

CONGRESSO INTERNACIONAL DE RELAÇÕES INTERNACIONAIS DO AMAZONAS

SIMPÓSIO DE INICIAÇÃO CIENTÍFICA -08 SEGURANÇA INTERNACIONAL E DEFESA

CIBERESPAÇO E A NOVA FRONTEIRA DA GEOPOLÍTICA CONTEMPORÂNEA.

*Anne Caroline
Pedro Gabriel
Macsynie Silva
Faculdade La Salle Manaus*

Resumo:

O presente artigo possui como enfoque analisar as definições de ciberguerras e avaliar sua reflexão em âmbito internacional, buscando identificar como elas interferem nas relações político-sociais entre os atores internacionais de todo o mundo, elencando fatos correlacionados a respeito do ciberespaço e seus âmbitos, elucidando conceitos primordiais para com o debate a respeito do tema, como, a noção do que é o ciberespaço, momento de surgimento desse espaço cibernético e o papel tanto de entidades privadas quanto do próprio Estado dentro do tema. A Ciberguerra tem induzido nações a adotar novas medidas de proteção, o que fez surgir novas instituições públicas e privadas voltadas para a cybersecurity.

Palavras-Chave: Ciberespaço, cybersecurity, ciberguerras.

Abstract:

This article focuses on analyzing the definitions of cyberwars and evaluating their reflections at an international level, seeking to identify how they interfere in political and social relations between international actors around the world, listing correlated facts about cyberspace and its scopes, elucidating key concepts for the debate on the subject, such as the notion of what cyberspace is, the moment of emergence of this cybernetic space and the role of both private entities and the



State itself within the theme. Cyberwar has induced nations to adopt new protection measures, which has given rise to new public and private institutions focused on cybersecurity.

1. INTRODUÇÃO

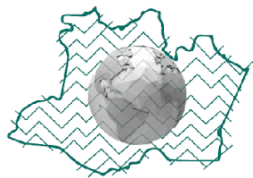
No mundo atual, onde a tecnologia permeia praticamente todos os aspectos de nossa vida, a ciberguerra emergiu como uma nova fronteira em conflitos internacionais. Com a proliferação da internet, das redes de comunicação e da dependência de sistemas digitais, as nações estão enfrentando uma ameaça crescente e invisível que transcende fronteiras físicas: a guerra cibernética.

A ciberguerra envolve o uso malicioso e intencional da tecnologia da informação e dos sistemas tecnológicos para realizar ataques contra infraestruturas críticas, instituições governamentais e empresas. Esses ataques podem assumir várias formas, desde a interrupção de serviços essenciais até o roubo de informações confidenciais ou até mesmo a manipulação de processos e sistemas.

Neste artigo, exploraremos os principais aspectos da ciberguerra, desde sua definição e formas de ataques até suas implicações em termos de segurança nacional, economia e privacidade. Além disso, discutiremos as estratégias e medidas que estão sendo adotadas para combater esse novo tipo de guerra, bem como os desafios futuros que precisaremos enfrentar.

2. CIBERGUERRA O QUE É?

O conceito de “guerra cibernética” surgiu a partir de abril de 2007, quando os principais sites do governo estoniano sofreram uma série de ataques classificados como “negação de serviços” pelo Denial of Service - DDoS. Esse ataque fez com que as autoridades e os atores internacionais sobre a defesa do mundo sobre a existência do fato que a internet a partir daquele momento estaria se tornando uma arma para espionagem e sabotagem internacional.



CONGRESSO INTERNACIONAL DE RELAÇÕES INTERNACIONAIS DO AMAZONAS

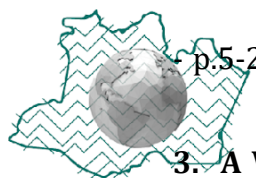
Muito antes do ataque à Estônia, a guerra cibernética já havia sua participação na evolução dos ataques, por exemplo em 1982, com a explosão do grande gasoduto Trans-ciberiano. A explosão teria sido causada pelo serviço secreto dos EUA de um bug no software do sistema de gerenciamento e prospecção de gás, roubado pela KGB de uma empresa canadense. (...) the most monumental non-nuclear explosion and fire seen from space” (REED, 2005, p. 269).

A guerra cibernética é consequência direta da evolução dos sistemas de comunicação ocorridos durante e depois da Segunda Guerra Mundial. A invenção de radares, o aperfeiçoamento dos sistemas operacionais de comunicações na esfera militar e civil, todas essas características revolucionaram a maneira como se fazia guerra até então.

Dentro do conceito de “ciberguerra” há também o surgimento da “guerra eletrônica” que tem como característica todas as ações militares, destinadas a assegurar o uso mais eficaz possível de emissões eletromagnéticas e eletro-ópticas e impedir que o inimigo consiga fazer uso dos seus serviços.

