UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO SOCIOECONÔMICO
DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS
CURSO DE GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

Luiz Filipe Brüske

O Departamento de Defesa dos EUA e a Network-Centric Warfare na Guerra do Iraque

Florianópolis,
2024

Luiz Filipe Brüske

O Departamento de Defesa dos EUA e a Network Centric Warfare na Guerra do Iraque

Trabalho de Conclusão de Curso de Graduação em Relações Internacionais do Centro Socioeconômico da Universidade Federal de Santa Catarina, como requisito obrigatório para a obtenção do título de Bacharel em Relações Internacionais.

Orientador(a): Profa. Graciela de Conti Pagliari, Dra.

Florianópolis,

2024

Brüske, Luiz Filipe
O Departamento de Defesa dos EUA e a Network-Centric Warfare na Guerra do Iraque / Luiz Filipe Brüske ; orientadora, Graciela de Conti Pagliari, 2024.
77 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro Socioeconômico, Graduação em Relações Internacionais, Florianópolis, 2024.

Inclui referências.

1. Relações Internacionais. 2. Relações Internacionais. 3. Geopolítica. 4. Tecnologia. 5. Segurança Internacional. I. Pagliari, Graciela de Conti. II. Universidade Federal de Santa Catarina. Graduação em Relações Internacionais. III. Título.

Luiz Filipe Brüske

O Departamento de Defesa dos EUA e a Network-Centric Warfare na Guerra do Iraque

Florianópolis, 07 de junho de 2024.

O presente Trabalho de Conclusão de Curso foi avaliado e aprovado pela banca examinadora composta pelos seguintes membros:

Lisa Belmiro Camara

Universidade Federal de Santa Catarina

Gustavo Fornari Dall'agnol

Universidade Federal de Santa Catarina

Certifico que esta é a **versão original e final** do Trabalho de Conclusão de Curso que foi julgado adequado para obtenção do título de Bacharel em Relações Internacionais por mim e pelos demais membros da banca examinadora.

Documento assinado digitalmente
Graciela de Conti Pagliari
Data: 17/06/2024 22:30:41-0300
CPF: ***.263.070-**
Verifique as assinaturas em https://v.ufsc.br

Profa. Graciela de Conti Pagliari, Dra.

Orientadora

Florianópolis, 2024.

Aos amigos e à minha família.

From the beginning, we knew that this war would never happen. After the hot war (the violence of conflict), after the Cold War (the balance of terror), here comes the dead war - the unfrozen cold war - which leaves us to grapple with the corpse of war and the necessity of dealing with this decomposing corpse which nobody from the Gulf has managed to revive. America, Saddam Hussein and the Gulf powers are

fighting over the corpse of war (Baudrillard, 1991, p.30)

RESUMO

O objetivo central deste trabalho é analisar de que forma a doutrina militar intitulada de Network-Centric Warfare (NCW) influenciou os aspectos táticos da invasão americana ao Iraque em 2003. O trabalho é dividido em três grandes seções. A primeira delas trata de apresentar a história intelectual e científica da NCW, focando-se na relação do Departamento de Defesa (DOD) dos EUA com o desenvolvimento das Ciências Cibernéticas. A segunda seção aborda diretamente os principais intelectuais responsáveis pela teorização da NCW, e como essa doutrina se inseriu e foi internalizada pelo DOD. A terceira seção aborda especificamente como essa doutrina influenciou a forma pela qual os Estados Unidos (EUA) conduziram sua invasão ao Iraque em 2003, e como a NCW acabou sendo contestada nesse contexto bélico, tendo em vista que a Guerra do Iraque teria sido o grande teste empírico dessa doutrina. Os métodos utilizados para esse trabalho foram o Hipotético-Dedutivo em conjunto com o de Estudo de Caso, pretendendo-se assim comprovar uma hipótese a partir de constantes tentativas de falseamento e, ao final, verificar as dinâmicas trabalhadas em um caso concreto.

Os principais resultados desse trabalho foram: o impacto específico da NCW na condução americana da Guerra do Iraque e a conexão do pressuposto estratégico da superioridade informacional ligado à NCW com a consolidação do estado de vigilância global instaurada a partir da liderança dos EUA.

Palavras-chave: Network-Centric Warfare; Revolução Informacional; Cibernética; Guerra do Iraque; Pentágono; Contrainsurgência computacional.

ABSTRACT

The central objective of this work is to analyze how the military doctrine known as Network-Centric Warfare (NCW) influenced the tactical aspects of the American invasion of Iraq in 2003. The work is divided into three main sections. The first one aims to present the intellectual and scientific history of NCW, focusing on the relationship between the U.S. Department of Defense (DOD) and the development of Cybernetics. The second section directly addresses the key intellectuals responsible for theorizing NCW and how this doctrine was integrated and internalized by the DOD. The third section specifically examines how this doctrine influenced the way the United States conducted its invasion of Iraq in 2003 and how NCW was ultimately contested in this war context, considering that the Iraq War was considered the major empirical test of this doctrine. The method used for this work was the Hypothetico- Deductive, aiming to verify a hypothesis through constant attempts of falsification. The main results of this work are: the specific impact of NCW on the American conduct of the Iraq War and the connection of the strategic assumption of informational superiority of NCW with the consolidation of the global surveillance state established under the leadership of the USA.

Keywords: Network-Centric Warfare; Information Revolution; Cybernetics; Iraq War; Department of Defense; Computational counterinsurgency.

.

LISTA DE PRINCIPAIS ABREVIATURAS E SIGLAS

NCW	Network-Centric Warfare.
DOD	Department of Defense.
RMA	Revolution in Military Affairs.
DARPA	Defense Advanced Research Projects Agency
WW2	World War 2

SUMÁRIO

1. INTRODUÇÃO

O sociólogo e filósofo francês Jean Baudrillard, conhecido por suas provocações e reflexões acerca de simulações e simulacros, escreveu ao longo do ano de 1991 um conjunto de três estranhos artigos em relação à Guerra do Golfo. Seguindo-se a ordem cronológica dos eventos, tendo em vista respectivamente o lapso temporal entre a autorização do Conselho de Segurança da ONU à invasão, para o início das operações de fato e o rápido término do conflito, os artigos se intitulam: *The Gulf War will not take place, The Gulf War: is it really taking place?, The Gulf War did not take place*[1].

Em suma, o filósofo francês percebia que as profundas alterações tecnológicas e midiáticas que envolviam as operações no Iraque desafiavam quaisquer definições formais de Guerra (enquanto um fenômeno político bem definido). Evidentemente, Baudrillard não negava a profunda realidade material das operações lideradas pelos EUA em resposta à invasão iraquiana ao Kuwait, mas buscou provocar os seus leitores no sentido de avaliar o que de fato ocorria com a Guerra.

A cobertura midiática ao vivo do conflito e a utilização ostensiva de tecnologias até então pouco vistas, como as bombas inteligentes e os caças *stealth,* além da própria estratégia militar dos EUA que consistiu do bombardeio *offshore* praticamente irrestrito da infraestrutura civil e militar iraquiana, contribuíram para a criação de um senso de irrealidade fabricada, em que os significados e significantes perdiam-se no consenso manufaturado da grande mídia americana, em que a fascinação e o horror fundiam-se em um perfeito simulacro imagético (Baudrillard, 1991, pg.54).

Esses elementos devem ser levados em conta ao se analisar a Guerra do Iraque, que afinal nunca foi uma guerra por definição: não houve declaração de guerra por parte dos EUA. O desenvolvimento da tecnologia militar nos EUA (culminante na Network-Centric Warfare) e sua influência na condução americana de sua invasão ao Iraque em 2003 é o tema central deste trabalho.

Precisamente, o que está em análise não é apenas a tecnologia (especialmente a informacional) em si, como algo dissociado da realidade social e

[1] Respectivamente: A Guerra do Golfo não irá ocorrer, a Guerra do Golfo está mesmo ocorrendo?, e A Guerra do Golfo não ocorreu (Baudrillard, 1991, pg. 8, tradução nossa).

política que moldaram o desenvolvimento dessas técnicas e ciências, como será apresentado, mas sim deve-se analisar as interpretações e fantasias que os seres humanos fazem dessas tecnologias. Mais especificamente, será exposta a história material e intelectual da vaga doutrina chamada de NCW e como esse conjunto de ideias, oras mais concretas, e oras mais vagas, moldou a estratégia dos EUA em seus conflitos armados no final da década de 1990 e nos avançares do século 21.

O período do pós Guerra Fria trouxe à tona uma série de novos desafios à segurança global, em um contexto de enfraquecimento de determinados Estados Nacionais e desafio às formas tradicionais de condução de conflitos. Ao mesmo tempo, a década de 90 foi marcada pela expansão dos mercados produtivos e financeiros globais (expansões muitas vezes violentas), conectados especialmente pelo Espaço Cibernético, entendido como o conjunto de estruturas físicas e digitais aceleradas pelas Tecnologias da Informação.

