REVISTA MUNDO EM MOVIMENTO
Uninassau-Caruaru
1(1): 01-14, 2024
ISSN: 2966-2176

AMEAÇAS CIBERNÉTICAS À SEGURANÇA NACIONAL: O PAPEL DAS FORÇAS ARMADAS NO COMBATE A CRIMES DIGITAIS

CYBER THREATS TO NATIONAL SECURITY: THE ROLE OF THE ARMED FORCES IN COMBAT DIGITAL CRIMES

Edson Vinícius da Silva Nunes
Bacharelado (em andamento) em Direito, Uninassau-Caruaru. Email: viniedsondos3@gmail.com

Givaldo Bezerra de Lima Junior
Bacharelado (em andamento) em Direito, Uninassau-Caruaru. Email: givaldo1215@hotmail.com

Nathalia Oliveira Ferreira
Advogada. Docente da UNINASSAU - Caruaru. Especialista em Ciências Criminais. Caruaru-PE, Brasil. Orientadora. Email: advnathaliaoliveiraa@gmail.com

RESUMO: A presente pesquisa tem como escopo refletir, explorar e debater as ameaças cibernéticas à segurança nacional em casos de ataques cibernéticos, mais precisamente no tocante ao papel das Forças Armadas no combate a crimes digitais. Por se tratar de tema atual e diante da escassez de livros da área, a metodologia restringiu-se em pesquisas de artigos com a mesma pertinência temática, inclusive de forma comparativa com trabalhos de outros países, documentos oficiais e de biografia para conceituar institutos pertinentes ao assunto. Para tanto, partiu-se da conceituação e contextualização dos crimes digitais, passando-se pelas políticas de segurança cibernética no âmbito global até se chegar à discussão nacional, observando e prevendo como as Forças Armadas podem

combater os crimes e as ameaças do assunto. Conquanto seja extremamente difícil e até mesmo inadequado afirmar que houve conclusão, por se tratar de trabalho científico, restou mais do que evidente que o Brasil deve se preocupar em traçar estratégias, de forma a combater as ameaças cibernéticas as Forças Armadas que ameaçam a segurança Nacional. Por outro lado, justifica-se a realização do trabalho não só no âmbito científico, mas também social, haja vista que ameaças cibernéticas podem colocar em risco não só o indivíduo, mas também o corpo social e a própria soberania do Estado.

PALAVRAS-CHAVE: Ameaças Cibernéticas, Segurança Nacional, Crimes Digitais.

ABSTRACT: The scope of this research is to reflect, explore and debate cyber threats to national security in cases of cyber attacks, more specifically regarding the role of the Armed Forces in combating digital crimes. Since this is a current topic and given the scarcity of books in the area, the methodology is limited to researching articles with the same thematic relevance, including comparative studies with works from other countries, official documents and biographies from reputable institutes relevant to the subject. To this end, the study started with the conceptualization and contextualization of digital crimes, moving on to cyber security policies on a global scale until reaching the national discussion, monitoring and predicting how the Armed Forces can combat crimes and threats related to the subject. Although it is extremely difficult and even inappropriate to state that there was a conclusion, since this is a scientific study, it was more than evident that Brazil should be concerned with outlining strategies in order to combat cyber threats to the Armed Forces that threaten national security. On the other hand, it is justified to carry out the work not only in the scientific but also in the social sphere, given that cyber threats can put at risk not only the individual, but also the social body and the sovereignty of the State itself.

KEYWORDS: Cyber Threats, National Security, Digital Crimes, Security.

1. INTRODUÇÃO

Desde os primórdios, a humanidade tem sido marcada por conflitos, seja para sobrevivência, demonstração de força, imposição cultural ou defesa de seus interesses. Essa natureza humana permanece inalterada ao longo do tempo. Com o advento da era tecnológica e com o crescente conhecimento nas mais diversas áreas o ser humano não mudou seus comportamentos, com isso afirmamos que o homem sempre foi o mesmo o que mudou foi a tecnologia.

Surgem, então, os impactos que a era digital causa nas relações sociais e, como o Direito que está entranhado nelas, têm se afetado com essas transformações. O uso da internet e a integração de automação dentro de uma rede que, conecta o mundo inteiro em informações imediatas, gera impactos geopolíticos e problemas a segurança nacional no espaço cibernético.

O Brasil, que é considerado um país pacífico no tocante a guerras, entretanto, também está sujeito a novas ameaças. Sendo assim, precisa se aparelhar de mecanismos de defesas e combate a crimes cibernéticos que põe em risco a segurança da nossa nação.

