XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

INTERNET: DINÂMICAS DA SEGURANÇA PUBLICA E INTERNACIONAL

DANIELLE JACON AYRES PINTO

MAIQUEL ÂNGELO DEZORDI WERMUTH

I61

Internet: dinâmicas da segurança pública e internacional [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto; Maiquel Ângelo Dezordi Wermuth.

– Florianópolis: CONPEDI, 2022.

Inclui bibliografia
ISBN: 978-65-5648-609-3
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constitucionalismo, Desenvolvimento, Sustentabilidade e Smart Cities

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Internet. 2. Dinâmicas da segurança pública e internacional. XXIX Congresso Nacional do CONPEDI Balneário Camboriu - SC (3: 2022: Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

INTERNET: DINÂMICAS DA SEGURANÇA PUBLICA E INTERNACIONAL

Apresentação

Apresentação

É com imensa satisfação que apresentamos a obra que reúne os artigos apresentados no Grupo de Trabalho "INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL I", durante o XXIX Encontro Nacional do CONPEDI, no dia 9 de dezembro de 2022, no Campus de Balneário Camboriú da UNIVALI.

O artigo de Danielle Jacon Ayres Pinto e Rafael Gonçalves Mota, intitulado "A GUERRA CIBERNÉTICA COMO A QUINTA DIMENSÃO DA GUERRA MODERNA E O SEU ENFRENTAMENTO CONSTITUCIONAL NO BRASIL" analisa a relação entre a evolução tecnológica, especialmente a importância que a rede mundial de computadores passou a ter na vida cotidiana dos indivíduos, instituições e estados e os conflitos bélicos, notadamente considerando que a guerra através de meios virtuais e cibernéticos passou a ser a quinta dimensão possível de desenvolvimento bélico, seguindo o mar, terra, ar e espaço.

Ezequiel De Sousa Sanches Oliveira e Greice Patricia Fuller, no artigo "A GUERRA CIBERNÉTICA NO CONTEXTO DAS CIDADES INTELIGENTES NO MUNDO PÓS-PANDÊMICO: PROVOCAÇÃO ANALÍTICA SOB O VIÉS DA CIBERSEGURANÇA /HACKING", abordam o uso da internet no contexto das "Smart Cities", salientando que a rede mundial de computadores é tomada como tecnologia da informação e comunicação, por impactar as ações humanas, razão pela qual deve passar por uma reflexão sob o viés da defesa cibernética no que toca à segurança da informação, notadamente no cenário descortinado pelo mundo pós-pandêmico, marcado pela profusão da cibercultura e da disseminação do universo hacker.

O artigo intitulado "A VIRADA TECNOLÓGICA E O PRINCÍPIO DA NECESSIDADE EM DAVID SCHMIDTZ: A QUESTÃO DA SEGURANÇA PÚBLICA NA ERA DO COVID19", de autoria de Feliciano Alcides Dias, Fabiel dos Santos Espíndola e Ubirajara Martins Flores, a partir da teoria pluralista da justiça de David Schmidtz, destaca que a transição da modernidade para a hipermodernidade é marcada por um descompasso imposto pela rapidez da evolução das ferramentas de tecnologia da informação e da comunicação e pelo desenvolvimento dessas atividades na Segurança Pública. Nesse sentido, a alternativa

encontrada na teoria de David Schmidtz propõe o respeito à individualidade das pessoas que, na sua concepção, significa justiça.

Em “ASPECTOS DIFERENCIADORES EM CURSOS DE FORMAÇÃO BÁSICA POLICIAL MILITAR”, Anderson Morais De Oliveira tematiza a formação policial no Brasil, apontando para a existência dos chamados currículos “ocultos” na formação de soldados da Polícia Militar. O estudo destaca as condições que fomentam o ingresso na carreira policial, alguns aspectos da cultura corporativa interna, bem como o aspecto influenciador nas relações de poder da atividade policial.

O artigo de Maiquel Ângelo Dezordi Wermuth e Fernando Antonio Sodre De Oliveira, sob o título “DA BIOPOLÍTICA DE MICHEL FOUCAULT À NECROPOLÍTICA DE ACHILLE MBEMBE: A FUNÇÃO DO RACISMO NA DIMENSÃO ESTRUTURANTE DA SEGURANÇA PÚBLICA NO BRASIL”, explora a possível conexão entre os conceitos de biopolítica (desenvolvido no percurso filosófico de Michel Foucault) e de necropolítica (que ocupa lugar de centralidade na filosofia de Achille Mbembe), perquirindo qual é a função que o racismo desempenha tanto no exercício do biopoder quanto do necropoder. Além disso, o texto busca-se analisar de que forma o racismo estrutura os Estados a partir da Modernidade, notadamente no que se refere à sua atuação no campo da segurança pública, ainda profundamente marcado pela seletividade étnico-racial.

No artigo “DESAFIOS À LEI GERAL DE PROTEÇÃO DE DADOS NA ERA DA INTELIGÊNCIA ARTIFICIAL: ENTRE O DIREITO À PRIVACIDADE E AS ROBOCALLS”, Matheus Adriano Paulo e Gilson Jacobsen analisam a oferta de produtos e serviços por meio de “Robocalls”, que são uma espécie de Inteligência Artificial desenvolvida para fazer ligações, emulando a ação humana e desafiando a melhor aplicação possível da Lei Geral de Proteção de Dados - LGPD, que pode e deve servir de freio a eventuais violações ao direito de privacidade dos cidadãos.

Em “DIREITO AO ESQUECIMENTO COMO FERRAMENTA TRANSNACIONAL PARA O ARMAZENAMENTO DE DADOS MAIS SUSTENTÁVEL”, Jaine Cristina Suzin, Jardel Anibal Casanova Daneli e Paulo Márcio da Cruz abordam a insustentabilidade do Armazenamento de Dados na Internet perante as dimensões ambiental, social e econômica, em um cenário que pode ser denominado de sociedade da informação transnacional. Nesse contexto, estudam a viabilidade do Direito ao Esquecimento enquanto ferramenta transnacional para a emergência da Sustentabilidade.