Essa expansão foi marcada por uma hegemonia econômica e militar global dos Estados Unidos, que visou ao máximo expandir a atuação de seu capital industrial e financeiro, além de sua posição militar através da OTAN, com a criação e expansão de novas frotas, bases e missões de paz ao redor do mundo.

Ao longo da década de 90, também se tornou evidente que o espaço informacional seria cada vez mais relevante para o espectro de dominação total perseguido pelos EUA em termos econômicos e militares (esferas inseparáveis em certo sentido), notando-se um crescente direcionamento da política militar e de inteligência dos EUA nessa direção (BANDEIRA, 2017, pg. 34). Afirma-se que a própria lógica econômica neoliberal, extremamente financeirizada, privatizada e desregulamentada, opera ao redor do acesso à informação, contribuindo para a percepção das oportunidades e riscos envolvidos no campo informacional.

Os ataques de 11 de Setembro marcam uma inflexão na política americana. Nos termos do historiador Moniz Bandeira, esses eventos marcaram uma “mutação de estado”, em que grupos da elite americana se posicionaram de forma essencialmente hegemônica na condução da política externa e interna do país, sendo eles: a elite financeira de Wall Street, o Complexo Industrial-Militar-Defesa, o complexo de extração mineral e energética e o *agrobusiness* (BANDEIRA, 2017, pg. 81).

A forma pela qual foi conduzida a invasão ao Afeganistão e ao Iraque são marcas dessa dominação, além de estarem envolvidas com o objetivo da criação

de um Novo Século Americano, preconizado por alas do neoconservadorismo ianque, que se baseia na eliminação de resistências regionais que pudessem ameaçar os interesses securitários e econômicos dos EUA, com o objetivo da consolidação de um verdadeiro império global (ARRIGHI, 2007, pg. 182)

Também no contexto do 11 de setembro é iniciada a chamada Guerra ao Terror, que concebeu às agências de segurança e inteligência dos EUA uma carta branca para a espionagem e vigilância global. Principalmente através da National Security Agency (NSA) e da Central Intelligence Agency (CIA), e também através de empresas privadas contratadas pelo estado americano, como a Lockheed Martin, os governos americanos perseguiam o objetivo de acumular dados sobre cidadãos de todo o mundo, civis ou combatentes, principalmente através de interceptação de ligações e, posteriormente, de rastros deixados no mundo digital, como em mídias sociais e mecanismos de busca, que passaram a ser percebidos como uma fonte de inteligência militar (GONZÁLEZ, 2015, pg. 3).

Ao mesmo tempo, a invasão do Iraque marca a primeira vez em que a doutrina da Network-Centric Warfare é utilizada em larga escala. Essa doutrina pode ser compreendida como resultado de uma longa tradição do pensamento militar americano, que privilegia o desenvolvimento tecnológico em sua estratégia bélica (BOUSQUET, 2008, pg. 50). Mais recentemente, a relação entre estratégias bélicas e tecnologias foi repensada pela Revolution in Military Affairs (RMA), que consistiu de um conjunto de autores (civis e militares) que se dedicaram a delinear cenários para o futuro das guerras, o papel da tecnologia dos conflitos armados e a reorganização do aparato securitário dos EUA (SINGER, 2009, pg. 199).

Além das ciências computacionais e cibernéticas, a instrumentalização militar do conhecimento de ciências sociais qualitativas (antropologia, sociologia etc.) em união com modelos computacionais preditivos pode ser observada ao exemplo do Projeto Camelot (1964), que consistiu de um conjunto de estudos em universidades americanas em conluio com a Defense Advanced Research Projects Agency (DARPA, conhecida como o cérebro do Pentágono) sobre contrainsurgência através de modelos computacionais (HUNT, 2007, pg. 12). Dessa maneira, vê-se como abordagens tecno-centradas dos conflitos são uma marca do pensamento militar dos EUA, que privilegia em grande medida a superioridade tecnológica em sua estratégia bélica.

Assim, é do objetivo deste trabalho compreender a história do desenvolvimento dessa abordagem tecno-centrada no planejamento estratégico do DOD, em especial relativamente à incorporação de tecnologias da informação e computação em uma lógica de redes (Network-Centric), e observar como esse conjunto de princípios e estratégias se expressou na Guerra do Iraque (em especial nos seus primeiros anos). Além desse objetivo principal, serão buscados outros objetivos específicos, conforme se apresenta a seguir:

- Compreensão dos pressupostos teóricos e estratégicos da Network Centric Warfare, compreendida como a doutrina que incorpora uma série de evoluções científicas de diversos campos do conhecimento.
- Verificar a história do desenvolvimento de modelos computacionais e demais tecnologias da informação aplicados aos conflitos internacionais por parte dos EUA.
- Abordar aspectos teóricos relativos à busca de superioridade informacional nas disputas geopolíticas globais.
- Abordar aspectos relativos ao transbordamento da vigilância pretendida para o combate ao terrorismo dos EUA em todo o mundo, instaurando-se a Vigilância Global.
- Abordar as estratégias militares dos EUA em relação a sua invasão ao Iraque, e como essas estratégias se coadunam com os pressupostos da NCW.
- Discutir brevemente aspectos teóricos de abordagens bélicas tecno-centradas, especialmente em relação aos EUA.
- Discutir a relação do projeto de superioridade informacional dos EUA enquanto uma ramificação de suas estratégias informacionais.

Nesse contexto, busca-se abordar o tema exposto e os objetivos do trabalho a partir da seguinte pergunta de partida: Em que sentido a doutrina militar da Network-Centric Warfare, desenvolvida pelo Pentágono e que buscou incorporar as revoluções da tecnologia da informação, orientou a estratégia militar dos EUA em relação à Guerra do Iraque?

Verifica-se nesse caso a percepção de uma ligação causal entre a doutrina NCW e a condução dos EUA de sua invasão ao Iraque, comportando-se assim enquanto variável independente e dependente, respectivamente.

Com base no exposto, expõe-se que a hipótese principal a ser trabalhada é que Network-Centric Warfare se estruturou no sentido de adaptação aos desafios geopolíticos globais enfrentados pelos EUA, buscando também absorver e integrar as recentes inovações tecnológicas desenvolvidas no campo da informação e computação, assim orientando a estratégia militar dos EUA em sua invasão ao Iraque.

A hipótese secundária trabalhada ao longo do trabalho trabalha a afirmação de que o estado de Vigilância Global pode ser compreendido como um fruto e uma estratégia de defesa nacional americana da Network-Centric Warfare, já que a superioridade informacional é um pressuposto estratégico indispensável dessa doutrina, e que pode ser buscado através da vigilância em escala global.

O método de abordagem escolhido para esse trabalho é o Método Hipotético-Dedutivo, no qual há a perspectiva de comprovação de uma hipótese a partir de constantes tentativas de falseamento. Além disso, busca-se utilizar dessa base metodológica para a avaliação de um caso concreto, especificamente se tratando da invasão dos EUA ao Iraque em 2003. Nesse caso, as tentativas de falseamento se dão no sentido de verificar se de fato há uma relação direta entre a NCW e a condução da invasão ao Iraque, ou se essa relação pode ter sido supervalorizada de alguma forma.

Assim, ao mesmo tempo em que se busca encontrar uma resposta ao problema exposto, também se verifica o desdobramento desse problema em outras dimensões. A escolha desse método se dá pela sua flexibilidade e clareza, já que se define de antemão qual será o problema e a hipótese a ser comprovada. O método de procedimento escolhido é o da documentação indireta, buscando-se mapear os conteúdos abordados através de livros, artigos científicos, teses, entrevistas etc. Busca-se também analisar documentos de defesa e outras fontes primárias, que auxiliam no embasamento do estudo de caso apresentado.

A estrutura do trabalho segue uma divisão em três grandes seções. Após a introdução, o primeiro capítulo tem dois principais objetivos: apresentar a história das Ciências Cibernéticas e sua relação com o Departamento de Defesa dos EUA, e também abordar de forma teórica a relação entre Ciência, Tecnologia e Poder nas Relações Internacionais, focando-se especialmente no setor da informação.

Após o primeiro capítulo de cunho histórico e teórico, que pretende organizar as principais dinâmicas a serem analisadas posteriormente, o segundo capítulo é

organizado de forma a abordar especificamente o desenvolvimento da Network Centric Warfare nos EUA. Para isso, são pensados três subcapítulos.

