Excelência em
TI e Gestão
Educação Presencial e EAD
www.faculdadefaps.edu.br
FAPS
Faculdade Professor Sérgio Silva

Ciberguerra
O Novo Campo de Batalha no Século XXI

ALEXANDRE BONNAMAIN[1]
JOÃO PADILHA MOREIRA[2]

Resumo

A ciberguerra, um conceito emergente da globalização, representa hoje uma capacidade de guerras realizadas num campo completamente diferente daqueles das tradicionais. Essas guerras são travadas silenciosamente, no ciberespaço. Uma vez que a evolução digital globalizada conecta, de maneira significativa, governos, indústrias privadas e particulares a um ataque cibernético, a consequência desse tipo de ataque pode ser devastadora. Embora sejam perigosas as conotações trazidas pelo ciberataque para o crime, os ataques políticos tornam-se ainda mais perigosos quando vão para o campo militar; eles são capazes de desestabilizar uma república inteira. No atual contexto de globalização, que vê as tecnologias digitais entrelaçadas com infraestruturas críticas de cada país, a ciberguerra é vista como uma verdadeira ameaça para qualquer nação. O conceito envolve ataques baseados em ferramentas digitais e consiste na execução de ações bélicas, como espionagem, sabotagem e desinformação contra a segurança nacional de terceiros. Este artigo fornece uma história da ciberguerra, suas ferramentas e métodos, suas consequências geopolíticas, bem como uma visão do futuro desse fenômeno.

Palavras-chave: cyberwar; ciberguerra; war; guerra.

[1] Aluno do Curso Técnico em Informática - bonnamainalexandre@gmail.com
[2] Professor do Curso Técnico em Informática – joao_moreira@alcidesmaya.edu.br

Excelência em
TI e Gestão
Educação Presencial e EAD
www.faculdadefaps.edu.br
FAPS
Faculdade Professor Sérgio Silva

2. Histórico da Ciberguerra

2.1 Origens e primeiros incidentes

A história da ciberguerra começou a ser escrita nos anos 1980, quando os primeiros ataques cibernéticos foram registrados. No entanto, foi na década de 2000 que o termo "ciberguerra" ganhou relevância. Um marco inicial foi o ataque ao sistema de defesa de computadores dos Estados Unidos, conhecido como **Morris Worm**, em 1988. Embora não tenha sido uma ação de guerra, o incidente demonstrou a vulnerabilidade dos sistemas digitais e iniciou a conscientização sobre os riscos do ciberespaço. Na década seguinte, o aumento do uso da internet e de sistemas interligados evidenciou o potencial de ataques cibernéticos com objetivos políticos ou militares. Em 2007, ocorreu o famoso ataque à Estônia, no qual hackers, supostamente vinculados ao governo russo, derrubaram a infraestrutura digital do país, paralisando serviços essenciais, como sistemas bancários e comunicações governamentais. Este foi um dos primeiros exemplos claros de ciberguerra.

2.2 A evolução do conceito

Na década de 2000, com o aumento dos incidentes, o termo "ciberguerra" consolidou se como um campo estratégico no cenário militar e político. Episódios como o ataque à Estônia em 2007 demonstraram o potencial devastador dos ciberataques, consolidando o ciberespaço como um campo de batalha estratégico.

3. Ferramentas e Métodos de Ciberguerra

A ciberguerra abrange uma ampla gama de ferramentas e técnicas para atacar, penetrar ou desestabilizar sistemas inimigos. A seguir, destacam-se os principais métodos utilizados:

3.1 Tipos de ataques cibernéticos

Malware e ransomware

O uso de malware (software malicioso) e ransomware é comum na ciberguerra.

Malware pode ser utilizado para infectar sistemas e roubar informações sensíveis, enquanto ransomware impede o acesso a sistemas, exigindo pagamento para liberá los.

3

Phishing e engenharia social

O phishing envolve mensagens fraudulentas destinadas a enganar os destinatários para que revelem informações confidenciais. Quando aplicados no contexto da ciberguerra, esses ataques comprometem redes governamentais ou militares.

DDoS (Distributed Denial of Service)

Ataques DDoS sobrecarregam servidores com tráfego massivo, interrompendo serviços essenciais de uma nação, causando impacto significativo na segurança nacional. **Ataques a infraestruturas críticas**

Esses ataques visam danificar ou destruir infraestruturas críticas, como redes elétricas e sistemas de transporte. Um exemplo notório é o "Stuxnet", um vírus que sabotou centrífugas de enriquecimento de urânio no Irã.

3.2 Ameaças emergentes

A inteligência artificial (IA) é uma ameaça emergente na ciberguerra. Ela pode ser utilizada em ataques altamente personalizados, adaptando-se rapidamente às defesas dos sistemas alvo. Além disso, deepfakes são usados para desinformação, manipulando opiniões públicas e afetando a estabilidade política de nações.

Excelência em
TI e Gestão
Educação Presencial e EAD
www.faculdadefaps.edu.br
FAPS
Faculdade Professor Sérgio Silva

4. A Ciberguerra no Contexto Geopolítico

4.1 Impactos estratégicos

Os impactos estratégicos da ciberguerra abrangem diversas áreas. Ataques cibernéticos substituem armamentos tradicionais, desestabilizando economias e comprometendo a estabilidade interna e externa de Estados.

4.2 Exemplos de impactos políticos

O ataque contra a Estônia em 2007 e a intervenção russa nas eleições dos EUA em 2016 são exemplos de como a ciberguerra pode ser utilizada para manipular a soberania de Estados e a opinião pública.

4.3 Ciberguerra e diplomacia

A diplomacia cibernética emerge como uma área importante nas relações internacionais, com esforços para desenvolver normas e convenções que governem o uso de armas cibernéticas. A ONU discute, por exemplo, uma convenção internacional para regulamentar ataques no ciberespaço.

Referências

- TEIXEIRA JÚNIOR, Augusto; VILLAR-LOPES, Gills; FREITAS, Marco T. As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica. **Revista Carta Internacional**, v. 12, n. 3, 2017.
- LIFF, Adam. Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War. **Journal of Strategic Studies**, v. 35, n. 3, p. 401–428, 2012.
- PAKHARENKO, Glib. Cyber Operations at Maidan: A First-Hand Account. In: GEERS, Kenneth (Ed.). **Cyber War in Perspective**.