É por essa razão que surge o objeto desse estudo, que diante das ameaças dos crimes cibernéticos a segurança nacional, qual tem sido o papel das forças armadas na prevenção e combate a esses delitos, como o Brasil tem se posicionado a propiciar meios para coibir esses crimes.

Diante da escassez bibliográfica pertinentes ao assunto, com sua atualidade e expansionismo, o presente estudo, em relação a metodologia,

pautou-se em pesquisas de outros artigos, na analogia, em sites oficiais, no direito comparado de outros países e também em documentos oficiais.

2. CONTEXTO E CONCEITO DOS CRIMES DIGITAIS

A sociedade da informação adveio de um longo processo e, não repentinamente, o marco dessa transformação foi a Revolução Industrial da segunda metade do século XVIII. Esta, ficou marcada pela substituição da mão de obra humana por máquinas, assim encerrando uma grande era agrícola, dando início a uma nova ralação de capital e trabalho entre as nações.

A sociologia entende que a Revolução industrial passou por três momentos e que, atualmente, estamos passando pela quarta fase. A segunda desenvolveu a indústria química, elétrica, de petróleo e aço, além de avanços nos meios de transporte e comunicação. A terceira marcada pela substituição gradual da mecânica analógica pela digital, com o uso de microcomputadores e criação da internet. Já a quarta revolução, segundo dados de Schwab, presidente do Fórum Econômico Mundial, e autor do livro "A Quarta Revolução Industrial". Segundo ele, o conceito está ligado ao de Indústria 4.0. Esse modelo empresarial visa utilizar todas as tecnologias atualmente disponíveis para gerar conhecimento e produtividade.

O avanço tecnológico para fins bélicos, continuou a evoluir após o fim da Segunda Guerra Mundial. Esse desenvolvimento, foi impulsionado pela instauração da Guerra Fria, durante a qual a troca de informações tornou-se algo extremamente sigilosa. Isso visava evitar que as mensagens vitais

fossem captadas pelo lado inimigo, o que desdobraria em vantagem no conflito.

Já vimos que, a sociedade tem passado por transformações significativas que interferem na sua organização e subsistência. Na era digital, surgem novos crimes que exploram o vasto campo da rede de informações. Condutas que não são aprovadas socialmente surgem e colocam em risco até a segurança dos Estados.

Conforme Patrícia Pinheiro (2016, p. 12) "aqueles em que a tecnologia foi utilizada como ferramenta-meio ou alvo-fim da atividade criminosa no meio ambiente computacional da sociedade complexa da informação e comunicação". Essa definição é fundamental para entender a complexidade desses delitos, que são uma forte ameaça para milhões de pessoas e países.

Observar como esses crimes podem apresentar uma ameaça ao País é primordial, pois podemos melhor entender com o que estamos lidando e como a Segurança Nacional pode combater essas ameaças. Com efeito:

> No que toca ao ciberterrorismo podemos afirmar que se trata do uso de redes e instrumentos informáticos para desligar e perturbar infraestruturas nacionais importantes (tal como a energia, transportes, governo) ou para coagir ou intimidar um governo ou a sua população. Um grupo ou nação hostil pode explorar as vulnerabilidades de um governo, organização ou Estado, com o intuito de penetrar nessa rede informática e perturbar (ou mesmo até desligar) as suas funções mais importantes. Carla Sofia Carreira Jacinto (2002, p. 5)

Diante dessa problemática, olharemos como os serviços de inteligências das nações têm trabalhando e se preparando para reprimir e evitar tais problemas à sua segurança.

3. ATAQUES CIBERNÉTICOS NO CENÁRIO MUNDIAL

Em 1994, a Organização das Nações Unidas (ONU), por meio do relatório "Human Development Report" do Programa de Desenvolvimento das Nações Unidas (PNUD), ampliou o conceito de segurança no contexto internacional. Passou a englobar o indivíduo como como sujeito e expandiu a visão, anteriormente centralizada no Estado. Como resultado os objetos de estudo de segurança passaram a incluir aspectos de ordem econômicos, ambientais, políticos e de saúde. Além disso, atualmente entendemos que o ambiente digital globalizado, também se insere desse contexto de segurança.

A União Internacional das Telecomunicações (UIT), organização especializada das Nações Unidas, tem como finalidade padronizar as telecomunicações. Nesse contexto, a UIT organiza a Cúpula Mundial sobre a Sociedade da Informação. Além disso, promove a segurança cibernética por meio do "Programa Global de Segurança Cibernética". Um grupo de especialistas foi criado para desenvolver, a longo prazo, estratégias técnicas e legais para remediar falhas de software, detectar ataques informativos e gerenciar crises.