O primeiro tem como objetivo apresentar os principais autores responsáveis pela teorização e conceituação dessa doutrina militar, inclusive os responsáveis pelas teorias da Revolution in Military Affairs (RMA), assim possibilitando mapear os campos intelectuais nos quais essas teorias foram gestadas, além de fornecer subsídios para a posterior verificação de como essas teorias influenciaram a condução americana da Guerra do Iraque.

No segundo subcapítulo, pretende-se justamente apresentar como essa doutrina militar foi gradualmente incorporada às Forças Armadas dos EUA, um processo marcado por resistências e contradições.

No terceiro subcapítulo, pretende-se abordar a hipótese secundária apresentada anteriormente, que afirma uma ligação íntima entre o pressuposto de Superioridade Informacional do Full-Spectrum Dominance, e que está no centro da NCW, com o estado de Vigilância Global desenvolvido pelos Estados Unidos. Para isso, será analisado o documento Joint Vision 2020: America's Military— Preparing for Tomorrow, publicado em 2000, no qual se verifica o interesse americano em desenvolver a Superioridade Informacional do país.

Na terceira grande seção, intende-se por apresentar de fato a análise relativa à tática de guerra conduzida pelos Estados Unidos em sua invasão ao Iraque, e como essa tática se coaduna, ou não, com os preceitos definidos na Network-Centric Warfare. Divide-se assim o capítulo em três subseções. O primeiro, de caráter mais descritivo, pretende apresentar concretamente quais foram as medidas das agências americanas no sentido de atualização ou reorientação de sua estratégia com base na NCW. Para isso, será necessário avaliar principalmente documentos primários do conflito, principalmente relacionados ao próprio exército americano, e avaliação de análises posteriores.

No segundo subcapítulo, pretende-se apresentar o conjunto de contradições estratégicas e operacionais que acometeram a estratégia americana em sua invasão ao Iraque, em especial na fase de manutenção efetiva do território iraquiano.

No terceiro subcapítulo, o objetivo é fornecer um balanço dos resultados e contradições encontrados com a NCW no Iraque, buscando-se assim viabilizar um apanhado das principais consequências dessa doutrina no Departamento de Defesa dos EUA atualmente. Argumenta-se de antemão que parcela considerável dos

principais pressupostos da NCW permaneceu sendo implementada nos posteriores usos de força dos EUA, como se verifica na ampliação da utilização de drones e target-killings no contexto de contrainsurgência.

Assim, a divisão proposta para esse trabalho pretende demonstrar a profunda ligação entre o DOD dos EUA com o desenvolvimento do campo informacional-computacional, um dos pontos fundamentais para a compreensão da NCW e de sua aplicação (ou tentativa de aplicação) na Guerra do Iraque.

2. COMPUTADORES TAMBÉM VÃO À GUERRA: O DEPARTAMENTO DE DEFESA DOS EUA E O MODELAMENTO MATEMÁTICO-COMPUTACIONAL DE CONFLITOS ARMADOS.

Esse capítulo trata da história e das dinâmicas de desenvolvimento das ciências cibernéticas e sua conexão com o Departamento de Defesa dos Estados Unidos (e, de forma mais ampla, com o complexo industrial-militar desse país), e também de considerações teóricas acerca dos impactos da Revolução Informacional para a Segurança Internacional. Assim, esse é um capítulo de caráter histórico-teórico, cumprindo o objetivo de embasar e fundamentar análises posteriores.

Essa possibilidade de embasamento se verifica pela consideração de que as ciências cibernéticas e computacionais, desenvolvidas principalmente no Pós-Segunda Guerra Mundial, influenciaram decisivamente o DOD em direção à NCW. Além disso, teorizar a relação da Revolução Informacional com a Segurança Internacional possibilita enxergar o conjunto de hipóteses e variáveis de forma mais contextualizada e abrangente, especialmente quando se analisa o papel do Estado no desenvolvimento científico.

2.1. CÉREBROS E COMPUTADORES SÃO A MESMA COISA: AS CIÊNCIAS CIBERNÉTICAS E O DEPARTAMENTO DE DEFESA DOS EUA.

> *I would like to compare artificial automata, specifically computing machines, with natural automata, particularly the human nervous system* (VON NEUMANN, 1966, p.2).

O campo intelectual-científico da Cibernética surgiu durante a Segunda Guerra Mundial e em seus anos subsequentes, em um momento em que um grupo de matemáticos, neurocientistas, físicos, antropólogos e engenheiros juntaram-se em uma rede científica inicialmente informal para a consolidação de interesses científicos em comum (CAPRA, 1997, pg. 67). Entre os principais nomes de destaque desse movimento, pode-se destacar Norbert Wiener, Claude Shannon (o criador da Teoria da Informação), Warren McCullough, Margaret Mead e John Von Neumann (um dos teorizadores do computador digital). Em seus respectivos campos

do conhecimento, essas pessoas representavam a elite científica dos EUA, apesar das distintas origens de seus membros.

Em termos gerais, a Cibernética pode ser definida como o estudo da comunicação e seus efeitos no exercício do controle de sistemas, sejam essas comunicações realizadas entre sistemas feitos de silício ou de carbono (WIENER, 1950, pg. 22). A palavra Cibernética deriva do grego, e significa algo como a arte do piloto ou timoneiro (WIENER, 1950, pg. 22). Ademais, para Wiener (1950) a sociedade humana como um todo poderia ser vista como um conjunto de sistemas comunicadores e mensagens, assim posicionando a informação (ou, mais precisamente, a troca de informação) como o elemento fundamental da própria humanidade.

As palavras-chave da Cibernética, portanto, são a Comunicação e o Controle, que se relacionam no sentido de como diferentes sistemas podem se comunicar e afetar suas estruturas através de *feedbacks.* Uma das marcas da Cibernética é a comparação, ou muitas vezes a equivalência, dos sistemas digitais computacionais e o sistema nervoso humano, muito devido às evoluções da neuropsicologia, que avançava no sentido da descoberta do funcionamento lógico-binário dos neurônios humanos. Nesse sentido, pode ser observado que a elaboração teórica de Von Neumann sobre o computador digital e as teorias de funcionamento análogo do cérebro humano evoluíram de forma interligada, sendo virtualmente impossível determinar qual delas surgiu primeiro (BOUSQUET, 2008, pg. 117). Os computadores digitais baseavam-se em modelos do cérebro humano, e vice-versa.

Por isso, os primeiros ciberneticistas ocupavam-se de desenvolver uma linguagem comum para a mente e para a máquina, ambos entendidos enquanto sistemas de funcionamento semelhante (CAPRA, 1997, pg. 67). O surgimento da cibernética, portanto, está intimamente relacionado às dinâmicas científicas do cérebro e do computador, que de certa forma surgem em suas formas contemporâneas de maneira indissociável (PICKERING, 1992, pg. 16). Já se nota, portanto, uma espécie de pensamento científico, fortemente financiado pela lógica militar, com tendências de caráter simbiótico entre a tecnologia e o ser humano, algo fundamental a ser notado no desenvolvimento posterior da NCW.

Outra marca do movimento cibernético era um grande otimismo em relação à tecnologia e sua capacidade de planejamento e controle de diversos aspectos da

sociedade humana, algo compartilhado em geral pelo *zeitgeist* do Pós Guerra (HEIMS, 1991, pg. 191).

Como mencionado, a Cibernética era um campo científico bastante heterogêneo em termos das áreas de especialização e atuação de seus membros, que variavam de matemáticos aos antropólogos, algo que se refletia nas diferentes opiniões de seus membros em relação à incômoda presença dos militares americanos e seus interesses no desenvolvimento desse campo científico (CAPRA, 1997, pg. 68).

As discordâncias entre Wiener, um autodeclarado pacifista, em especial após sua participação no esforço da WW2 (quando auxiliou o exército dos EUA a desenvolver sistemas anti-aéreos), e Von Neumann, que atuava enquanto consultor militar e participou de diversos projetos militares (como no próprio Projeto Manhattan e posterior desenvolvimento da estratégia nuclear americana), eram flagrantes nesse sentido (CAPRA, 1997).

Assinala-se que desde o início do desenvolvimento da cibernética durante a Segunda Guerra Mundial, a lógica da demanda militar por sistemas de *tracking and shooting* impulsionou esse campo científico, sendo um dos problemas mais recorrentes na pesquisa desses cientistas (CAPRA, 1997, pg. 66). Essa relação pode ser averiguada nos primórdios da cibernética, com a pesquisa de Norbert Wiener em sistemas de mira automáticas conduzida no Massachusetts Institute of Technology (MIT), considerada o coração do complexo acadêmico-militar dos EUA, e financiada pelo aparato securitário dos país (PICKERING, 1992, pg. 67).