O artigo intitulado “ERA DA IA E O 5G: QUAL A VELOCIDADE DA (DES) INFORMAÇÃO?”, de Patrícia da Silva Almêda Sales e Debora Bonat, analisa a relação circunscrita entre a Inteligência Artificial (IA) e o Direito, especialmente no que diz respeito à desinformação na participação democrática com a expansão do 5G, enfocando as possíveis implicações na próxima fase de comunicação e compartilhamento de informações na 5ª geração de banda larga móvel, a exemplo da repressão digital, da vigilância em massa, do perfil de usuário aprimorado e microsegmentação etc.

No texto “FAKE NEWS E O PROCESSO ELEITORAL, A BUSCA PELO ENFRENTAMENTO E DIMINUIÇÃO DO FENÔMENO”, Rennan Gonçalves Silva, Lucas Gonçalves da Silva e Karla Thais Nascimento Santana discutem os impactos das fake news no processo eleitoral e analisam as medidas de enfrentamento a essas notícias durante o período eleitoral.

“O DILEMA DO SUJEITO MONITORADO NO PÓS-MUROS DO SISTEMA PRISIONAL” é o título do artigo e Joice Graciele Nielsson e Adriane Arriens Fraga Bitencourt, que analisa a posição do sujeito em monitoração eletrônica no sistema penal, ressaltando a necessidade de implementação de políticas públicas de apoio a esses sujeitos, com o efetivo acompanhamento de equipe multidisciplinar como condição mínima para a garantia da maior efetividade do sistema de liberdade monitorada.

Em “O DIREITO FUNDAMENTAL DA PROTEÇÃO DE DADOS PESSOAIS NA SEGURANÇA PÚBLICA E ÂMBITO PENAL: POSSIBILIDADES E DESAFIOS”, Joice Graciele Nielsson e Milena Cereser da Rosa abordam a proteção de dados pessoais enquanto direito fundamental e os desafios e possibilidades para a construção de uma Lei Geral de Proteção de Dados (LGPD) no âmbito da segurança pública e penal, como forma de garantir o direito fundamental a proteção de dados pessoais, diante da necessidade de equilibrar a privacidade e a efetividade da jurisdição penal, de modo a não prejudicar tanto o sistema jurisdicional quanto o titular do direito à proteção dos dados.

Mariana Chini e Maiquel Ângelo Dezordi Wermuth, no artigo “O “FUTURO” SOBRE CORPOS PENALIZADOS: TECONOLOGIA, SISTEMA PENAL E MONITORAÇÃO ELETRÔNICA DE PESSOAS” abordam os avanços da tecnologia no sistema penal, tendo por escopo central a monitoração eletrônica de pessoas, especialmente no contexto brasileiro, perspectivada a partir da estigmatização de pessoas eletronicamente monitoradas na esfera penal.

“RECONHECIMENTO FACIAL E (IN)SEGURANÇA PÚBLICA: VIOLAÇÃO A DIREITOS DA PERSONALIDADE IMPULSIONADA PELO EXCESSO DE VIGILÂNCIA” é o título do texto de Micaela Mayara Ribeiro, Vinícius Fachin e Zulmar Antonio Fachin, que analisa o uso da tecnologia de reconhecimento facial na segurança pública, aferindo os impactos que o excesso de vigilância pode ocasionar nos direitos da personalidade dos cidadãos

Por fim, Maite Neves Guerra e Thiago Santos Aguiar de Pádua, no artigo intitulado “VALIDADE JURÍDICA DO PRINT SCREEN DE WHATSAPP COMO PROVA NO PROCESSO PENAL”, discutem a necessidade de validação e autenticação de provas digitais, em especial as conversas do aplicativo WhatsApp, sugerindo o auxílio das novas tecnologias.

O(a) leitor(a), por certo, perceberá que os textos aqui reunidos, além de ecléticos, são críticos quanto à realidade a utilização das novas tecnologias na contemporaneidade – notadamente no campo da segurança pública e da segurança internacional–, o que reflete o compromisso dos(as) autores(as) na busca pela adequação do uso dessas tecnologias aos textos convencionais e constitucionais centrados na dignidade da pessoa humana.

Tenham todos(as) uma ótima leitura! É o que desejam os organizadores.

Danielle Jacon Ayres Pinto – UFSC

Maiquel Ângelo Dezordi Wermuth - UNIJUÍ

A GUERRA CIBERNÉTICA COMO A QUINTA DIMENSÃO DA GUERRA MODERNA E O SEU ENFRENTAMENTO CONSTITUCIONAL NO BRASIL

CYBER WARFARE AS THE FIFTH DIMENSION OF MODERN WARFARE AND ITS CONSTITUTIONAL FACING IN BRAZIL

Danielle Jacon Ayres Pinto [1]
Rafael Gonçalves Mota [2]

Resumo

A guerra em geral faz parte indissociável da história e são fatores fundamentais no que diz respeito a definição das relações de poder estatais. Os conflitos bélicos acabaram por influenciar decisivamente a formação dos povos e dos estados, e sempre caminharam ombro a ombro com a evolução tecnológica, especialmente considerando que as inovações industriais e tecnológicas sempre foram utilizadas de forma direta nas guerras. Nesse contexto o trabalho analisa a relação entre a evolução tecnológica, especialmente a importância que a rede mundial de computadores passou a ter na vida cotidiana dos indivíduos, instituições e estados e os conflitos bélicos, notadamente considerando que a guerra através de meios virtuais e cibernéticos passou a ser a quinta dimensão possível de desenvolvimento bélico, seguindo o mar, terra, ar e espaço. Comenta-se a seguir como a tecnologia e a rede mundial de computadores transformaram-se em um instrumento bélico, especialmente considerando a relevância que os processos cibernéticos e virtuais adquiriram no mundo moderno. Por fim, analisa-se os reflexos de tal modalidade de conflito na soberania estatal, especialmente a ressignificação do conceito e da relevância das fronteiras geográficas estatais e a previsão de um modelo constitucional de enfrentamento de situações críticas de conflitos cibernética. A metodologia utilizada foi bibliográfica. O Objetivo principal é analisar o reflexo para a soberania estatal da guerra cibernética.

