
# COMANDO DE OPERAÇÕES TERRESTRES
## Escola de Comando e Estado-Maior do Exército
## XXI CICLO DE ESTUDOS ESTRATÉGICOS

# *CIBERESPAÇO: A NOVA DIMENSÃO DO CAMPO DE BATALHA*

# SUMÁRIO



# AS DIMENSÕES/DOMÍNIOS DO CAMPO DE BATALHA

EB70-MC-10.223

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
COMANDO DE OPERAÇÕES TERRESTRES

Manual de Campanha

OPERAÇÕES

5ª Edição
2017


Fig 2-1 – Dimensões do ambiente operacional

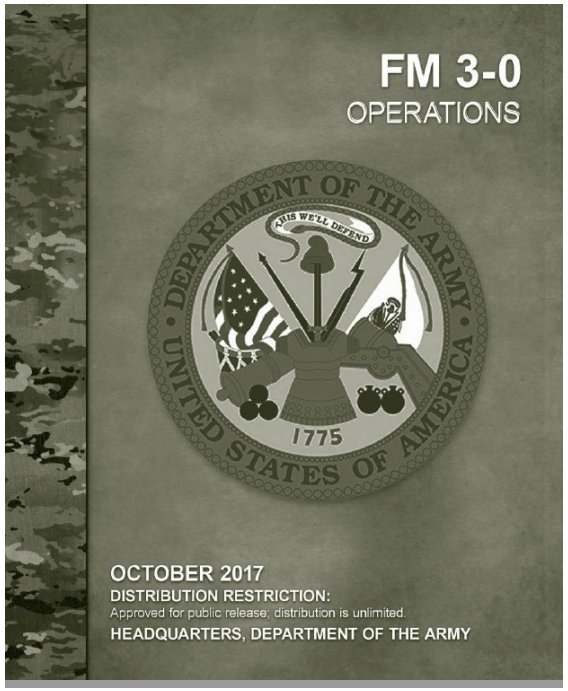
***O doutrina do Exército Brasileiro considera que o ambiente operacional é o conjunto de condições e circunstâncias que afetam o espaço onde atuam as forças militares e que interferem na forma como são empregadas, sendo caracterizado pelas dimensões física, humana e informacional.***

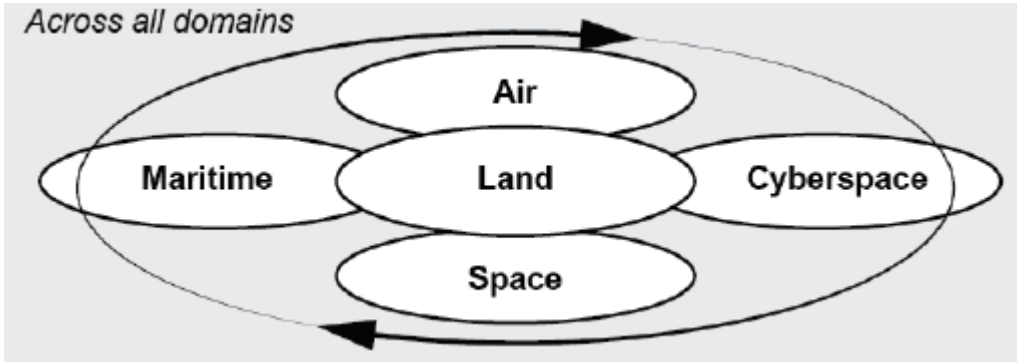
# AS DIMENSÕES/DOMÍNIOS DO CAMPO DE BATALHA


Fig 2-1 – Dimensões do ambiente operacional

***A dimensão informacional abrange os sistemas utilizados para obter, produzir e atuar sobre a informação.***

# AS DIMENSÕES/DOMÍNIOS DO CAMPO DE BATALHA




***O doutrina dos EUA considera que a guerra é travada atualmente em cinco domínios: terra, ar, mar, espaço e ciberespaço.***