Também os militares representavam parcela considerável dos fundos destinados à pesquisa cibernética, que posteriormente foram aplicadas no palco de batalha, como será averiguado em relação à Guerra do Vietnã e o conjunto de ideias defendidas pelo então Secretário de Defesa Robert McNamara. A própria presença e financiamento do aparato securitário e de inteligência dos EUA em relação à cibernética acabou por privilegiar um conjunto de ideias, teorias e modelos científicos (especialmente relacionados ao computador digital e ao cérebro humano) aplicáveis ao setor militar (HEIMS, 1991, pg. 192).

A principal promessa da Cibernética, nesse contexto, seria de aumentar a eficiência e a inteligência dos sistemas armados dos EUA através da aplicação dos conceitos cibernéticos de comunicação, controle e *feedback,* além de fornecer um arcabouço intelectual e científico em um sentido de simplificação da Guerra a um

conjunto de funções matemáticas e dinâmicas informacionais que permitiram a realização de simulações computacionais de conflitos, análise de sistemas e incremento na capacidade de controle (BOUSQUET, 2008, pg. 124).

Nesse contexto, pode-se afirmar que a Cibernética, enquanto uma ciência do controle e da comunicação, busca ao máximo minimizar a perda de informação e diminuir o ruído comunicacional, contribuindo para uma comunicação fluida entre diferentes sistemas. Nesse caso:

> Nesse framework conceitual, a incerteza e a imprevisibilidade - caos em outras palavras - são entendidas como deficiências informacionais e assim são suscetíveis de serem superadas pelo emprego apropriado de tecnologias informacionais-comunicacionais negentrópicas e simulações computadorizadas de conflitos (BOUSQUET, 2008, pg. 125, tradução nossa).

Pode-se compreender, portanto, o interesse militar dos EUA nas ciências cibernéticas. Em resumo, o pensamento do estrategista prussiano preconiza que qualquer conflito armado está sujeito à “névoa da guerra”, tratando-se da dificuldade de obter informações confiáveis e o panorama intrinsecamente confuso e caótico de qualquer conflito (SINGER, 2009, pg. 215).

A promessa central da Cibernética em sua aplicação ao campo militar seria, de certa maneira, dissipar essa névoa em direção ao controle central e completo do palco de batalha, algo que será também verificado de formas atualizadas em relação à NCW, conforme será abordado posteriormente.

Ao eliminar-se, ou ao menos reduzir-se, as nuances e subjetividades do fator humano dos conflitos, a Névoa da Guerra poderia ser manejada de forma menos caótica e incerta através do controle dos fluxos informacionais. Nesse contexto:

> O computador, também um produto do esforço de guerra, se tornou a nova metáfora tecnológica dominante pela qual o mundo poderia ser compreendido em termos de processamento de informação. O sonho da completa previsibilidade e controle central da guerra mecanicista renasceu com a guerra cibernética através da computação e ‘servomechanistic technologies’ e as ferramentas analíticas de pesquisas operacionais e análise de sistemas. A Guerra Fria e a ameaça permanente da aniquilação nuclear requerem níveis ainda maiores de automação e centralização da máquina de guerra e a promessa de estabilidade, em detrimento da perturbação, das tecnologias cibernéticas pareciam encaixar-se com a contenção e administração de um conflito de possíveis proporções apocalípticas. A guerra cibernética, portanto, enxergava a organização militar puramente como um processo vertical, uma vasta máquina tecno-social a ser integrada e dirigida através de uma hierarquia rígida com base

> em cálculos de pesquisas operacionais e análise de sistemas.
> (BOUSQUET, 2008, pg. 49, tradução nossa).

Essa exposição demonstra de forma clara e sintética como a cibernética foi inserida e interpretada pelo complexo securitário e de inteligência dos EUA, em suma tratando-se de um arcabouço teórico que preconizava um maior controle sobre a estrutura militar do país através da tecnologia da informação, muitas vezes referenciada de forma teórica, haja vista que essas tecnologias ainda estavam em desenvolvimento, e de análises operacionais e de sistemas. Assim, após essa breve contextualização intelectual e científica da Cibernética, busca-se analisar de que forma esse conjunto de ideias e práticas discursivas foram levadas ao palco operacional de batalha.

Em primeiro lugar, deve-se notar o papel especialmente relevante desempenhado pela pesquisa científica e a tecnologia militar durante o período da Guerra Fria, marcado pela constante ameaça da destruição nuclear e o enquadramento generalizado de praticamente todos os aspectos das Relações Internacionais ao redor do *framework* da bipolaridade, ou seja, da rivalidade entre o Bloco Ocidental (liderado pelos EUA) e o Bloco Socialista (liderado pela União Soviética).

Em termos metafóricos, pode-se argumentar que a Guerra Fria se organizou ao redor de um mundo-fechado, isto é, um domo enclausurado em si mesmo constantemente marcado pela crescente vigilância global e exercício do controle e do poder interestatal através da superioridade da alta tecnologia militar por parte das potências dominantes, e em que todos os eventos eram encarados a partir da lógica bipolar (EDWARDS, 1996, pg. 23).

Nesse contexto, a tecnologia computacional passou a tornar-se não apenas um componente da grande estratégia americana, conforme argumenta Edwards com base nos diversos projetos financiados e implementados pelos EUA (como a SAGE e posteriormente as redes precursoras da Internet), mas também se tornou um símbolo e uma miragem das disputas políticas e rivalidades da Guerra Fria (EDWARDS, 1996, pg. 23). Considerando-se o cenário exposto de desenvolvimento da computação a partir do campo cibernético, que considera também a interação entre os seres humanos e sistemas digitais, pode-se verificar a relevância do

pensamento cibernético para a política internacional desse período, especialmente na grande estratégia dos EUA.

Ressalta-se que além dos fatores levantados para o desenvolvimento da cibernética e sua influência no pensamento militar do período, existem fortes fatores culturais e históricos para que essas ideias relacionadas a abordagens tecno-centradas fossem especialmente férteis nos EUA. Fatores como o privilegiamento da matemática e a engenharia no Academia Militar de West Point e o fato de que a tecnologia e a capacidade industrial estiveram na base das vitórias americanas em seus conflitos armados, desde a vitória do Norte Industrial contra o Sul Agrícola, e a relevância da base industrial americana para a vitória do país na Primeira e Segunda Guerra Mundial, contribuíram para a criação de uma tradição militar que privilegia a superioridade tecnológica e industrial em relação aos demais países (BOUSQUET, 2008, pg. 129).

No pós WW2, as primeiras reestruturações do aparato securitário dos EUA no sentido de adaptação às transformações computacionais-cibernéticas se dão principalmente na Força Aérea, com o desenvolvimento do Semi-Automatic Ground Environment (SAGE), que se tratou do primeiro comando baseado em um sistema de controle e comunicações (lembrar das palavras chave da cibernética) de computadores dedicado ao monitoramento e defesa do espaço aéreo dos EUA iniciado em 1958 (BOUSQUET, 2008, pg. 132). Ainda que sua real eficiência tenha sido reduzida, a SAGE teria influenciado e incentivado um conjunto de projetos de comando-controle baseados na computação-cibernética a partir desse contexto (EDWARDS, 1996, pg. 97). Vê-se, portanto, as teorias cibernéticas e computacionais de fato adentrando os meandros do mundo material-estrutural.

Ao longo do tempo, o desenvolvimento desses sistemas de vigilância e controle automatizado dos espaços geográficos e humanos, sistemas esses baseados em radares, satélites, sensores e computadores, transbordou ao mundo civil, como se vê no caso do NAVSTAR Global Position System (GPS) e as consequências políticas da The Strategic Defense Initiative (Star Wars) do Governo Reagan, considerado um projeto sucessor ao SAGE (BOUSQUET, 2008, pg. 136).

No contexto da Guerra Fria, o principal meio de difusão e influência do conjunto de ideias relacionados à cibernética, análise de sistemas e pesquisa operacional aplicados à Segurança Internacional tratava-se da RAND Corporation, um *think-tank* criado pela Força Aérea dos EUA em 1948. A análise

militar/securitária da RAND baseava-se extensamente em simulações computacionais, jogos de guerra e doutrinas informacionais tecno-centradas, algo contraditório com visões mais conservadoras e tradicionais do alto comando militar dos EUA dos anos 1950, demonstrando que a adoção dessas ideias e práticas não se deu sem contradições (BOUSQUET, 2008, pg. 148).

Todavia, os defensores do campo intelectual estimulado pela RAND tiveram uma vitória considerável em 1961, quando Robert McNamara chegou ao posto de Secretário de Defesa, por indicação de Kennedy, já sendo conhecido por suas predileções para abordagens voltadas à tecnologia computacional (BOUSQUET, 2008, pg. 148). Em seu polêmico mandato (que durou de 1961-1967), McNamara cercou-se de analistas da RAND e conduziu um conjunto de políticas destinadas a aplicar o arcabouço teórico-científico da cibernética-computação no setor militar, principalmente através da concentração e coordenação do orçamento militar do país (EDWARDS, 1996, pg. pg. 27).