Podemos classificar as “ações” da guerra eletrônica em quatro tipos: i. detecção (radares, sonares, receptores de alerta antecipado); ii. coleta de informações (Sigint - Signals Intel- ligence, Elint - Eletronic Intelligence, Comint - Communications Intelligence); iii. contrame- didas (chaffs, flares, anti-jamming); e iv. interferência intencional (jamming, desvio de sinais/ dissimulação e armas do tipo Electro-magnetic Pulse). (...) Revista Política Hoje - Vol 26, n. 1 (2017) - p. 202-217

O ciberespaço é o mais novo local de "disponibilização" de informações possibilitado pelas novas tecnologias. Uma nova mídia que absorve todas as outras e oferece recursos inimagináveis, há algumas décadas. Como Lévy (2000) o caracteriza, Trata-se de um espaço que ainda não se conhece completamente, cheio de desafios e incertezas, tanto na sua práxis, quanto em suas formulações filosóficas e teóricas. Um espaço aberto, virtual, fluido, navegável. Um espaço que se constrói em cima de sistemas, e, por esse mesmo fato, é também o sistema do caos. (...) DataGramZero - Revista de Ciência da Informação - v.8 n.3 Jun/07, n. 03



CONGRESSO INTERNACIONAL DE RELAÇÕES INTERNACIONAIS DO AMAZONAS

3. A VISIBILIDADE DAS CYBERGUERRAS NA ATUALIDADE.

Como observam Silva e Silva (2004), o ciberespaço é uma região abstrata invisível que permite a circulação de informações na forma de imagens, sons, textos, movimentos; um espaço virtual que está em vias de globalização planetária e já constitui um espaço social de trocas simbólicas entre pessoas dos mais diversos locais do planeta.

Baseando-nos nas definições dos autores citados, podemos entender o ciberespaço como um universo virtual proporcionado pelas redes de comunicações, nesse caso a Internet.

Como campo de batalha atual, podemos usar como exemplo a guerra RÚSSIA x UCRÂNIA, que por muito é considerada uma guerra híbrida, tem como grande característica o grande número de ataques cibernéticos. As pesquisas aqui levantadas não pretendem questionar se existem duas guerras cibernéticas, mas sim, retratá-las e dar a visibilidade, tendo em vista que os ciberataques não ocorrem apenas contra empresas e estados, mas também com civis.

É importante levantar a questão da relação que a sociedade tem com a internet, a evolução e a difusão da tecnologia na rotina dos civis que vêm transformando o mundo e a sociedade, fazendo cada vez mais integrados ao ciberespaço. O crescimento da necessidade de manutenção tecnológica da sociedade faz com que a exposição e a vulnerabilidade dos cidadãos cresça em relação às ameaças cibernéticas.

No cenário político internacional, levamos em consideração a evolução das guerras ao decorrer da história, que evoluíram e desenvolveram características peculiares, tais como: guerras irregulares, guerras assimétricas, guerras compostas, guerras híbridas, dentre outras. Sabendo disso, é evidente que quanto maior o registro de dados de um Estado no ciberespaço, maiores serão suas vulnerabilidades aos ataques de outros, no caso de Rússia e China que hoje são os



dois países com maior poder cibernético defensivo e de ataque, ao longo de seus desenvolvimentos tiveram grandes investimentos em áreas tecnológicas e possuem hoje essa maior soberania tecnológica.

Na atualidade, temos grandes quantidades de crimes cibernéticos acontecendo, isso se deu com a pandemia de Covid-19 que intensificou o número de ameaças, a visibilidade desta pauta se torna cada vez mais necessário na sociedade, o Estado necessita dar uma maior atenção às políticas e leis em relação ao ciberespaço, a conscientização sobre o uso correto e consciente da internet.

4. O PAPEL DAS INSTITUIÇÕES NA CIBERGUERRA.

Controlar o ciberespaço é um desafio complexo devido à sua natureza descentralizada e global. Embora as instituições possam implementar medidas para promover a segurança e a governança do ciberespaço, é importante equilibrar o controle com a proteção da privacidade e a preservação.

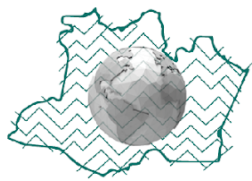
As instituições podem promover a conscientização e a educação em segurança cibernética, tanto para indivíduos como para organizações. Fornecendo diretrizes e melhores práticas de segurança, incentivando a implementação de tecnologias seguras e investindo em pesquisa e desenvolvimento.

A criação de leis e regulamentações para orientar o comportamento no ciberespaço. Isso pode incluir leis de proteção de dados, leis de combate ao cibercrime e regulamentações para promover a segurança cibernética em setores críticos, como serviços financeiros e infraestrutura.

É necessário encontrar um equilíbrio adequado entre o controle necessário para proteger a sociedade e os direitos individuais no mundo digital.