Palavras-chave: Guerra, Guerra cibernética, Soberania, Exceções constitucionais

Abstract/Resumen/Résumé

War in general is an inseparable part of history and they are fundamental factors with regard to the definition of state power relations. War conflicts ended up decisively influencing the formation of peoples and states, and they always walked hand in hand with technological evolution, especially considering that industrial and technological innovations were always used directly in wars. In this context, the work analyzes the relationship between

[1] Coordenadora da Pós-Graduação em Relações Internacionais da UFSC, Vice-Presidente da Associação Brasileira de Estudos de Defesa - ABED.

[2] Doutor em Direito Constitucional pela Universidade de Fortaleza – UNIFOR. Professor Auxiliar da Universidade de Fortaleza - UNIFOR. Professor Assistente da Faculdade Ari de Sá (Fortaleza/CE).

technological evolution, especially the importance that the world wide web has come to have in the daily life of individuals, institutions and states and war conflicts, notably considering that war through virtual and cybernetic means has passed to be the fifth possible dimension of war development, following the sea, land, air and space. It is discussed below how technology and the World Wide Web have become a weapon of war, especially considering the relevance that cybernetic and virtual processes have acquired in the modern world. Finally, the reflexes of this type of conflict on state sovereignty are analyzed, especially the re-signification of the concept and relevance of state geographic borders and the prediction of a constitutional model to face critical situations of cyber conflicts. The methodology used was bibliographic. The main objective is to analyze the reflection for state sovereignty of cyber warfare.

Keywords/Palabras-claves/Mots-clés: War, Cyber war, Sovereignty, Constitutional exceptions

INTRODUÇÃO

O estudo da guerra confunde-se com a própria história, fazendo com que se compreenda que o desenvolvimento humano teve no conflito bélico um elemento presente e decisivo para a formação do cenário político e econômico moderno. A natureza do conflito sofreu grandes e profundas alterações no avançar dos séculos, tendo o mundo assistido à sua escala maior no século XX com duas guerras de proporções planetárias.

Dessa forma, a guerra acompanhou a evolução da sociedade, bem como incorporou os avanços técnicos e tecnológicos para o melhor desenvolvimento bélico e imposição de poder militar. No presente trabalho, inicialmente se analisará a evolução da guerra como fenômeno histórico próprio da humanidade, especialmente diante do fato dos conflitos bélicos estão presentes há séculos na realidade mundial, culminando com duas guerras de proporções globais O conflito bélico, portanto, sempre foi determinante para a definição das forças políticas e econômicas.

A seguir, analisa-se como a guerra cibernética passou a ter uma relevância indiscutível no cenário bélico, especialmente considerando que os indivíduos, corporações e estados passaram a utilizar cada vez mais meios cibernéticos e virtuais nas suas relações cotidianas, tornando tais elementos mais passíveis de ações militares diante do reflexo grave que produzem.

Dentre os reflexos trazidos com a maior utilização de meios cibernéticos e virtuais, alguns atingem o conceito clássico de soberania e da relevância das fronteiras nacionais, impondo uma ressignificação obrigatória da relevância dos limites geográficos entre os estados. Por fim, busca-se analisa-se os reflexos que um conflito cibernético produz para a soberania estatal uma vez que os conflitos bélicos já não são travados mais, necessariamente na dimensão cinética mas também na dimensão cibernética, quer num contexto tático, quer estratégico.

Desta forma, resta necessário a criação de um modelo constitucional de enfrentamento de conflitos cibernéticos que tenha como alvo as instituições nacionais brasileiras, seus cidadãos ou empresas. A necessidade advém do fato de que os modelos para o enfrentamento de situações críticas existentes na Constituição Federal de 1988, estado de sitio e de defesa, não são mais eficientes para o enfrentamento de uma crise ou ataque de matriz cibernética. Desta forma no presente trabalho analisa se as

características da guerra cibernética e a fórmula constitucional de enfrentamento de situações excepcionais ainda se mostra eficaz tal qual desenhada pelo legislador constituinte de 1988.

1 CONSIDERAÇÕES GERAIS SOBRE A GUERRA E OS CONFLITOS BÉLICOS NA HISTÓRIA

O homem tem no conflito armado uma realidade tão indissociável de sua própria evolução que é difícil entender o caminhar da sociedade, antiga ou moderna, sem a perfeita compreensão dos conflitos bélicos em suas mais variadas matizes. O conflito bélico seria intrínseco à política e à convivência humana, sendo entendido quase como um fenômeno "normal". (Magnoli, 2009, p.11)

Por outro lado, Luigi Ferrajoli indica que a guerra, como elemento caracterizado com um proposito de aniquilamento mútuo nem sempre existiu sendo, em boa verdade e na sua visão um fenômeno moderno, produzido e gerado pelos potentes meios de tecnologia militar. (2004, p. 30)

A guerra foi, é, e sempre será, fruto do conflito entre povos e estados, que independente da motivação e forma, leva a humanidade ao limite de sua existência. Na lição clássica de Clausewitz, a guerra nada mais é do que um duelo de grandes proporções onde, cada um tenta impor ao inimigo suas vontades e seus desejos, em resumo, seu objeto é abater o adversário sendo a guerra "um ato de violência destinado a forçar o adversário a submeter-se à nossa vontade". (2003, p. 7)

Norberto Bobbio indica que a guerra é vista por alguns como o problema central dos tempos atuais, e está intimamente ligado aos conceitos de Estado e direito. Indica o autor a existência de quatro espécies de relação entre guerra e direito: "a guerra como antítese do direito, como meio para realizar o direito, como objeto do direito e como fonte de direito" (2003, p. 117)

Divergências políticas, econômicas, religiosas ou meramente territoriais sempre foram motivadoras de guerras e conflitos, obrigando os envolvidos a organizarem-se para o enfrentamento das situações críticas, bem como redefinirem seus conceitos políticos e jurídicos fundamentais.

Na antiguidade os conflitos entre clãs, tribos e, posteriormente, reinos, fizeram com que as relações sociais, humanas e políticas fossem transformadas, especialmente

diante da necessidade de um nível mais elaborado de organização para o enfrentamento de tais situações.