Com a intensificação dos conflitos armados no Vietnã, principalmente a partir de 1965, e o aprofundamento do envolvimento militar dos EUA nesse país, as ideias e práticas de McNamara passaram a ser de fato testadas em um ambiente bélico real. Sendo assim, a Guerra do Vietnã pode ser considerada o primeiro grande teste empírico da aplicação militar do conjunto de interpretações do campo cibernético-computacional, e que acabou resultando em uma derrota inegável das estratégias cibernéticas tradicionais (BOUSQUET, 2008, pg. 153).

A Guerra do Vietnã pode ser considerada um dos momentos chave da Guerra Fria e da política internacional do Século 20, haja vista a escala do conflito e sua relação com a contestação da hegemonia militar americana e sua suposta invencibilidade (ARRIGHI, 2007, pg. 139). Seus impactos também puderam ser sentidos na economia política internacional, dado a contestação do dólar enquanto moeda internacional e posterior quebra do padrão dólar-ouro, além de seus impactos na política interna dos EUA (ARRIGHI, 2007, pg. 144).

E, como pode-se notar, a derrota dos EUA nesse conflito também alterou decisivamente todo um conjunto de ideias e práticas relacionadas à aplicação da computação e cibernética aos conflitos armados, sendo cada vez questionada a própria ideia de que os conflitos armados poderiam ser simplesmente simulados e completamente compreendidos através da ciência, demonstrando assim a limitação dessas práticas.

Assim sendo, as abordagens tecno-centradas estiveram no centro da estratégia dos EUA em relação ao Vietnã, principalmente a partir de 1965, quando, aos auspícios de McNamara, os EUA iniciam um maciço bombardeio ao norte vietnamita (EDWARDS, 1992, pg. 159). Ao longo dos movimentos de entrada iniciais das tropas americanas, a criação da superioridade informacional e tecnológica dos EUA no palco de batalha tornou-se a prioridade estratégica dos EUA, principalmente através de equipamentos eletrônicos de comunicação e computadores dedicados ao processamento de informações e estatísticas de combate (EDWARDS, 1992, pg. 160). Todavia, logo verificou-se que a realidade concreta do palco de batalha vietnamita estava longe das simulações e teorias computacionais e cibernéticas preconizadas pelos cientistas e analistas do Pentágono.

Entre os desafios encontrados pelos EUA no Vietnã, deve-se destacar o forte fator de descentralidade da resistência local, que se utilizava em larga escala de técnicas de guerrilha, e a falta de um *front* único, fatores esses que desafiavam as concepções tecno-centradas de *hard power* (BOUSQUET, 2008, pg. 153). Mais tarde, as falhas táticas dos EUA no Vietnã frente às insurgências norte-vietnamitas e as transformações descentralizadoras e complexificadoras do palco de batalha seriam analisadas por analistas estadunidenses para a formação de uma nova doutrina de contrainsurgência (KALDOR, 2012, pg. 72). Decisivamente, esses aspectos futuramente viriam a influenciar a condução dos EUA em relação a sua invasão ao Iraque (apesar de que muitos erros tenham sido repetidos, curiosamente).

De qualquer forma, os EUA conduziram suas operações no Vietnã através de uma lógica voltada ao acúmulo e processamento de informações através de computadores e sistemas de vigilância em massa, além do uso extensivo de seu *hard-power* através de bombardeios, em um processo que poderia ser caracterizado como uma espécie de patologia informacional (BOUSQUET, 2008, pg. 153). Nesse caso, dois exemplos são relevantes para a compreensão de como essa “patologia” se expressou no Vietnã: a Operação Igloo White e o Civil Operations Revolutionary Development Support (CORDS), com sua ligação com o Projeto Phoenix.

Entre 1967 e 1972, a Força Aérea dos EUA conduziu a Operação Igloo White, que consistiu da utilização de aviões de reconhecimento e de milhares de sensores instalados ao longo dos territórios considerados relevantes para a Trilha de Ho Chi Minh, que consistia de um conjunto de estruturas logísticas da resistência

norte-vietnamita especialmente no Laos e no Vietnã do Norte, e cujas informações eram enviadas para uma central de processamento computacional na Tailândia (EDWARDS, 1992, pg. 157). A rede de sensores e voos de reconhecimento pretendiam registrar quaisquer sinais de movimentação humana nas zonas analisadas, fossem esses sinais de calor, som, vibrações ou mesmo o cheiro de urina, para assim possibilitar que os ataques aéreos e terrestres das tropas americanas fossem mais efetivos e letais (BOUSQUET, 2008, pg. 157).

As informações coletadas pelos aviões de reconhecimento e pelos sensores eram processadas por computadores IBM 360/65 e enviados para os jatos de ataque Phantom J-4, que recebiam a localização dos alvos a serem atacados com base nas informações coletadas, em um contexto em que os pilotos dos jatos sequer viam os alvos que estavam atacando e confiavam a decisão de ataque completamente às informações recebidas pela central de processamento de informações (EDWARDS, 1992, pg. 26). Nesse caso, observa-se já nesse momento um certo alienamento do indivíduo humano em relação a decisões centrais em conflitos armados.

Ainda que a Operação Igloo White fosse primeiramente propagandeada enquanto um sucesso das doutrinas cibernéticas de McNamara e seus analistas, logo verificou-se que a operação era não apenas excessivamente custosa (cerca de 1 bilhão de dólares por ano), mas era também ineficaz e muitas vezes mascarava os verdadeiros resultados de suas operações e da própria Guerra do Vietnã (EDWARDS, 1992, pg. 27).

Enquanto as estatísticas e relatórios oficiais da operação declaravam a destruição das infraestruturas críticas da resistência comunista, alardeando uma suposta taxa de 90% de sucesso na destruição de equipamentos que se utilizavam da Trilha Ho Chi Minh, a realidade do conflito demonstrou o sucesso da resistência norte-vietnamita em enganar e manipular a estratégia tecnológica dos EUA, que gerava falsos positivos e infectava os dados coletados pelos sensores (BOUSQUET, 2008, pg. 157). A grande marca do fracasso americano em conter a movimentação de equipamentos e veículos através dessa trilha foram as operações com tanques e artilharia pesada conduzidas pela resistência comunista dentro do Vietnã do Sul em 1972, que demonstraram a inabilidade dos EUA em eliminar as redes logísticas da resistência (EDWARDS, 1992, pg. 28). Nessa situação, a engenhosidade da resistência norte-vietnamita/comunista e a falibilidade dos sistemas informacionais

foram subestimadas, criando assim justamente aquilo que os ideais cibernéticos buscavam evitar, ou seja, a falha comunicacional e o aumento do caos na condução bélica.

No segundo caso, pode-se observar a busca dos EUA por uma melhor compreensão das dinâmicas humanas e populacionais da resistência através do CORDS, que consistia de um programa de contato civil-militar com a população sul-vietnamita, com o objetivo de identificar redes infiltradas de resistentes no ambiente rural dessa região (GONZÁLEZ, 2008, pg. 6). O aspecto informacional dessa operação era a coleta em massa de dados locais de através de militares dos EUA, com o suposto objetivo humanitário de ganhar as mentes e corações dos vietnamitas, e posterior armazenamento e processamento dessas informações em computadores IBM 1401 (VALENTINE, 1990, pg. 248). Nesse caso, verifica-se o interesse dos EUA em computacionar e enquadrar o conflito no Vietnã não apenas em termos de capacidades bélicas e identificação de alvos, mas também em termos socioculturais e populacionais, algo que será verificado também em relação à Guerra do Iraque.

O CORDS, todavia, possuía um lado paramilitar secreto e atuante (orientado ao redor do infame Projeto Phoenix), em que as informações coletadas e processadas pelos computadores americanos eram compartilhadas com agentes do governo sul-vietnamita e de outras agências do aparato militar dos EUA com o objetivo de justamente eliminar os insurgentes comunistas (GONZÁLEZ, 2008, pg. 1). Sabe-se atualmente, através de documentos oficiais revelados, que cerca de 26.843 insurgentes e simpatizantes comunistas não militares (incluindo professores) foram assassinados e/ou torturados em decorrência direta das informações do CORDS e o Projeto Phoenix (VALENTINE, 1990, pg. 364).

