IMPORTÂNCIA DA SEGURANÇA CIBERNÉTICA NA ESTRUTURAÇÃO DE DEFESAS ONLINES NO ÂMBITO MILITAR NACIONAL E INTERNACIONAL

Vinicius de Camargo Fantin[1], João Victor Surdi[2], Gabriel de Oliveira [3], Rafael Simon Borga [4], Fabiano Wonzonsk[5]

1. Discente do curso de graduação em Ciência da Computação, Unoesc, Videira, SC
2. Discente do curso de graduação em Ciência da Computação, Unoesc, Videira, SC
3. Discente do curso de graduação em Ciência da Computação, Unoesc, Videira, SC
4. Discente do curso de graduação em Ciência da Computação, Unoesc, Videira, SC
5. Docente do curso de graduação em Ciência da Computação, Unoesc, Videira, SC

Autor correspondente: Vinicius de Camargo Fantin, vinifantin302@gmail.com

Área: Ciências Exatas e Tecnológicas

Introdução: O avanço das tecnologias da informação transformou a natureza dos conflitos contemporâneos, especialmente no campo militar. A digitalização das infraestruturas de defesa trouxe o ciberespaço como um novo campo de batalha, como demonstrado na guerra entre Rússia e Ucrânia. Nesse contexto, ferramentas de espionagem digital, disseminação de desinformação e ataques com malwares e ameaças persistentes avançadas (APAs) passaram a integrar estratégias militares. A aliança entre forças estatais e grupos hackers destacou como a supremacia digital pode influenciar os desfechos bélicos, redefinindo a soberania e o equilíbrio geopolítico global. **Objetivo:** Analisar o papel estratégico da cibersegurança na estruturação das defesas militares nacionais e internacionais, destacando como as estratégias digitais moldam o equilíbrio de poder entre nações e influenciam os conflitos híbridos contemporâneos. **Método:** A pesquisa foi realizada a partir de revisão bibliográfica e análise de dados sobre ataques cibernéticos em contextos de guerra. Foram consultados estudos sobre militarismo digital, invasões, vazamentos de dados e técnicas de proteção cibernética. O estudo busca compreender como a digitalização impacta a segurança nacional e internacional, a partir da comparação de eventos recentes envolvendo a Rússia e a Ucrânia. **Resultados:** De acordo com o artigo Cyber Dimensions of the Armed Conflict in Ukraine (2023), foram registrados 97 ataques cibernéticos na Ucrânia, 13 na Rússia e 472 em outros países. Cerca de 89% dos incidentes foram ataques de negação de serviço (DDoS), com maior incidência nos setores público, de mídia, tecnologia da informação, financeiro e comercial. Organizações como Fancy Bear, Sandworm e CyberBerkut, com apoio de agências russas como FSB e GRU, lideraram ataques coordenados. Ferramentas como BlackEnergy e X-Agent foram utilizadas para sabotagem e espionagem, e ações de phishing reforçaram o papel da engenharia social nos conflitos modernos. **Conclusão:** A cibersegurança tornou-se componente essencial das estratégias de defesa diante dos conflitos híbridos. O domínio do ciberespaço deixou de ser apenas técnico, passando a ser estratégico. Para pesquisas futuras, recomenda-se aprofundar os estudos sobre cooperação internacional em defesa cibernética e os desafios éticos e legais da guerra digital. Compreender essas dinâmicas é crucial para políticas públicas eficazes frente às ameaças digitais crescentes.

Palavras-chave: Cibersegurança; Defesa cibernética; Guerra hibrida; Soberania digital ; Conflito Rússia-Ucrânia .

Agradecimentos: Agradecemos ao Uniedu e ao Programa Universidade Gratuita pelo apoio financeiro, à UNOESC pela estrutura oferecida e ao professor Fabiano Wonzonski pela orientação. Estendemos nossa gratidão a todos que contribuíram para a realização deste Artigo