A dualidade entre guerra e paz sempre esteve presente na história, afirmando Thiago Rodrigues (2008; p. 211/212) que a guerra e paz representam uma contraposição perene, sendo uma elemento determinante para que a outra seja obtida e representando de forma clara uma forma de determinação da ordem social, bem como, em muitos casos de processo de legitimação do poder soberano.

Após a batalha de Waterloo, e com a conseqüente derrota francesa, o Congresso de Viena estabeleceu um novo sistema europeu de forças políticas e militares, que dominaria até a eclosão da Primeira Guerra Mundial. Neste sentido, afirma Demétrio Magnoli que "na passagem de um sistema para o outro, a guerra conheceu uma mudança radical. Clausewitz decifrou o sentido da mudança e elaborou o paradigma da guerra contemporânea." (2009, p. 12)

O século XX chega com uma nova dimensão do conflito armado, as guerras mundiais. Exatamente um século atrás, a humanidade era levada a conhecer uma nova proporção de enfrentamentos bélicos, especialmente caracterizada por uma escala transcontinental de conflito armado. Tal realidade mudou de forma significativa a forma de ver a guerra como fenômeno político, principalmente considerando o surgimento de novos países, o desaparecimento de outros, a atuação maciça de tropas, a produção em escala industrial e os danos e mortes em escala até então impensada.

Neste sentido, como afirma Demétrio Magnoli (2009; p. 13/14) as guerras conduzidas no século passado levaram o conflito bélico a outra escala e dimensão, influenciando a política e a economia, que subverteram e explodiram os alicerces teóricos até então existentes sobre a guerra e a paz.

Tais conflitos, no entanto, por mais complexos que tenham sido, ainda mantiveram preservada a ideia central de soberania estatal e, principalmente, o significado das fronteiras nacionais e das formas tradicionais de produção industrial ou econômica, especialmente quando se considera que o processo de globalização da economia mundial acentuou-se apenas na segunda metade do século passado.

Assim como o século XX trouxe uma novidade na concepção de conflito bélico, a escala mundial, o atual século é iniciado consolidando uma tendência surgida nas últimas décadas do anterior, e que evolui numa velocidade vertiginosa: a guerra cibernética. Neste sentido afirma Joseph S. Nye Jr. que

> O que é novo neste século é o aumento dos conflitos irregulares e as mudanças tecnológicas que ampliam as vulnerabilidades e colocam o poder destrutivo nas mãos de pequenos grupos de atores não estatais que teriam sido considerados caros demais para serem utilizados em eras anteriores. E agora a tecnologia trouxe uma nova dimensão à guerra: as perspectivas dos ataques cibernéticos. (2012, p. 50)

As fronteiras geográficas já não possuem a mesma relevância já que o conceito clássico de soberania não mais responde satisfatoriamente às questões nacionais. A presença de tropas no terreno já não é garantia de supremacia militar ou sucesso bélico. A guerra foi levada a uma nova e ainda quase que integralmente desconhecida dimensão, não só política, mas também econômica. Como lembra Joseph S. Nye Jr., atualmente as guerras ocorrem muito mais dentro dos próprios estados ou em regiões bastante delimitadas do que entre países independentes e autônomos. (2012, p. 50)

Nesse sentido a existência de um Estado Nacional, tomando-se como referência o conceito moderno, passa necessariamente pela capacidade bélica concreta e permanente de proteger-se de ameaças intestinas e estrangeiras, bem como pela efetiva possibilidade de possuir e implementar um parque industrial e um cenário econômico que possam efetivamente dar lastro à atuação estatal no cenário internacional. Diante de tal ideia explica Smith que

> As guerras e os conflitos são travados a quatro níveis – político, estratégico, táctico e operacional -, com cada nível enquadrando o seguinte por ordem decrescente, a partir do político; é isto que confere contexto a todas as atividades de todos os níveis na prossecução dos mesmos objetivos, e lhes permite serem coerentes entre si. O primeiro nível, o político, é a fonte do poder e da decisão. Este nível existiu sempre, pois os exércitos entram em combate não apenas porque dois ou mais se encontram por acaso num campo de batalha e decidem ocupar o tempo, mas sim porque uma questão entre duas ou mais entidades políticas não pode ser resolvida de outro modo, exigindo o recurso aos meios militares. (2008, p. 30)

Afirma ainda Rupert Smith (2008, p. 30) que na guerra moderna a política é quem controla os militares, ou seja, a decisão de ir a guerra e dela sair fica adstrita apenas a esfera política, sendo tomada com base em eventuais ameaças a elementos caros ao estado, tais como, território, soberania, comércio, recursos, honra, justiça, religião, etc.

Diante dessa nova perspectiva não se pode deixar de associar as novas tendências da guerra moderna ao processo de globalização econômica, especialmente considerando que assim como em relação aos conflitos bélicos, não se pode mais atribuir às fronteiras a mesma importância. As novas tecnologias, especialmente a rede mundial de computadores (*internet*) passaram a impor novas formas de relação entre

indivíduos, empresas e estados. Tal mudança foi refletida nas questões militares e bélicas.

Percebe-se, portanto, que os conflitos bélicos representam uma realidade que não pode, ou pelo menos, não deve ser ignorada pela maioria dos estados nacionais modernos, especialmente pelas conseqüências econômicas, políticas e sociais. Nesse sentido, mesmo países com clara tradição pacífica como o Brasil, e que não possuem problemas aparentes e minimamente imediatos que os conduzam a um conflito bélico, não podem negligenciar os esforços relacionadas à criação e manutenção de uma política de defesa e segurança nacional minimamente estruturada, especialmente considerando a estrutura macroeconômica exigida para dotar o país de uma indústria capaz de garantir recursos para a promoção de tal segurança.

2 A GUERRA CIBERNÉTICA COMO A NOVA DIMENSÃO DA GUERRA

O desenvolvimento tecnológico rápido e intenso vivido nas últimas décadas no século passado e no começo do atual acabaram por impor mudanças em vários setores, desde das relações pessoais e humanas, até o incremento de negócios e transações comerciais e financeiras. O lado positivo de tanto incremento técnico é a facilitação de negócios, aproximação de pessoas, dentre outras, porém há um outro lado, o uso de recursos tecnológicos como instrumento de crimes ou mesmo com o arma bélica.