Verifica-se, portanto, que parte das derrotas militares sofridas pelos EUA no Vietnã e o prolongamento inesperado desse conflito se devem, em partes, ao limite encontrado do conjunto de estratégias e táticas tecno-centradas de hard-power utilizadas pelos EUA nesse conflito, ainda que esses aspectos tenham sido sub analisados em relação à Guerra do Vietnã (BOSQUET, 2008, pg. 152). Algumas facetas dos limites desse conjunto doutrinário de ideias são, por exemplo, a desconexão do aparato militar com o palco concreto dos conflitos, inclusive em termos das dinâmicas populacionais e socioculturais dos conflitos armados (especialmente em contextos de insurgência e contrainsurgência).

A exposição das dinâmicas científicas relativas ao desenvolvimento do campo cibernético e a relação desse conjunto de teorias com o setor militar dos EUA é relevante para os posteriores desenrolares da NCW, haja vista que em diversas instâncias os teóricos da NCW e seus "praticantes" destacam a cibernética enquanto referência, seja em termos de contraponto ou de embasamento teórico. Para compreender o envolvimento do setor militar dos EUA com o desenvolvimento da cibernética, e as posteriores evoluções e revoluções relacionadas a essas teorias, é preciso avaliar de forma teórica a relação entre ciência, tecnologia e poder nas Relações Internacionais, tendo em vista principalmente tecnologias relacionadas à computação e informação.

2.2. A REVOLUÇÃO INFORMACIONAL E SEUS IMPACTOS PARA A SEGURANÇA INTERNACIONAL

Analisar a formação política e ideológica da Network Centric-Warfare passa necessariamente por uma discussão acerca do impacto da tecnologia na prática de conflitos armados, ou, mais precisamente, na percepção de um determinado conjunto de sujeitos acerca de uma suposta revolução dos conflitos com base na tecnologia informacional. É impossível, portanto, discutir a NCW sem aprofundar-se minimamente no processo histórico e econômico chamado de Revolução Informacional.

A Revolução Informacional, ligada intrinsecamente à expansão das redes de comunicação digital e aos computadores, permitiu que o custo de criação, processamento e troca de informações fosse drasticamente reduzido, possibilitando que um número crescente de indivíduos, empresas e Estados-Nacionais obtivessem acesso a tecnologias até então concentradas nos países desenvolvidos do Norte Global (especialmente os EUA e o Reino Unido) (ERIKSSON; GIACOMELLO, 2006). Para alguns autores, as transformações da economia política global ocorridas entre as décadas de 70 e 80, com a contestação efetiva dos arranjos econômicos e políticos do Pós Segunda Guerra, em união com as revoluções tecnológicas ocorridas no campo da computação e da informação, significaram uma alteração profunda na própria organização do capitalismo global: de uma sociedade industrial, caminhava-se para uma sociedade pós-industrial, ou, ainda, uma sociedade informacional (ERIKSSON; GIACOMELLO, 2006). Todavia, ainda que os

impactos da Revolução Informacional tenham sido estudados em diversas áreas de concentração, o subcampo da Segurança Internacional parece ter sido pouco avaliado de forma sistemática e abrangente em relação a essas dinâmicas.

Ainda que o Espaço Cibernético, compreendido como o amálgama das dinâmicas e evoluções da Revolução Informacional, possa ser enquadrado de distintas formas pelas diversas teorias das Relações Internacionais, esse trabalho busca compreender de forma específica como os Estados-Nacionais se relacionam com esse setor, e, ainda mais especificamente, como essas tecnologias influenciam a interpretação, a estratégia e a condução de conflitos armados. Por isso, a lente principal a ser utilizada nesse trabalho é a do Neorrealismo Ofensivo, estruturada principalmente por John J. Mearsheimer, ainda que o Neorrealismo Defensivo, estruturado principalmente por Kenneth N. Waltz, também possa ajudar na compreensão do envolvimento do Estado-Nacional no espaço cibernético. Todavia, ressalta-se que ao longo do trabalho outras visões e abordagens teóricas são apresentadas, sendo o Neorrealismo, por sua vez, a orientação teórica geral do trabalho.

Nesse caso, essas outras visões e abordagens teóricas possibilitam a compreensão de aspectos mais específicos das discussões tratadas, haja vista o caráter essencialmente estrutural do Neorrealismo. Essas outras abordagens, por sua vez, não apresentam incompatibilidade inerente com a vertente teórica principal do trabalho (isto é, o Neorrealismo), sendo assim ferramentas de compreensão de fenômenos mais particulares.

Em linhas gerais, o pensamento Neorrealista Defensivo aplicado ao campo informacional-cibernético preconiza que os Estados-Nacionais estão interessados em desenvolver capacidades materiais nesse campo para a defesa de suas infraestruturas críticas (crescentemente conectadas ao Espaço Cibernético em níveis cada vez mais elementares), haja vista a percepção de ameaças de ataques cibernéticos de origem interna ou externa (ROCHA; FONSECA, 2019). Assim, ainda que o Espaço Cibernético seja muitas vezes tratado como um campo essencialmente informacional (e assim muitas vezes quase etéreo), há uma enorme materialidade para a construção desse espaço, composto por quilômetros de redes, milhões de computadores, satélites e afins. Infraestruturas físicas, portanto, estão no centro de qualquer discussão acerca de Guerras Cibernéticas ou Informacionais.

Acrescenta-se a essa visão defensiva que o Espaço Cibernético-Informacional é um meio dual, em que ações ofensivas e defensivas podem ocorrer. Nesse caso, pode-se afirmar que os Estados estão interessados em desenvolver também capacidades ofensivas para que seus objetivos estratégicos sejam buscados, assim significando que ataques através do ciberespaço são também uma ferramenta de poder nas Relações Internacionais (TABANSKY, 2011)./

Nesse caso, verifica-se uma consonância relevante com o pensamento Neorrealista de Mearsheimer, que afirma que os Estados estão interessados na ampliação de seu poder relativo através de ações ofensivas, tendo em vista que a guerra é considerada historicamente, de forma geral, uma das principais formas de aumento do poder de um determinado Estado Nacional (MEARSHEIMER, 2001).

Dessa forma, pode-se afirmar que a condução de ações ofensivas através do ciberespaço se dá, quando analisadas a partir do Estado, em uma lógica de ampliação do poder relativo de um determinado país, necessariamente em detrimento de outros. Acrescenta-se a isso a percepção de que o domínio da utilização de determinadas tecnologias pode acrescer o poder relativo de determinado país em relação a outros. Surgem-se assim rivalidades digitais, ancoradas em questões sistêmicas da política internacional.

Isso posto, torna-se imperativo compreender em detalhes o que foi a Revolução Informacional e de que forma os Estados se relacionam especificamente no campo cibernético-informacional e quais são as principais dinâmicas políticas desse espaço e como essas questões são enquadradas pelo Estado.

A definição categórica do que exatamente é e está sendo a Revolução Informacional se trata de uma tarefa complicada, haja vista os inúmeros processos e contradições que envolvem essa revolução, que é assim chamada em uma direta referência à Revolução Industrial (SSI, 2000). Percebe-se de antemão uma avaliação bastante corajosa de que a evolução do espaço cibernético-informacional poderia se tratar de um fenômeno histórico de volume e relevância semelhante à Revolução Industrial, um evento conhecido por suas profundas alterações e reorganizações da economia e da política global. Outro aspecto pouco comentado em relação a esse paralelo é que de fato, se a Revolução Informacional for semelhante à Industrial, pode-se afirmar que a formação do Espaço Informacional é um processo ainda em andamento, sendo essencialmente impossível avaliar como esse espaço se construirá e se conectará em um futuro de médio prazo.

A Revolução Informacional, portanto, é um processo em atual desenrolamento, cujas origens podem ser remontadas pelo menos para os primeiros esforços de desenvolvimento tecnológico no campo da computação durante a Segunda Guerra Mundial (SSI, 2000, pg. 8). Todavia, é durante a consolidação do processo da globalização (outro processo de difícil enquadramento) que a Revolução Informacional de fato se consolida e passa a abranger inúmeros espaços ao redor do mundo, tornando-se de fato uma Revolução em nível mundial principalmente com a disseminação da internet e a expansão da comunicação em massa em todo o mundo, ocasionando uma possível transformação na própria natureza do Poder (NYE, 2004). Portanto, a expansão do campo informacional é uma das primeiras expressões da Globalização Neoliberal (com todas as suas implicações geopolíticas e econômicas), ao mesmo tempo em que moldou a forma pela qual a Globalização se expressou em diversos outros campos, principalmente em relação à conectividade financeira e interpessoal, transformando radicalmente a política e a economia global em diversas instâncias.