# O ESPAÇO CIBERNÉTICO

***O Espaço Cibernético é um dos cinco domínios operacionais e permeia todos os demais, que são o terrestre, o marítimo, o aéreo e o espacial. As atividades no domínio cibernético podem criar liberdade de ação para atividades em outros domínios.***

***É um espaço virtual, composto por dispositivos computacionais, conectados em rede ou não, onde as informações digitais transitam, são processadas e/ou armazenadas.***

# CAMPO DAS IDEIAS OU REALIDADE?

X

# ALGUNS CONCEITOS

***- HACKER** é alguém com capacidade para escrever códigos ou instruções para computadores;*

***- CRIMINOSO CIBERNÉTICO** é aquele que o faz de forma ilegal;*

***- GUERREIRO CIBERNÉTICO** é aquele que o faz em guerra entre nações; e*

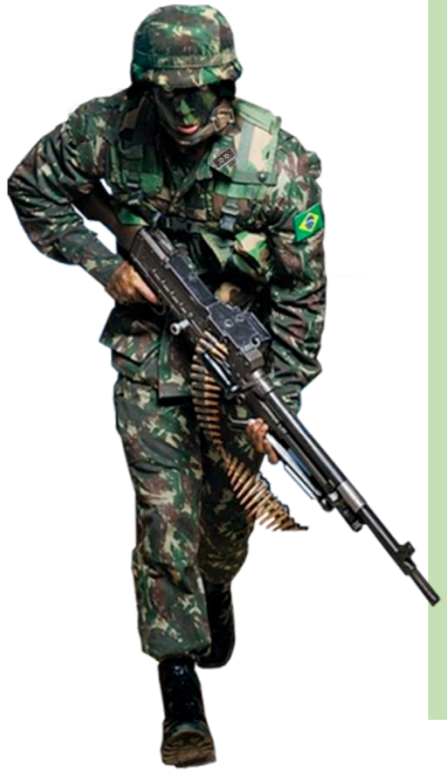
***- GUERRA CIBERNÉTICA** são ações de um Estado-Nação para invadir computadores de outro com a intenção de causar danos ou transtornos.*

# CASOS REAIS

- ***2003 – EUA invadem rede do Min Def iraquiano - envia milhares de email aos soldados inimigos, desestimulando a resistência e orientando o abandono de posição – operação psicológica beneficiando-se da Op cibernética.***

- ***2007 – Operação "Fora da Caixa" - Força Aérea Israelense atacou instalação nuclear síria. Os radares sírios foram infectados e não detectaram o ataque aéreo.***

# CASOS REAIS



- ***2007 – Ataque russo à Estônia –*** ***ataque de negação de serviço. A Estônia é um dos países mais conectados do mundo. Os sistemas bancário, de comunicações, comércio e outros ficaram indisponíveis por dias.***

- ***2008 – Invasão russa da Geórgia –*** ***os russos desencadearam ataques de negação de serviço, degradando sistemas de C2, impedindo as comunicações no país (a população não sabia o que estava acontecendo) e isolando o país do mundo.***

# CASOS REAIS

- ***2009 – Coreia do Norte ataca EUA - Ataque de negação de serviços contra sites do governo dos EUA e Coreia do sul, além de empresas internacionais, tirando-os de serviço.***

- ***2010 – Ataque ao Irã (STUXNET): EUA e Israel produziram um sofisticado malware para atacar a usina de enriquecimento de urânio de Natanz, no Irã, causando danos físicos às cascatas de centrífugas, por meio de alteração deliberada de dados do sistema de controle das máquinas (sistema SCADA), atrasando em anos o programa nuclear iraniano. Foi um ataque cibernético com efeito cinético.***

# CASOS REAIS

- ***2016 – Eleições dos EUA** – fortes indícios de interferência russa nas eleições, com uma campanha cibernética compondo uma Op Psico, em desfavor da candidata Hillary Clinton.*

- ***2019 – Ataque ao Hamas:** Israel bombardeou o prédio que abrigava o comando cibernético do Hamas, causando severos danos às ações do Hamas no ambiente da web. Foi um ataque cinético, com efeitos cibernéticos.*