É perceptível que a formação de alianças entre países e organizações internacionais é essencial para combater e detectar os ataques cibernéticos considerando a complexidade e necessidade de cooperação, sobre a política de cibersegurança e ciberdefesa adotada nos países membros da OTAN:

> A principal prioridade da OTAN para a defesa cibernética é a proteção das comunicações e sistemas de informação (CIS), que são operados pela OTAN. A Organização precisa de infraestruturas nacionais confiáveis e seguras. Para este fim, a OTAN trabalha com as

> autoridades nacionais para desenvolver princípios, critérios e mecanismos para assegurar um nível adequado de defesa cibernética para CIS nacionais. A Organização ajuda os seus países membros em seus esforços para proteger infraestruturas críticas através da partilha de informações e melhores práticas, e através da realização de exercícios de defesa cibernética para ajudar a desenvolver competências nacionais. Da mesma forma, os países aliados individuais podem, numa base voluntária e facilitado pela OTAN, ajudar os outros Aliados a desenvolver as suas capacidades de defesa cibernética nacional. Maria Ramos (2015, p. 60)

Nos Estados Unidos os objetivos em relação as estratégias de combate à segurança cibernética foram introduzidos em 2003, com a publicação do documento "Estratégia Nacional para Proteger o Ciberespaço", pela Casa Branca. Após seis anos, em 2009, o então Presidente Barack Obama, apresentou suas perspectivas e visões políticas sobre o Ciberespaço, resultando na publicação da "Revisão da Política para o Ciberespaço"

Em 2002, a União Europeia adotou a Estratégia "Europeia de Segurança" (EES) um marco importante para segurança continental. O documento (UNIÓN EUROPEA, 2013) aborda os desafios globais e principais ameaças à segurança, considerando a conexão entre segurança interna e externa.

> As economias modernas dependem em grande medida das infraestruturas vitais, como transportes, comunicações e fornecimento da energia, e também a Internet. A estratégia da EU para uma "Sociedade da Informação" segura na Europa, adotada em 2006, faz referência ao crime causado na Internet. No entanto, os ataques contra sistemas privados ou governamentais de TI nos Estados-Membros da EU têm dado uma nova dimensão a este problema, como uma nova arma econômica, política e militar em potencial. Deve-se continuar trabalhando neste campo para explorar uma abordagem global da EU, conscientizando as pessoas e

> intensificando a cooperação internacional. (UNIÓN EUROPEA , 2008, p. 5).

Na América Latina os ataques cibernéticos são uma ameaça crescente. De acordo com um relatório da Fortinet, foram registradas 137 bilhões de tentativas de ataques cibernéticos na região apenas no primeiro semestre de 2022. O México foi o país mais atingido seguido pelo Brasil e Colômbia. Diante desse crescimento exponencial, é imperativo que as partes interessadas desenvolvam estratégias eficazes para enfrentar essas ameaças multifacetadas. Isso exige uma colaboração com múltiplos esforços regionais e nacionais para garantir a segurança do Ciberespaço.

4. ATAQUES CIBERNÉTICOS NO BRASIL E O PAPEL DAS FORÇAS ARMADAS

Brasil, tem um papel menos sensível aos ataques cibernéticos , haja visto seu papel secundário que desempenha dentro do contexto internacional. Mas é essencial que o País esteja preparado para enfrentar e combater futuras ameaças.

O Livro Branco de Defesa do Brasil (LBDB) salienta que "a ameaça cibernética se tornou uma preocupação por colocar em risco a integridade de infraestruturas sensíveis, essenciais à operação e ao controle de diversos sistemas e órgãos diretamente relacionados à segurança nacional" (Ministério da Defesa 2012b, 69).

O Brasil é signatário da Convenção de Budapeste, criada em 2001, na Hungria, pelo Conselho da Europa, e vigente desde 2004. Em 12 de abril de

2023, foi publicado o Decreto nº 11.491, que promulgou a Convenção sobre o Crime Cibernético.

Segundo André Zaca Furquim, coordenador-geral de Cooperação Jurídica Internacional em Matéria Penal do Ministério da Justiça e Segurança Pública (MJSP), a Convenção de Budapeste deve aumentar os pedidos de cooperação jurídica internacional, pois "as investigações brasileiras necessitam cada vez mais de provas eletrônicas de outros países. Esta Convenção facilitará e incentivará os investigadores a utilizarem essa estratégia".