Uma das facetas dessas novas dinâmicas e discussões relativas à expansão do espaço informacional é o questionamento da própria ideia de soberania estatal e da organização hierárquica da sociedade humana e da economia, que foram marcas indeléveis da organização capitalista das primeiras revoluções industriais e da política global da Guerra Fria (NYE, 2004). Mais especificamente, pode-se verificar que o conjunto de ideias políticas e econômicas que permeia o espaço informacional-cibernético e sua expansão através da globalização neoliberal está diretamente relacionado ao desafio neoliberal da ordem keynesiana-fordista, que assumia até então a primazia da organização capitalista do Pós-WW2.

As implicações desses processos entre si e com a própria reorganização da política global no Pós-Guerra Fria liderada pelos EUA, justamente o país que impulsionou o desenvolvimento da cibernética no Pós-WW2, são inúmeras e de primeira importância. Compreender a ligação entre a pretensão de poder global (muitas vezes praticado de forma unilateral) dos EUA com a contra-revolução neoliberal, e consequentemente com a expansão do espaço cibernético, é fundamental inclusive para melhor interpretação da NCW e a Guerra do Iraque, objeto alvo deste estudo.

Deve-se constatar a evidente realidade de que o ciberespaço se trata de um espaço (geográfico? antropomórfico?) novo, e que se expandiu em níveis globais

apenas há poucas décadas. Esse fato deve ser levado em conta ao analisar-se as teorias de Segurança Internacional, e de outras áreas afins, que tentaram enquadrar esse novo espaço em suas análises, principalmente ao se averiguar aparentes exageros e ingenuidades, ou mesmo em casos de extremo ceticismo. Nesse caso, diferentes visões privilegiaram distintos pontos relacionados à Revolução Informacional e a formação do ciberespaço, principalmente no potencial verdadeiramente disruptivo dessas tecnologias para o campo da Segurança Internacional.

Em seu livro “Cyber War Will Not Take Place”, cujo título parece referenciar os artigos de Baudrillard analisados anteriormente, Thomas Rid analisa os discursos e as percepções, em sua opinião muitas vezes infundadas, de que a tecnologia informacional e o ciberespaço alterariam as estruturas profundas da guerra e da política, por defender que essas novas dinâmicas informacionais e cibernéticas eram muito mais continuações de velhas práticas dos conflitos (como a espionagem, a sabotagem e a subversão), que de fato são novas disrupções ou destruições criativas (RID, 2013, pg. 13). Nessa visão, o alcance e o real potencial disruptivo das tecnologias informacionais-computacionais, ao menos para a Segurança Internacional, teriam sido supervalorizadas, ao menos em relação às dinâmicas estruturais profundas dos conflitos internacionais. Essa será uma contradição observada com autores que percebiam que os aspectos acrescidamente informacionais da sociedade humana iriam alterar de forma drástica as lógicas profundas dos conflitos armados, como se observa em relação aos autores e ideólogos da NCW.

Uma das características percebidas em relação ao espaço cibernético é sua possibilidade assimétrica de efeitos ofensivos, ou seja, mesmo Estados ou grupos não-estatais com poucas capacidades materiais tradicionais (como número de membros da organização e capacidade de financiamento) poderiam causar grandes estragos em um espaço interconectado, configurando assim novas percepções de vulnerabilidades (ERIKSSON; GIACOMELLO, 2006). Da mesma forma, a crescente conectividade global de diferentes territórios e a ampliação do ciberespaço através de novos sistemas possibilitou que analistas imaginassem uma nova maneira de conduzir conflitos em um ambiente crescentemente conectado (STEVENS, 2017, pg. 91).

Argumenta-se que esse é o caso da Network-Centric Warfare, que se tornou um amálgama de um conjunto de teorias relacionadas à Revolução Informacional e ao ciberespaço, e que se dedicava a possibilitar a aplicação dessas ideias no palco de batalha, sendo assim uma expressão do conjunto de ideias que preconizava a utilização dessas tecnologias em sentido ofensivo. Pode-se afirmar que a NCW foi, de fato, uma tentativa de adaptação de formatos militares mais tradicionais às novas dinâmicas informacionais (ou, mais precisamente, da interpretação específica dessas dinâmicas por parte dos analistas de segurança e militares envolvidos).

Voltando-se às origens e as perturbações da Revolução Informacional para a política internacional, deve-se notar de antemão que o campo cibernético-informacional-computacional está diretamente relacionado às políticas de desenvolvimento tecnológico do Departamento de Defesa dos EUA no Pós-WW2, conforme avaliado no primeiro subcapítulo. Isso não significa dizer que o Espaço Cibernético atual é completamente dominado por essa organização e suas ramificações, evidentemente, mas sim significa dizer que é impossível avaliar de forma concreta a evolução da computação, informática e a cibernética sem considerar o papel desempenhado pelo complexo de defesa e inteligência dos EUA.

Esse é um aspecto importante para a desmistificação de um conjunto de mitos e ideologias, geralmente de caráter neoliberal, que parecem identificar uma origem quase orgânica ou espontânea para a Revolução Informacional e a expansão desse espaço ao redor do mundo, processo que teria se dado única e exclusivamente pelas mãos invisíveis e digitalizadas do mercado e inspiradas pelas visões de empreendedores visionários (sonhadas ao fundo de uma garagem suburbana, em que garotos de Harvard tomavam coca-cola e jogavam videogames). A desconsideração do papel do Departamento de Defesa e do complexo industrial-militar dos EUA no desenvolvimento tecnológico e intelectual da Revolução Informacional é não apenas uma imprecisão, mas sim uma completa falácia, conforme demonstrado.

Ainda em relação ao papel das percepções acerca da Revolução Informacional e o impacto dessas visões para a Segurança Internacional, é notório o fato de que se construiu ao redor desse processo um conjunto de ideias alinhadas ao contexto internacional especialmente das décadas de 80 e 90. Em um artigo escrito em 1998, o pesquisador da RAND e diplomata dos EUA, David C. Gombert, escreve o seguinte em relação à Revolução Informacional:

> Essa explosão da criatividade humana, oriunda de um rápido crescimento no processamento de informação e compartilhamento de conhecimento, está se provando benéfica em três sentidos. Primeiro, está contribuindo para a Segurança Internacional ao espalhar o ideal da liberdade, e colocando o poder estatal opressivo na defensiva ou mesmo derrubando-o, e ajudando sociedades tradicionalmente pobres a se modernizarem. Em segundo, está aumentando o poder dos Estados Unidos em detrimento de nações opostas aos seus princípios e interesses através do valor estratégico do livre mercado, a ciência e a tecnologia. Em terceiro, está modificando a guerra em um sentido que permitirá aos EUA proteger seus interesses e a paz internacional a custos aceitáveis, apesar da disseminação de armas de destruição em massa (GOMBERT, 1998, tradução nossa).

Inúmeros aspectos dessa passagem podem ser salientados para se verificar como a Revolução Informacional não se trata apenas de questões tecnológicas, mas que possui também facetas fortemente políticas, principalmente pela forma pela qual foi gestada e interpretada por sujeitos ligados à burocracia dos EUA (mas não apenas desse país, evidentemente).

Pode-se verificar como a expansão desse ciberespaço está relacionada, de acordo com essas interpretações, com a expansão da democracia liberal contemporânea ao nível mundial. Através do compartilhamento teoricamente ilimitado e irrestrito de informações, acreditava-se que o espaço informacional seria um meio naturalmente difusor de ideias de liberdade democrática e seria também um facilitador para o desenvolvimento econômico. Claro, tratando-se de um desenvolvimento marcado pela abertura de mercados através da Globalização e da hegemonia militar dos EUA no Pós-Guerra Fria.

Para os objetivos desse trabalho, ressalta-se o destaque dado ao fato de que inegavelmente o autor supracitado identifica a liderança tomada pelos EUA no campo informacional como uma fonte de poder estatal, e um poder que poderia se expandir em relação a outras nações resistentes, combinando-se assim com a percepção neorrealista de que o ciberespaço é utilizado pelos estados-nacionais para ganhar vantagens relativas. Também não escapa o fato de o autor diferenciar nesse caso uma defesa de princípios e de interesses, possibilitando a interpretação de que essas vantagens estratégicas escapam do nível securitário e podem se expressar em outros campos, como o econômico e o ideológico.

Ainda mais relevante que esses aspectos, para a compreensão específica da NCW, pode-se verificar a percepção do autor de que a Revolução Informacional transformará permanentemente a forma de condução de conflitos, e que permitirá

aos EUA defender seus princípios e interesses a custos aceitáveis. Isso significa dizer, analiticamente, que as tecnologias associadas a esse processo permitiriam aos EUA sofrer menos danos materiais e humanos para atingir seus objetivos estratégicos. Em essência, é a redução da guerra a uma relação de custos e benefícios, marca clara da teoria econômica, algo que será também verificado na tônica dos teóricos ligados à NCW.