Até o início do Século XX os conflitos bélicos eram travados em apenas duas dimensões, ou seja, no mar e na terra. As primeiras décadas daquele século assistiram ao incremento de uma nova dimensão, a guerra aérea, com a invenção e popularização do avião, tendo tal dimensão bélica alcançado grande destaque na Segunda Grande Guerra Mundial. A corrida pela exploração espacial travada por Estados Unidos e União Soviética nas décadas de 1950 e 1960 inaugurou uma quarta dimensão da guerra, a especial.

Como explica Gabriel Espírito Santo

> "O lançamento do primeiro satélite artificial no espaço pela URSS, em 1957, abriu o caminho para o que os teorizadores da estratégia militar consideram ser «o novo terreno elevado» cujo controlo constituirá uma «área importante» na condução de guerras futuras. Potências globais atuais como os EUA, ou emergentes, como a China, confiam mais no controlo do espaço do que noutras capacidades militares para o desenvolvimento de uma estratégia militar para o futuro. Para os EUA, um ataque que eliminasse as capacidades dos satélites que controla seria um «Pearl Harbor do espaço»" (2014, p. 350)

O atual século acabou por produzir mais uma dimensão bélica, a guerra cibernética, especialmente caracterizada pelo uso de recursos cibernéticos e virtuais como elementos de guerra, utilizando-se como meio de enfrentamento de inimigos, recolha de informações e preparação de defesas para ações ofensivas internas e externas. Neste contexto, Richard Clarke e Robert Knake definem a guerra cibernética como "ações de um estado-nação para invadir computadores ou redes de outra nação como a intenção de causar danos ou transtornos." (2015, p. 11)

Tais dimensões representam, portanto, os cinco domínios operacionais, e "as atividades no ciberespaço podem criar liberdade de ação para atividade em outros domínios assim como atividades em outros domínios também criam efeitos dentro e através do ciberespaço." (Carneiro, 2012, p. 79)

Aqui cabe um esclarecimento conceitual. Apesar da rede mundial de computadores (internet) acabar sendo, pelo óbvio motivo de estar acessível praticamente em qualquer lugar do planeta, o principal "espaço" onde as ações de guerra cibernética são realizadas, o conceito de ciberespaço é mais amplo e "inclui a Internet, além de várias outras redes de computadores que não deveriam ser acessíveis a ela." (Clarke e Knake, 2015, p. 60)

A velocidade com que o uso de meios tecnológicos e cibernéticos como elemento militar se difundiu é a prova de que as sociedades cada vez mais dependentes de tecnologia nas mais diversas esferas, tornaram-se na mesma frequência vulneráveis. A nova realidade impôs novas realidades bélicas, especialmente diante da velocidade dos atos característicos, fazendo com que "devido à natureza única da guerra cibernética, podem existir incentivos para se atacar primeiro." (Clarke e Knake, 2015, p. 2)

A guerra cibernética, portanto, passa a ser utilizada tanto do ponto de vista tático como estratégico, sendo desenvolvida de forma autônoma ou combinada com a chamada guerra cinética ou convencional. Nestes termos ensinam Richard Clarke e Robert Knake

> "A segunda guerra contra o Iraque e o mais recente ataque israelense contra a Síria demonstraram duas formas diferentes de guerra cibernética. Uma é o uso da guerra cibernética para facilitar um ataque convencional (o exército dos Estados Unidos prefere o termo ataque "cinético"), desativando as defesas do inimigo. A outra é o uso da guerra cibernética para enviar propaganda e desmoralizar o inimigo, distribuindo e-mails e outras mídias da Internet, no lugar da antiga prática de soltar panfletos de aviões." (2015, p. 14)

No mesmo sentido, afirmam Paulo Santos, Ricardo Bessa e Carlos Pimentel que o chamado *cyberwarfare*

> "materializa acções de defesa ou de ataque contra todo o gênero de estruturas de informação e redes de computador, em que o campo de batalha é conduzido numa dimensão digital. Em termos mais específicos, dele deviram várias acções, das quais se destacam os acessos ilegítimos a redes de computadores, ataques de negação a serviços (Dos – Denial of Services), sabotagem a equipamentos através do ciberespaço e manipulação de fontes de informação tendo como fim influenciar os processos de gestão de informação e de decisão do adversário" (2008, p. 102)

A tecnologia, portanto, acaba por ser um elemento determinante e influenciador e que alterou o conceito de guerra, fazendo com que o *warfare* atual se produza d forma irregular, imprecisa e assimétrica, onde o campo de batalha clássico, ou seja, físico e concreto, passe a ser compartilhado com outro sem bases ou grandes efetivos, porém de extrema letalidade e eficiência que é o campo de batalha virtual. (Santos, Bessa e Pimentel, 2008, p. 99)

Tal modalidade de guerra não apenas é capaz de trazer novas realidades e elementos, mas também gera uma ressignificação de conceitos já existentes. Como exemplo podemos citar a necessidade de desenvolvimento de uma estratégia de segurança das chamadas infraestruturas críticas, ou seja, a proteção de áreas sensíveis e fundamentais para qualquer estado, tais como usinas de energia, centrais de desenvolvimento de água, estações de controle do tráfego aéreo ou de transporte ferroviário, metroviário ou rodoviário. Neste sentido, e comentando a matéria, destacam Paulo Santos, Ricardo Bessa e Carlos Pimentel "a Protecção de Infraestruturas Críticas, em inglês *Critical Infrastructure Protection (CIP)*, deve constituir uma preocupação central de um país perante as diversas ameaças que surgem do ciberespaço." (2008, p. 102)

No mesmo sentido indica Robert T. Uda, a vitalidade econômica de um Estado, bem como a segurança nacional e a proteção dos indivíduos depende decisivamente da proteção das chamadas infraestruturas críticas, não apenas do ponto de vista físico, mas igual ou principalmente do ponto de vista cibernético e tecnológico. (2009, p. 76)

A guerra cibernética pode ser vista sobre três grandes dimensões ou funções. A primeira delas é a defensiva, pelo qual os estados criam estratégias, políticas, protocolos e instituições para se proteger de ações agressivas de outros estados-nacionais, grupos criminosos ou terrorista ou mesmo ações individuais. A segunda função é a recolha de informações sobre países e pessoas que apresentam algum tipo de interesse ou ameaça. A terceira e mais complexa das funções é a face agressiva da guerra cibernética, pela

qual o estado irá atuar para agredir atores internacionais, diminuindo ou mesmo aniquilando sua capacidade militar, econômica ou política.