# CASOS REAIS

O GLOBO MUNDO

BUSCAR ACESSE NO

## EUA lançaram ataques cibernéticos contra o Irã, afirma imprensa americana

Trump teria autorizado de forma secreta represálias contra computadores de lançamentos de mísseis e contra uma rede de espionagem iraniana

Da AFP
23/06/2019 - 09:00 / Atualizado em 23/06/2019 - 18:40

O presidente americano Donald Trump conversa com a imprensa neste sábado, na Casa Branca, em Washington
Foto: SAUL LOEB / AFP

CORREIO DO POVO

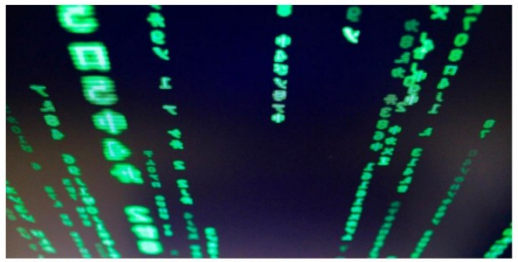
PORTO ALEGRE, SEXTA-FEIRA, 19 DE JULHO DE 2019

PORTO ALEGRE 12°C MENU ENTRAR ASSINE

## Ataques cibernéticos do Irã a EUA aumentaram, dizem empresas de segurança

Ciberataques acompanham a escalada de tensões entre os dois países

22/06/2019 | 13:07
Por AE



Especialistas afirmam que ciberataques do Irã acontecem de diferentes formas | Foto: Marcos Santos / USP Imagens / CP Memória

Made for minds.

Search TOP STORIES

TOP STORIES MEDIA CENTER TV RADIO LEARN GERMAN

GERMANY BREXIT WORLD BUSINESS SCIENCE ENVIRONMENT CULTURE SPORTS

TOP STORIES

NEWS

## US hits Iran with cyberattack: reports

The US reportedly launched a cyberattack on Iran in response to the downing of an unmanned drone. Cybersecurity firms have also reported a rise in Iranian attempts to hack US companies and government agencies.


Date 23.06.2019
Related Subjects Iran, White House
Keywords Iran, United States, cyber
Send us your feedback
Print Print this page
Permalink https://p.dw.com/p/3KvaR

NEWS

Netherlands partially responsible for Srebrenica massacre, court rules 26M AGO

Angela Merkel: 'I understand questions about my health' 40M AGO

German diplomat's 'likes' of anti-Israel tweets provoke anger 1H AGO

Taiwan open to granting Hong Kong protesters asylum 1H AGO

Turkish jets bomb Iraqi

# CASOS REAIS

***Na maioria dos casos os governos negam envolvimento, afirmando, quando são identificados ataques vindos de seus territórios que são pessoas, e não o governo.***

***Mas as " pessoas" não são reprimidas!***

# ESTRUTURAS CONHECIDAS

- ***EUA – US CYBER COMMAND – Comando conjunto criado em 2008***
- ***CHINA – FORÇA DE APOIO ESTRATÉGICO – criada em 2015 (mais uma força armada para guerra cibernética, eletrônica e espacial)***
- ***RÚSSIA – AGÊNCIA FEDERAL PARA COMUNICAÇÕES E INFORMAÇÕES – criada em 1991***
- ***OTAN – CENTRO DE OPERAÇÕES CIBERNÉTICAS – em processo de criação***

***Estima-se que entre 20 e 30 países no mundo possuam capacidade cibernética ofensiva***

# POR QUE É POSSÍVEL?

- ***O ciberespaço está em toda a parte, onde existe um computador, um processador ou um cabo conectado a uma rede.***

- ***Não é só a internet, que é a maior rede aberta. Ele inclui a internet e as outras redes que estejam a ela conectadas (e que, muitas vezes, não deveriam estar).***

- ***Em conjunto, o design da internet, as falhas de hardware e software e a utilização de máquinas controladas a partir do ciberespaço tornam os ataques cibernéticos possíveis.***