A percepção do setor cibernético como um elemento chave para a defesa e a segurança nacional do Brasil se materializou em 2008 com a elaboração da Estratégia Nacional de Defesa (END). Em 2012 foi revisada, atualizada e publicada conjuntamente com a Política Nacional de Defesa (PND). Este documento destaca o setor cibernético como um dos três setores estratégicos para a defesa nacional, ao lado o setor nuclear e espacial, com base na concepção de que a segurança é a condição em que o Estado, sociedade ou indivíduos se sentem livres de riscos e que a defesa é a ação para se obter o grau de segurança desejado. (MINISTÉRIO DA DEFESA, 2012).

> A implantação do Setor Cibernético tem como propósito conferir: confidencialidade, disponibilidade, integridade e autenticidade dos dados que trafegam em suas redes, os quais são processados e armazenados. Esse projeto representa um esforço de longo prazo, que influenciará positivamente as áreas de ciência e tecnologia e operacional. Sob a coordenação do Exército, significativos avanços têm se concretizado na capacitação de pessoal especializado e no desenvolvimento de soluções de elevado nível tecnológico. (Ministério da Defesa 2012b, 69).

O Ministério da Defesa aprovou, em 23 de outubro de 2023, por meio da Portaria nº 5.081, a Doutrina de Defesa Militar Cibernética. Esta doutrina estabelece os fundamentos da Defesa Cibernética Militar, proporciona unidade de pensamento sobre o assunto no âmbito da Defesa Nacional e promove a atuação conjunta das Forças Armadas (FA) na proteção do Espaço Cibernético de Interesse do Brasil. Além disso, apresenta conceitos, aplicações, informações e diretrizes para aprimoramento. No dia 23 de dezembro de 2023, o decreto n° 11.856 que institui a Política Nacional de Cibersegurança (PNCiber), com a finalidade de orientar a atividade de segurança cibernética no País. Estas legislações demonstram a preocupação e a importância de se ter meios e mecanismos que possam cobrir e combater os ataques digitais contra a Nação.

Por fim, os documentos brasileiros sobre defesa cibernética demonstram esforços significativos em estabelecer bases sólidas para as Forças Armadas. No entanto, eles não abordam explicitamente a guerra cibernética, conferindo ao Estado brasileiro flexibilidade para agir no ambiente virtual quando necessário.

5. CONSIDERAÇÕES FINAIS

Este artigo pretendeu analisar os Crimes Cibernéticos, os impactos à Segurança Nacional e o papel das Forças Armadas no combate. Para isso, partiu-se da definição dos crimes, a evolução histórica, traçando o cenário mundial até chegar no Brasil, bem como entender as ações estão sendo tomadas nesse setor.

A falta de regulamentação internacional no ciberespaço gera desafios para definir a legalidade de ações repressivas. Isso ocorre devido à ausência de previsão jurídica e normativa em regimes e instituições internacionais. Como resultado, alguns Estados buscam estabelecer limites soberanos virtuais para identificar agressores e punir transgressões. Ademais como vimos, as alianças entre países têm reforçado a importância e buscado formas de cooperar para combater essas ameaças.

Assim, ao se explorar a atuação brasileira na área, salienta-se as vulnerabilidades, que apesar das legislações e participação em treinamentos para a atuação das Forças Armadas, é necessário um maior aporte e meios sofisticados para que efetivamente a norma e as determinações de decretos possam vigorar de fato. Salienta-se que o Brasil tem se preocupado com a situação e tem investido mais forças armadas para o combate dos crimes Cibernéticos e proteção da soberania nacional.

REFERÊNCIAS

PINHEIRO, Patrícia; GROCHOCKI, Luiz R. (2016) **Noções de Direito Cibernético**. Campinas/SP: Editora Millennium.

VILAR, G.; GUSMÃO, E.; FRANCO, D.; GROCHOCK,L. (2016). **Tratado de computação forense**.

BARROS, Leonardo. (2018) **O ano da evolução dos ataques cibernéticos**. Canaltech. Disponível em: https://canaltech.com.br/seguranca/2018-o-ano-da-evolucao-dos-ataquesciberneticos-107168/. Acesso em 1 de novembro de 2019.

MACHADO, Jussara O. **Ciberguerra: conceitos, doutrinas, estratégias, operações, Instituições e o caso dos Estados Unidos**. (2014). 126f. Dissertação de Mestrado. Pontifícia Universidade Católica de Minas Gerais. Belo Horizonte, 2014.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa**. Brasília: MD, (2012). http://www.defesa.gov.br/arquivos/2012/mes07/pnd.pdf

Livro Verde Segurança Cibernética no Brasil. Brasília (2010) http://dsic.planalto.gov.br/legislacao/1_Livro_Verde_SEG_CIBER.pdf

Livro Branco da Defesa Nacional. Brasília (2012). http://www.defesa.gov.br/projetosweb/livrobranco/lbdndigital/

MINISTÉRIO DA DEFESA. **Especialistas debatem formas de coibir ataques cibernéticos no Brasil**. ASCOM. (2017) Disponível em:https://www.defesa.gov.br/noticias/33559-especialistas-debatem-formas-de-coibir-ataques-ciberneticos-no-brasil. Acesso em 01 de novembro de 2024.