A Doutrina Militar de Guerra Cibernética publicada pelo Ministério da Defesa Brasileiro em 2014 sintetiza tais funções da seguinte forma: a) ataque cibernético; b) proteção cibernética; e c) exploração cibernética.

Por ataque cibernético deve-se compreender, nas palavras de tal doutrina, as "ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente." Já a proteção cibernética representa as medidas típicas da defesa cibernética, tendo caráter permanente e como foco principal proteger as redes de computadores e comunicações essenciais às atividades de segurança nacional. Por fim a "exploração cibernética" é caracterizada pelas "ações de busca ou coleta, nos Sistemas de Tecnologia da Informação de interesse, a fim de obter a consciência situacional do ambiente cibernético."

3 DO ENFRETAMENTO CONSTITUCINAL DA GUERRA CIBERNÉTICA COMO FORMA DE PROTEÇÃO DA SOBERANIA ESTATAL: O ESTADO DE EMERGÊNCIA CIBERNÉTICA

Esse cenário, onde a tecnologia ganha um espaço de relevância cada vez maior da vida cotidiana, leva naturalmente a conflitos bélicos de quinta dimensão, com dito, a cibernética. Isso acabou por produzir um impacto forte no conceito de soberania estatal, fazendo com que a relevância das fronteiras geográficas fosse ressignificada.

Classicamente as guerras eram travadas apenas no campo físico, ou seja, de forma cinética, e diante de tal realidade, a preservação das fronteiras tornava-se fundamental para a garantia da soberania estatal. Atualmente com a existência concreta de agressões virtuais às instituições, empresas e edificações, que se trate de infraestruturas críticas ou não, a soberania estatal pode estar gravemente ameaçada mesmo que não existe a presença concreta de um "inimigo" no limite fronteiriço definido pelo direito internacional.

Diante disso, a matriz constitucional de proteção para os casos de situações excepcionais precisa ser refeita na maioria dos países, sobretudo no Brasil. No caso brasileiro, a Constituição Federal de 1988 não poderia imaginar como possível um cenário de emergência constitucional que envolvesse a guerra virtual, notadamente

considerando que se tinha na época um cenário ainda bastante embrionária de tecnologias cibernética, estando por exemplo a rede mundial de computadores (*internet*) ainda em fase de desenvolvimento e popularização inicial.

A possibilidade de o Estado Nacional sofrer ataques em suas instituições mais vitais por meio de ações cibernéticas, faz com que se perceba que a soberania estatal foi claramente fragilizada ou flexibilizada, ou seja, diante do cenário atual de desenvolvimento tecnológico dos conflitos humanos, notadamente com a guerra cibernética, temos a matriz constitucional de soberania estatal precisa ser reconstruída, ou pelo menos sofrer nova significação.

Diante deste quadro, é evidente que o modelo constitucional brasileiro não está ajustado para regular uma situação como esta, especialmente considerando que legislador constituinte de 1988 não poderia imaginar, nem mesmo no mais radical dos exercícios de imaginação que, menos de trinta anos depois, a ameaça à segurança nacional não estaria em ataques convencionais a fronteira territorial, mas sim aos dados eletrônicos e toda gama de serviços por eles controlados.

A estruturação de um modelo constitucional que tenha em mente o cenário cibernético de guerra passa a ser imperativo na preservação do Estado Brasileiro uma vez que a relação clássica de tempo de reação ou manobra para buscar autorização legislativa para o enfrentamento da ofensa já não se mostra viável já que o conflito virtual apresente um grau de velocidade imediata jamais visto, obrigando muitas vezes como visto anteriormente, a ações ofensivas anteriores a concretização de agressões.

Vê-se com isso que a reação estatal, e neste sentido, necessariamente capitaneada pelo Executivo, deve ser imediata e rápida, porém isso representa agir em um contexto bélico ainda não imaginado na estrutura constitucional, representando um novo desafio já que a estrutura constitucional atual imagina um cenário de guerra convencional.

O artigo 137 da Constituição Federal de 1988 indica que o Presidente da República poderá decretar o Estado de Sítio em situações extremas, notadamente relacionadas à "comoção grave de repercussão nacional ou ocorrência de fatos que comprovem a ineficácia de medida tomada durante o estado de defesa e declaração de estado de guerra ou resposta a agressão armada estrangeira."

Vê-se com isso que o cenário de guerra permitirá ao Chefe do Executivo Federal a decretação de uma hipótese prevista para casos extremos e que permite a utilização

de instrumentos próprios para o momento e que segundo o texto constitucional devem ser tomadas “contra as pessoas”, cite-se:

> Art. 139. Na vigência do estado de sítio decretado com fundamento no art. 137, I, só poderão ser tomadas contra as pessoas as seguintes medidas:
>
> I - obrigação de permanência em localidade determinada;
> II - detenção em edifício não destinado a acusados ou condenados por crimes comuns;
> III - restrições relativas à inviolabilidade da correspondência, ao sigilo das comunicações, à prestação de informações e à liberdade de imprensa, radiodifusão e televisão, na forma da lei;
> IV - suspensão da liberdade de reunião;
> V - busca e apreensão em domicílio;
> VI - intervenção nas empresas de serviços públicos;
> VII - requisição de bens.
>
> Parágrafo único. Não se inclui nas restrições do inciso III a difusão de pronunciamentos de parlamentares efetuados em suas Casas Legislativas, desde que liberada pela respectiva Mesa.

Existe no texto constitucional um ferramental próprio para a defesa do Estado, porém, ao analisar com mais precisão tais ferramentas, percebe-se que todas fazem menção expressa, ou estão implicitamente ligados, a uma dimensão física/material. Desta forma são impróprias ao cenário do enfrentamento de ameaças cibernéticas pois são medidas que dizem respeito à “pessoas”, não havendo a possibilidade de utilização contras instituições, países ou mesmo máquinas e computadores.