# A GUERRA CIBERNÉTICA

- ***Não respeita fronteiras geopolíticas. As operações podem acontecer em qualquer lugar e serem deflagradas de locais fisicamente afastados.***

- ***Diferentemente de outras armas, seus alvos mais comuns são os civis, principalmente estruturas críticas.***

- ***A dissuasão da Guerra Nuclear, onde os arsenais são dados a conhecer, funciona de forma diferente na Guerra Cibernética, que é revestida de sigilo.***

# A GUERRA CIBERNÉTICA

- ***Necessidade de defesa da estrutura de governo, incluindo a defesa, e a estrutura corporativa civil.***

- ***Possibilidade de causar grandes danos. "Quanto mais desenvolvido o país, maior a dependência do ciberespaço e, consequentemente, a vulnerabilidade."***

- ***Poucas pessoas, com relativamente poucos meios, podem ter um poder destruidor significativo.***

- ***Dificuldade para Ct ações e atribuição responsabilidades. Necessidade Ct no mais alto nível.***

- ***Pode ser assimétrica.***

# COMPARE AS DUAS IMAGENS


***Guerra assimétrica***

# CENÁRIOS POSSÍVEIS EM UM AMBIENTE DE GUERRA CIBERNÉTICA

- ***Ataque ao Sistema Financeiro: apagar dados bancários, depósitos, contas, ativos, impossibilidade de utilização de meios eletrônicos.***

- ***Ataque aos Sistemas de Telecomunicações: isolamento total, Telefone, TV, etc***

# CENÁRIOS POSSÍVEIS EM UM AMBIENTE DE GUERRA CIBERNÉTICA

- ***Ataque ao Sistema de Transportes: Vulnerabilidade a acidentes aéreos, ferroviários, etc***

- ***Ataque a infra-estruturas críticas: apagão elétrico, danos a refinarias, usinas nucleares, hidrelétricas etc***

***Não se trata de cenário de filme de ficção. Tudo isto é possível em um ataque cibernético.***

# CENÁRIOS POSSÍVEIS EM UM AMBIENTE DE GUERRA CIBERNÉTICA

- ***Na área militar:***
  - ***degradação de sistemas de comando e controle;***
  - ***desativação e engano de radares, sensores, etc***
  - ***desativação de armas;***
  - ***utilização como instrumento de Op Psico.***

# CENÁRIOS POSSÍVEIS EM UM AMBIENTE DE GUERRA CIBERNÉTICA

***"Se você está apenas se defendendo no ciberespaço, já está muito atrasado. Se você não domina o ciberespaço, não pode dominar outras dimensões do campo de batalha. Se você está em um país desenvolvido e foi atacado no ciberespaço, sua vida pode parar repentinamente."***

***Ten Gen Robert Elder***
***Diretor da FT de Op no Ciberespaço, da F Ae EUA***

# ASPECTOS DA DOUTRINA CIBERNÉTICA NO BRASIL


SETOR NUCLEAR

ETOR CIBERNÉTICO

SETOR ESPACIAL

NÍVEL POLÍTICO – PRESIDÊNCIA DA REPÚBLICA
(SEGURANÇA CIBERNÉTICA)

NÍVEL ESTRATÉGICO – MD, EMCFA E FORÇAS
(DEFESA CIBERNÉTICA)

NÍVEL OPERACIONAL– COMANDO OPERACIONAL
(GUERRA CIBERNÉTICA)

NÍVEL TÁTICO F Cj G Ciber
(GUERRA CIBERNÉTICA)

# CONCLUSÕES

- ***A Guerra Cibernética é real, o que está acontecendo é uma amostra do que pode acontecer em larga escala. Os contendores ainda não mostraram todo o arsenal.***

- ***A Guerra Cibernética é global. A interconectividade mundial transforma um ataque em assunto de interesse mundial.***

***A Guerra Cibernética já começou!***

***O ciberespaço é o campo de batalha!***


A vitória terrestre começa aqui


INTERVALO
CAFÉ

# debates

# Vamos conversar