RAMOS, Maria. **Ciberguerra e a política de cooperação da EU com a OTAN**. Boa Vista. (2015) Disponível em: http://ufrr.br/relacoesinternacionais/index.php/monografias-menu?Download=101:monografia-maria-sharlyany-marques-ramos-ciberguerra-e-a-politica-decooperacao-de-eu-com-a-otan&start=20. Acesso em 02 de junho de 2024.

MINISTÉRIO DA DEFESA (MD). **Doutrina Militar de Defesa Cibernética**. Portaria Normativa nº 3.010. Brasil, 2014. Disponível em: <https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf>. Acesso em 02 de novembro de 2024.

BRASIL. **Estratégia Nacional de Segurança Cibernética** – E-Ciber. Presidência da República. Brasília, Decreto nº 10.222, Brasil, (2020). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm. Acesso em 2 de novembro de 2024.

MILHOMEM, Flavio; RODRIGUES, André. **Crimes militares cibernéticos: Aspectos materiais, processuais e de investigação.** (2022)

Disponível em: https://www.observatoriodajusticamilitar.info/single-post/crimes-militares-cibern%C3%A9ticos. Acesso 03 de novembro de 2024.

AYRES, Danielle. **Segurança e defesa cibernética: Desafios e perspectivas para os países da América do Sul.** 6º Encontro da Associação Brasileira de Relações Internacionais – ABRI Perspectivas sobre poder em um mundo em redefinição 25 a 28 de Julho de 2017 Belo Horizonte – MG PUC-MG. Disponível em: http://www.encontro2017.abri.org.br/resources/anais/8/1499705250_ARQUIVO_SegurancaeDefesaCibernetica-DanielleJaconAyresPInto.pdf Acesso em: 29 de outubro de 2024.

BALDWIN, D. A. **Power and International Relations: a conceptual approach.** New Jersey: Princeton University Press. (2016)

24CYBER REVIEW 2019. BRASIL. Disponível em: http://www.brasil.jlt.com/midia/noticias-e-releases/2019/04/nova-edicaocyber-view-2019. Acesso em 29 de outubro de 2024.

MINISTRY OF PUBLIC SECURITY. **Disposições sobre Supervisão e Inspeção de Segurança na Internet por Órgãos de Segurança Pública.** República Popular da China. (2018). Disponível em: www.gov.cn/gongbao/content/2018/content_5343745.htm. Acesso em 04 de novembro de 2024.

BRASIL. **Lei Geral de Proteção de Dados (LGPD)** – Lei nº 13.709/2018. Presidência Da República. Brasília, Brasil, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/L13709.htm. Acesso em 01 de novembro de 2024.

BOBBIO, N.; MATTEUCCI, N.; PASQUINO, G. **Dicionário de Política**. Brasília: Editora Universidade de Brasília (1998).

WENDT, Alexander. **Social Theory of International Politics.** 1. Ed. Cambridge: Cambridge University Press, 1999.

UNITED NATIONS. **Human Development Report.** United Nations Development Programme. Oxford University Press. New York, 1994.

Disponível em: <http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf>. Acesso em 01 de novembro de 2024

RAMOS, Hugo. **Ciberguerra: apropriação da tecnologia hoje, hegemonia das nações amanhã.** In: Instituto Universitário de Lisboa – ISCTE (2013) Lisboa. Disponível em: http://scholar.googleusercontent.com/scholar?q=cache:jPOVDiCUPoAJ:scholar.goo gle.com/+russia-+ciberconflito&hl=pt-BR&as_sdt=0,5. Acesso em 05 de novembro de 2024.

MERCOSUL. **Decisão sobre o repúdio à espionagem por parte dos Estados Unidos da América nos países da região**. Montevidéu, 12 de julho de 2013.

INSTITUTO DA DEFESA NACIONAL. **Reflexões sobre a nova "estratégia global da União Europeia para a política externa e de segurança"**. (2016) Lisboa. Disponível em: https://www.idn.gov.pt/conteudos/documentos/ebriefing_papers/PolicyPaper8_CarlosGaspar_AnaSantosPinto.pdf. Acesso em 05 de novembro de 2024.