Comente-se, apenas para ilustrar, algumas das medidas acima citadas. Elas tratam de limitar a permanência de pessoas a em determinada “localidade”, detenção em “edifício”, busca e apreensão “domiciliar”, suspensão do direito de “reunião” ou mesmo a requisição de bens. Percebemos com isso que tais instrumentos tem necessariamente uma dimensão corporal, ou seja, restringir o direito de locomoção motora ou mesmo apreender ou utilizar bens e objetos úteis ao, digamos, esforço de guerra.

Tais ferramentas, no entanto, mostram-se plenamente inócuas ou ineficazes diante de um cenário de guerra virtual, pois como restringir a liberdade de um agressor virtual ou mesmo como é possível evitar digamos uma “reunião cibernética” de agentes inimigos, especialmente quando localizados em estados estrangeiros? Como apreender documentos ou elementos virtuais? Como reagir a ataques ocorridos apenas no âmbito da rede mundial de computadores com tais instrumentos?

Mesmo os dispositivos que podem ser utilizados no contexto cibernético, como o previsto no inciso III do citado artigo, qual seja, *restrições relativas à inviolabilidade*

da correspondência, ao sigilo das comunicações, à prestação de informações e à liberdade de imprensa, radiodifusão e televisão, na forma da lei terão uso restrito e limitado, pois será que é possível entender tais restrições como uma autorização para retirada do ar de um sítio de internet nocivo, ou mesmo autorizarão o ataque a redes de computadores nocivas ou inimigas? Ou ainda a inutilização de sistemas eletrônicos de corporações ou países considerados inimigos ou ameaçadores?

Estas são apenas algumas questões que precisam ser enfrentadas do ponto de visto teórico, e principalmente, devem estar presentes na norma constitucional antes da efetiva ocorrência da agressão para que se evite o arbítrio ou a exceção fora do direito. Em resumo, a exceção oriunda de um ataque cibernético ao Brasil, ou as suas instituições essenciais, deve estar prevista antecipadamente para garantir o respeito ao modelo democrático de estado que escolhemos e que seja adequado à preservação dos direitos e garantias constitucionais.

Vê-se, portanto, que a ação estatal no cenário de um conflito cibernético é pautado por outros elementos e instrumentos, muitas vezes utilizados fora do território nacional porém partindo dele. Desta forma os conceitos clássicos de soberania e poder estatal exigem uma revisão.

Neste sentido afirmam Richard Clarke e Robert Knake (2015, p. 41) que:

> Em uma análise mais aprofundada, entretanto, a estratégia reflete uma compreensão de alguns dos principias problemas criados pela guerra cibernética. Sobre a geografia do ciberespaço, a estratégia reconhece implicitamente o problema da soberania (“a falta de fronteiras geopolíticas...permite que ocorram operações em quase qualquer lugar), bem como a presença de alvos civis (“o ciberespaço atravessa fronteiras geopolíticas... e é firmemente integrado às operações de infraestrutura crítica e à atuação do comércio”). No entanto, não sugere que esses alvos civis devam ficar de fora dos limites dos ataques norte-americamos. Quando se trata de defender alvos civis nos Estados Unidos, a estratégia passa a vez para o Departamento de Segurança Interna (DHS).

Assim as permissões mais extremas que são encontradas atualmente no texto constitucional são incapazes de dar ao Estado Brasileiro condições eficientes de agir na defesa da segurança nacional no cenário aqui apresentado, qual seja, o de uma ciberguerra.

É diante desse quadro que surge a necessidade de discussão dos limites da proteção à soberania estatal, bem como em que medida o Estado Brasileiro, atendendo

a dispositivos constitucionais pode agir diante de um ataque cibernético, com o devido respeito os direitos fundamentais e regras de governança.

Desta forma, algumas conclusões podem ser tomadas. Primeiro a partir do cenário de um conflito bélico cibernético surge a necessidade de um modelo constitucional de exceção preparado para o enfrentamento deste cenário peculiar. Tal modelo seria complementar aos já existentes, ou seja, não se trataria de uma substituição completa do sistema constitucional atual, mas sim uma complementação com o modelo de "estado de defesa e guerra cibernética".

Tal modelo, o "estado de emergência cibernética", habilitaria o texto constitucional a disciplinar medidas que viriam a ser implementadas em três níveis, distintos, conforme a ameaça apresentada: crimes cibernéticos de grande porte à setores ou infraestruturas sensíveis, terrorismo cibernético e guerra cibernética.

Cada uma dessas dimensões seria tratada de forma a habilitar as Forças Armadas, instituições policiais e outros entes estatais, mediante ordem expressa do Presidente da República e referendo do Poder Legislativo, a realizar todas as medidas preventivas, de defesa e ofensiva para fazer o eficaz enfrentamento de ataques cibernéticos internos ou externos.

Um dos pontos essenciais desse modelo é a existência de mecanismos de controle prévios e posteriores de dupla natureza – políticos e jurídicos – para que tais medidas sejam autorizadas e implementadas.

Dentre tais poderes e possibilidades de ações estaria assumir o controle de servidores públicos e privados em caráter provisório (apenas o suficiente para anular e controlar a ação agressora), bem como, analisadas as recomendações técnicas, atacar servidores, computadores ou redes localizados em países estrangeiros quando tal medida fosse a única cabível para preservar as infraestruturas criticas cibernéticas brasileiras.

Desta forma as ações policiais e militares de caráter cibernéticos estariam concentradas em duas frentes básicas. De um lado assumir o controle imediato de redes, servidores, computadores ou quaisquer outros sistemas necessários para a efetiva proteção das instituições, corporações e indivíduos. Por outro, do ponto de vista externo, ficam as autoridades militares brasileiras, autorizadas a agir de forma ofensiva contra entes estatais ou não estatais estrangeiros que representem risco imediato ou potencial à soberania nacional.