5. O PAPEL DO ESTADO NA CYBERGUERRA.

A partir da quarta fase da globalização, que vem a ser a revolução tecnológica, onde há um momento de nova ordem mundial, iniciada a partir do



CONGRESSO INTERNACIONAL DE RELAÇÕES INTERNACIONAIS DO AMAZONAS

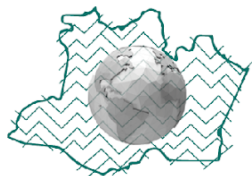
ano de 2011, torna-se claro que houve uma gigantesca eclosão no viés tecnológico ao redor de todo o mundo, as competições entre estados deixam o âmbito apenas físico e passam a ser mais cibernético do que nunca, o mundo torna-se ligado por um sistema de telecomunicações e informática, em uma rede de comunicações. Tornando todo esse globo depende dessas conexões, dando assim, cada vez mais abertura para invasores cibernéticos como os hackers e fazendo os estados cada vez mais vulneráveis por consequência.

Levando em conta o viés geopolítico mundial, na contemporaneidade os conflitos presentes e enfrentados pelos estados no século XXI contrapõem-se por completo aos enfrentamentos ocorridos durante o século XX. Em momentos históricos diferentes as guerras travavam-se a respeito de disputa e conquista de territórios e poder. No entanto, as divergências vividas pelos estados atualmente envolvem meios muitos mais tecnológicos e de inovação.

A luz das palavras de Joseph S. Nye JR, “Os países tendem a colher os frutos mais suculentos quando se beneficiam de tecnologias.” (2002, p. 53), sendo assim, os estados se utilizam da estratégia de investimento em todo o meio tecnológico e científico nos momentos atuais, para assim ganhar vantagens em relação aos demais, passando para trás estratégias diretas de ataque com tropas de soldados armados com lanças e armas de fogo.

Ademais, o momento em que a relação dos espaços cibernéticos e dos Estados se encontra, tanto em um cenário político como econômico se mostra nebuloso, considerando que, apesar dos Estados tanto investirem quanto possuírem setores voltados completamente para a inteligência de redes, desenvolvimentos de *softwares*, aparatos tecnológicos e em equipes treinadas para um possível ataque cibernético, de maneira alguma, esses Estados assumem para os demais que dedicam-se em desenvolver sistemas capazes de invadir e danificar sistemas rivais, ainda que existam evidências do uso de ataques por meio do ciberespaço e até mesmo confrontos cibernéticos entre os Estados.

Por fim, é cabível aos Estados que suas vulnerabilidades a respeito do



CONGRESSO INTERNACIONAL DE RELAÇÕES INTERNACIONAIS DO AMAZONAS

ciberespaço sejam sanadas. E há maneiras diversas de resolver essas deficiências, seja por meio de tratados bi e multilaterais, ou, buscando alianças com países que compartilham dos mesmo objetivos e interesses e também que os estados invistam em segurança cibernética para se resguardar a respeito de possíveis ataques.

6. CONCLUSÃO

O objetivo levantado neste artigo foi trazer à tona a reflexão da nova maneira de fazer guerra, como as mudanças decorrentes do avanço das tecnologias às relações entre os estados ou a forma de viver da sociedade. No sistema internacional o ciberespaço tornou-se um novo campo de batalha entre os países e atores, mesmo com o avanço tecnológico e o alastramento dos conflitos neste espaço.

A maneira como os Estados estão preparados em relação à cybersecurity e de que maneira cada um deveria investir nesse sentido, como a vulnerabilidade cibernética pode afetar a sociedade.

7. REFERÊNCIAS BIBLIOGRÁFICAS

ARQUILLA, John; RONFELDT, David. Cyberwar is Coming! RAND Corporation, Estados Unidos, v.12, n. 2, p. 141-165, 1993.

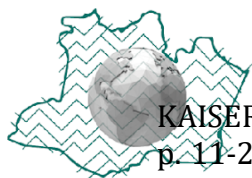
KAISER, Robert. The birth of cyberwar. ELSEVIER. Madison USA. 10. 2014

LOBATO, Luisa e KENKEL, Kai. A Ciberguerra É Moderna! Uma Investigação sobre a Relação entre Tecnologia e Modernização na Guerra, CNPq. Rio de Janeiro, 2014

FONSECA, Leila. Relações internacionais, Sergipe, 2023

NETO, Ricardo. Guerra cibernética / guerra eletrônica: conceitos, desafios e espaços de interação, Revista Política Hoje - Vol 26, n. 1, Pernambuco, 2017

TORRES, JHONNY BEZERRA. A Ciberguerra: Uma Forma de Confronto Entre Estados. Revista Desenvolvimento Intelectual, São Paulo, v. 7, n.7, p. 125-158, 2021.



CONGRESSO INTERNACIONAL DE RELACIONES INTERNACIONAIS DO AMAZONAS

KAISER, Robert. The birth of cyberwar. Political Geography, Estados Unidos, v. 46, p. 11-20, 2015.

NYE, Joséph S. O colosso americano. In: NYE, Joséph S. O paradoxo do poder americano: Por que a única superpotência do mundo não pode prosseguir isolada. Tradução: ARAÚJO, Luiz A. O. São Paulo: Editora Unesp, 2002, p. 25-82.