidade em que opera o cenário cibernético, é fundamental para orientar os tomadores de decisão num futuro próximo.

A perspectiva básica do livro sustenta que o panorama do ciberespaço é muito distinto do que era anos atrás. Segundo os autores, a principal vantagem é que as tecnologias atuais permitem a diminuição dos riscos representados por ações ofensivas de natureza cibernética. Ou seja, à medida que o desenvolvimento de novas tecnologias detém o potencial de criar novas ameaças, igualmente fornece aos Estados Nacionais novas e eficientes ferramentas virtuais para defender seus interesses e direitos.

Inicialmente, destacam os autores que o ciberespaço possui uma característica diferenciadora dos demais domínios operacionais (mar, terra, ar e espaço), já que é o único criado pelo homem. Tal fato, por si só, já faz com que o ambiente virtual possua elementos caracterizadores diferenciados, sendo necessário adaptar e compreender a natureza de tais ameaças.

No diagnóstico de riscos, não apenas ações agressivas realizadas por agentes estatais e não estatais, devem ser consideradas. Defeitos, falhas e imperfeiçoes nos softwares e sistema desenvolvidos nacionalmente – intencionais ou não – abrem uma brecha para que atividades maliciosas ocorram de forma mais fácil e potencialmente mais danosas. Com isso, Clarke e Knake sinalizam que a criação de uma política de segurança cibernética deve levar em conta tais variáveis.

Ainda tratando das potenciais vulnerabilidades advindas das características próprias do ciberespaço, os autores comentam a decisão do governo norte-americano de ampliar a participação da iniciativa privada no fornecimento de meios cibernéticos, especialmente os físicos. Em 2015, os servidores primários de *internet*, até então geridos por meio de contrato com o Departamento de Comércio, foram transferidos para a gestão privada.

Diante disso, há um compartilhamento de responsabilidade entre os setores público e o privado, caminhando além do uso de meios como "parcerias público-privadas" e instituindo esferas claras de compartilhamento de atuação. Embora o, campo estatal seja diretamente responsável por áreas como atuação militar, investigação criminal cibernética e coleta de inteligência, a proteção de dados e redes cibernéticas privadas não é responsabilidade estatal, podendo haver apenas uma colaboração do governo em situações extremas ou quando a atuação particular falhar.

Ao reconhecer a impossibilidade de o Estado garantir, por meios próprios e diretos, a segurança do ciberespaço, bem como a impropriedade de a iniciativa privada salvaguardar o ambiente cibernético, os autores indicam que não há caminho ou decisão fácil. O mais certo seria encontrar a solução menos ruim, não necessariamente a melhor, já que nenhuma é completamente eficaz ou plenamente adequada.

Desde o governo de Barack Obama os Estados Unidos passaram a se dedicar à construção de uma política estratégica de segurança cibernética, visando dotar não apenas os agentes estatais, como também os entes privados, de um grau de proteção mais concreto e efetivo para garantir a atuação no ciberespaço. Um exemplo disso é a criação da *National Strategy for Trusted Identities in Cyberspace (NSTIC)*. A ideia é dotar o ambiente virtual de meios mais seguros de identificação, e, por consequência, de atribuição dos atos ali realizados.

Um dos problemas identificados pelos autores no trato da questão cibernética é uma maior dificuldade de impor uma cultura de segurança unificada no ambiente privado já que, ao contrário dos entes estatais, indivíduos e empresas possuem atuações mais dispersas, dentro de dimensões próprias de ação.

No tocante à questão militar, os autores sinalizam que o objetivo do Pentágono em relação a um domínio operacional tão peculiar com o ciberespaço é o de buscar o controle completo do sistema virtual. Tal objetivo chega a ser expressamente indicado em documento datado de 2018, que define a estratégia cibernética o Departamento de Defesa.

Seguindo na análise da atuação militar no ciberespaço, os autores elaboram um questionamento fulcral: uma organização dirigida para a guerra pode atuar para diminuir as tensões e reduzir a probabilidade de conflitos? Clarke e Knake afirmam que a contribuição militar é fundamental para a redução de tensões e riscos cibernéticos. Porém, esta deve ocorrer ao lado de uma atuação diplomática que crie uma arquitetura de relações internacionais e favoreça o estabelecimento de um ambiente com menos conflitos potenciais e concretos.

A direção apontada pelos autores para a esfera de relações internacionais é a criação de um espaço cibernético construído a exemplo do "Espaço Schengen". Ao considerar a situação hipotética de um acordo internacional nessa linha, serie possível a edificação de regras comuns para a administração e a proteção de dados. Dessa forma a padronização das normas de controle e gestão do espaço cibernético produziria um ambiente ainda mais seguro para a atuação de companhias e empresas, que poderão competir seguindo regramentos comuns.

Avançando na análise, os autores tratam da necessidade de edificação de mecanismos eficientes de proteção das democracias no domínio virtual. Destacam a crescente importância do ciberespaço nos processos eleitorais, quer pela capacidade de comunicação quer pela evolução da tecnologia de virtualização das eleições.

Destacam os autores ainda que o desenvolvimento e aperfeiçoamento da inteligência artificial, notadamente no campo da *machine learning* sofrerá um incremento significativo nos próximos cinco anos, gerando habilidades mais eficientes de promoção de meios de defesa, salvo que igualmente houve um aperfeiçoamento dos atos agressivos.

A conclusão da obra é a de que as estratégias, ferramentas e políticas de administração e uso do ciberespaço já são conhecidas e o esforço agora deve ser canalizados pelos países para aproveitar as oportunidades e, principalmente, fazer escolhas racionais para delinear a próxima era do ciberespaço.


ECEME