Tais medidas e permissões seriam provisórias e apenas pelo prazo e na intensidade suficientes para reagir e inutilizar tais atos agressivos, sendo possível inclusive a realização de medidas e atos anteriores a agressões externas quando se mostrar que tal conduta é a única possível para a salvaguarda efetiva da soberania estatal.

Outro ponto essencial que caracteriza o "estado de emergência cibernética" é a existência do citado duplo controle. Por ele, fora as necessárias comunicações realizadas pelo Presidente da República das medidas a serem implementadas aos Presidentes dos demais Poderes da República.

O controle político será feito pelo Congresso Nacional, que ao ser comunicado da decisão presidencial para ativar o modelo constitucional de exceção cibernética poderá sustar tal decisão. Haverá, no entanto, uma diferença importante sobre os atuais modelos de exceção previstos na Constituição Federal. Diante da urgência que o panorama informático exige, notadamente pela velocidade típica de suas ações, o Parlamento terá um prazo concreto para referendar ou não a ativação do modelo, caso não faça, tacitamente o autoriza.

O controle jurídico será feito nos termos da legislação aplicável, passando a constituir crime de responsabilidade do Presidente da República (com a devida mudança legislativa) a utilização de tal medida sem que exista justificativa técnica e ameaça comprovada.

Também não se excluirá da apreciação do Poder Judiciário as medidas que são realizadas efetivamente, havendo a possibilidade de suspensão das mesmas caso haja uma ofensa concreta as regras constitucionais, sendo aqui a importância de as definir de forma prévia e concreta no texto constitucional para, com isso, evitar uma atuação casuística ou motivada por interesses indevidos.

CONCLUSÃO

A guerra esteve e está diretamente ligada ao caminhar da humanidade, estando relacionado a interesses políticos, econômicos, religiosos ou sociais. Desta forma, à medida que novas realidades passam a fazer parte do cotidiano, acabam por refletir diretamente nas relações humanas.

Nas últimas décadas o rápido desenvolvimento da tecnologia impôs grandes e irreversíveis mudanças na sociedade moderna, impactando decisivamente nos

indivíduos, empresas e nas ações do estado. Na mesma medida que os novos recursos tecnológicos, especialmente a rede mundial de computadores (internet) geraram desenvolvimento, facilitação de negócios, dentre outros aspectos positivos, também acabam por criar novas fragilidades e riscos.

O final do século passado e início desse acabou por inaugurar uma nova dimensão na guerra, ou seja, os conflitos bélicos não são travados apenas no mar, terra, ar e espaço, mas também no ciberespaço. Tal dimensão, acompanhando a tendência dos avanços tecnológicos, muito rapidamente acabou por atingir muita relevância e repercussão, quer do ponto de vista tático, quer estratégico.

Tal nova dimensão impõe não apenas a atualização de medidas técnicas e cibernéticas, mas igualmente a adaptação das constituições nacionais e respectivos ordenamentos jurídicos, especialmente considerando que tal espécie de conflitos apresenta um grau de urgência e pequena margem de manobra para reação, o que obriga a ações rápidas do estado, porém devidamente ajustadas aos princípios de um estado democrático de direito.

No caso brasileiro, resta evidente que não existe previsão constitucional adequada a um cenário de emergência cibernética já que os estados de defesa e sítio que atualmente representam os modelos de exceção constitucional em situações extremas são ineficazes diante das características próprias de tal dimensão bélica.

Desta forma, faz-se necessária a criação do "estado de emergência cibernética" a ser deflagrado por ordem do Presidente da República em situações de ameaças tecnológicas e virtuais, autorizando as Forças Armadas a agirem e reagirem a agressões e ofensas que comprometam as infraestruturas críticas cibernéticas brasileiras. Tal modelo, concebido previamente, sempre deve estar sujeitado ao duplo controle – político e jurídico – para garantir que as medidas realizadas não apenas são necessárias como harmônicas com os preceitos constitucionais.

REFERÊNCIAS

BOBBIO, Norberto. **Os problemas da guerra e as vias da paz**. São Paulo: Editora UNESP, 2003

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil.* Brasília, DF: Senado Federal: Centro Gráfico, 1988

_____, A Doutrina Militar de Guerra Cibernética, DF: Ministério da Defesa, 2014

CARNEIRO, João Marinonio Enke. **A guerra cibernética: uma proposta de elementos para formulação doutrinária no Exército Brasileiro**. 2012, Tese (Doutorado em Ciências Militares). Escola de Comando e Estado- Maior do Exército (ECEME), Rio de Janeiro.

CLARKE, Richard A. e KNAKE, Robert K. **Guerra Cibernética: A próxima ameaça à segurança e o que fazer a respeito**. Rio de Janeiro: Brasport, 2015.

CLAUSEWITZ, Carl Von. **Da Guerra.** São Paulo: Martins Fontes, 2003.

FERRAJOLI, Luigi. **Razones Jurídicas del Pacifismo.** Madrid: Editorial Trotta, 2004.

HANSON, Victor Davis. **Guerra: El origem de todo.** Madrid: Turner Publicaciones, 2011.

KEEGAN, John. **Uma história da guerra.** São Paulo: Companhia das Letras, 2006.

KISSINGER, Henry. **A Ordem Mundial: Reflexões sobre o carácter das nações e o curso da história.** Portugal: D. Quixote, 2014.

MAGNOLI, Demétrio (org). **História das Guerras.** São Paulo: Contexto, 2009.

NYE, Joseph S. Jr. **O Futuro do Poder.** São Paulo: Benvirá, 2012.

RODRIGUES, Thiago. **Guerra e política nas relações internacionais.** São Paulo: EDUC, 2010.

SANTO, Gabriel Espírito. **Da arte da guerra à arte militar**. Cascais: Tribuna da História, 2014.

SANTOS, Paulo; BESSA, Ricardo e PIMENTEL, Carlos. **Cyberwar: O fenômeno, as tecnologias e os actores.** Lisboa: FCA, 2008

SMITH, Rupert. **A utilidade da força:** a arte da guerra no mundo moderno. Coimbra: Edições 70, 2008.

UDA, Robert T. **Cybercrime, Cyberterrorism, and Cyberwarfare**. New Jersey: Xlibris, 2009