De fato, pode-se observar que a NCW é formada não apenas através dos legados advindos dos avanços das ciências cibernéticas e informacionais construídos principalmente após a Segunda Guerra Mundial, mas também absorve e exprime a consciência securitária das burocracias estadunidenses das décadas de 80 e 90. Há nesse quesito uma percepção de que a expansão das tecnologias relacionadas à Revolução Informacional seria de fato um propulsor do progresso nas Relações Internacionais, já que teria revitalizado o Primeiro Mundo, liberalizado o Segundo e reerguido o Terceiro (GOMBERT, 1998). Longe de ser um fenômeno neutro ou espontâneo, portanto, a Revolução Informacional exprime-se em um sentido bastante claro.

Porém, conforme observado no subcapítulo anterior, a construção das ideologias tecnocráticas relacionadas ao potencial dos computadores de planificar conflitos armados já se dava há vários anos, e inclusive refletiu-se na forma pela qual os EUA combateram a Guerra do Vietnã. Portanto, pode-se perguntar o que há de diferente na estruturação da NCW a partir da Revolução Informacional, já que muitos dos preceitos basilares dessa doutrina militar já se constituíam em anos anteriores.

Nesse ponto, afirma-se que a Revolução Informacional se tratou principalmente, especialmente em seu momento inicial, de uma inflexão em termos de massificação tecnológica (justamente o quesito de diminuição de custos de produção e compartilhamento de informação), possibilitando que muito dos preceitos e teorias construídas anteriormente pudessem ganhar novos horizontes perante a disseminação acelerada de dispositivos e estruturas informacionais. O sonho tecnocrático parecia ganhar substância por esse fator, e, pela primeira vez, os ideais de interconectividade e computação absoluta de todos os aspectos dos conflitos armados pareciam se tornar mais concretos.

Dessa forma, pode ser observado como a Revolução Informacional afetou decisivamente a Segurança Internacional, não apenas por haver transformado

permanentemente como os Estados-Nacionais percebem possíveis ameaças e oportunidades estratégicas em relação a seus rivais, mas como moldou a formação política e ideológica de formuladores de política. No caso específico dos EUA, país protagonista na Revolução Informacional, pode-se observar que a alta relevância dada à tecnologia computacional no planejamento securitário é já observada desde a Segunda Guerra Mundial. Não é ao acaso o papel desempenhado pelo complexo industrial-militar desse país no desenvolvimento de um conjunto de tecnologias relacionadas a esses processos, como o papel da Defense Advanced Research Projects Agency (DARPA) para o desenvolvimento da internet.

Dessa maneira, é fundamental compreender detalhadamente como a Network-Centric Warfare absorveu e interpretou essa tradição científica, militar e política dos EUA e buscou incorporá-la, a partir também de suas próprias inovações, de fato à organização e operacionalização das táticas estadunidenses em conflitos armados. Esses aspectos serão abordados no próximo capítulo.

2.3. CONCLUSÕES PARCIAIS

Conforme verificado, esse capítulo tratou de analisar o desenvolvimento das ciências cibernéticas e sua ligação com o complexo militar-industrial dos Estados Unidos, e de que maneira esse desenvolvimento se expressou em ocasião da Revolução Informacional e seus impactos para a Segurança Internacional. Além dos impactos estruturais dessa Revolução, também buscou-se verificar como esse processo foi enquadrado e analisado por sujeitos atuantes no corpo militar e estratégico dos EUA, o que será fundamental para se compreender a formação da Network-Centric Warfare.

Em relação aos principais resultados encontrados nesse capítulo, deve-se destacar a consideração de que a evolução, consolidação e expansão das ciências cibernéticas-computacionais e da Revolução Informacional não se deram em um vácuo político ou econômico, e tampouco foram frutos de processos espontâneos. De fato, é impossível analisar o desenvolvimento desses campos científicos e das inovações tecnológicas informacionais sem analisar-se o papel central e indispensável desempenhado por um conjunto de instituições ligadas ao complexo militar-industrial dos EUA. E essa ligação não se dá necessariamente por vias diretas, como através de programas de pesquisa financiados por organizações como

a DARPA, mas também através de instituições de pesquisa (como a RAND) e universidades (como o MIT), além de outras entidades aparentemente desconectadas desse aparato, mas que mantém ligações íntimas com agências de inteligência desse país (como a Fundação Ford).

Longe de ser uma exclusividade do campo cibernético-informacional, a influência do Estado Americano no desenvolvimento científico de diversos campos durante a Guerra Fria é ainda muitas vezes subestimada e sub analisada, inclusive em departamentos como a antropologia e mesmo as relações internacionais. De qualquer forma, verifica-se que a influência do complexo industrial-militar dos EUA no desenvolvimento do campo cibernético-computacional é irrefutável, e isso será importante para verificar-se como a NCW se estruturou, de forma teórica, e como adentrou no planejamento militar dos EUA.

Por fim, um aspecto importante abre-se aos olhos ao analisar-se a raiz do pensamento cibernético: a própria ideia de que o controle absoluto de sistemas complexos seria possível através da ciência. Longe de ser a pretensão do autor discutir os limites possíveis ao pensamento científico, é curioso observar como esse tipo de pensamento se estrutura em um Sistema Internacional pós-Guerra cuja ordem era a reconstrução dos países, a organização de regimes internacionais e o planejamento dos rumos econômicos do planeta (instituições de Bretton Woods, limitações ao capital financeiro e keynesianismo-militar). A cibernética, nesse caso, parecia dar às elites tecnocratas e políticas dos EUA uma certa gramática em relação a como esses desafios poderiam ser cumpridos, assegurando que ao fim mesmo os processos mais complexos, como as guerras, poderiam ser planificados e processados em computadores.

É da análise do autor que existe nessa relação algo de mais profundo, ligado à formação ideológica do projeto político global ensejado pelos EUA no Pós-Guerra, em que a ciência, a tecnologia e a “batalha pela mente dos homens” (conforme apresentado na carta fundadora da Organização das Nações Unidas para a Educação, a Ciência e a Cultura - Unesco) estariam conectadas.

3. O DESENVOLVIMENTO DA NETWORK-CENTRIC WARFARE NA DOUTRINA MILITAR AMERICANA.

Esse capítulo trata das raízes intelectuais específicas da Network-Centric Warfare, dado a apresentação preliminar do contexto científico fundacional dessas raízes encontrada no primeiro capítulo, além de analisar também como essa doutrina militar foi gradualmente incorporada ao Departamento de Defesa dos EUA. Além desses pontos, esse capítulo também analisa como a Superioridade Informacional, um termo encontrado em documentos de defesa dos EUA, se encaixa em uma perspectiva da criação de um estado de vigilância global buscado pelos EUA em meados do fim do século 20, e que se acelerou após as consequências políticas dos ataques de 11 de setembro de 2001.

Ao final desse capítulo, pretende-se que o leitor possa compreender como essa doutrina militar foi gestada, de forma específica, e como se organizou junto ao Estado americano e ao projeto de poder global dos EUA.

3.1. CLAUSEWITZ ENCONTRA AS CIÊNCIAS NÃO LINEARES: AS ORIGENS TEÓRICAS E CONCEITUAIS DA NCW.

> *From the enemy's character, from his institutions, the state of his affair: and his general situation, each side, using the laws of probability, forms an estimate of its opponent's likely course and acts accordingly.* (Clausewitz, 1832, p.80).

Teorizar acerca de Clausewitz, no Século 21, é uma tarefa complicada. Além de ser um autor inserido em um contexto intelectual bastante remoto, do ponto de vista contemporâneo, sua obra é tida como uma das fundadoras dos estudos estratégicos modernos, assim possuindo uma gama de interpretações e celeumas. Nesse caso, é raro encontrar alguma escola ou doutrina militar que não tenha influência direta ou indireta do estrategista prussiano, e isso será verificado em relação a NCW e seus autores, que buscaram enquadrar e atualizar, em alguma escala, o pensamento de Clausewitz no contexto da Revolução Informacional e das ciências não lineares.

Em primeira vista, argumenta-se que historicamente o desenvolvimento de determinadas ideias científicas e o desenvolvimento de determinadas tecnologias afetaram o pensamento humano em relação à guerra, o que se observa na influência da física newtoniana, da termodinâmica e da Revolução Industrial para a abordagem mecanicista dos séculos 18 e 19, e também no caso da cibernética e

dos primeiros computadores para o pensamento militar do Pós Segunda Guerra (BOUSQUET, 2008). Nesse caso, pode-se afirmar que a evolução das ciências não lineares (campo também chamado de “caos-complexidade”, em uma tradução bastante livre de “chaoplexic”), também influenciou o pensamento militar contemporâneo, sendo a NCW um exemplo direto dessa dinâmica.

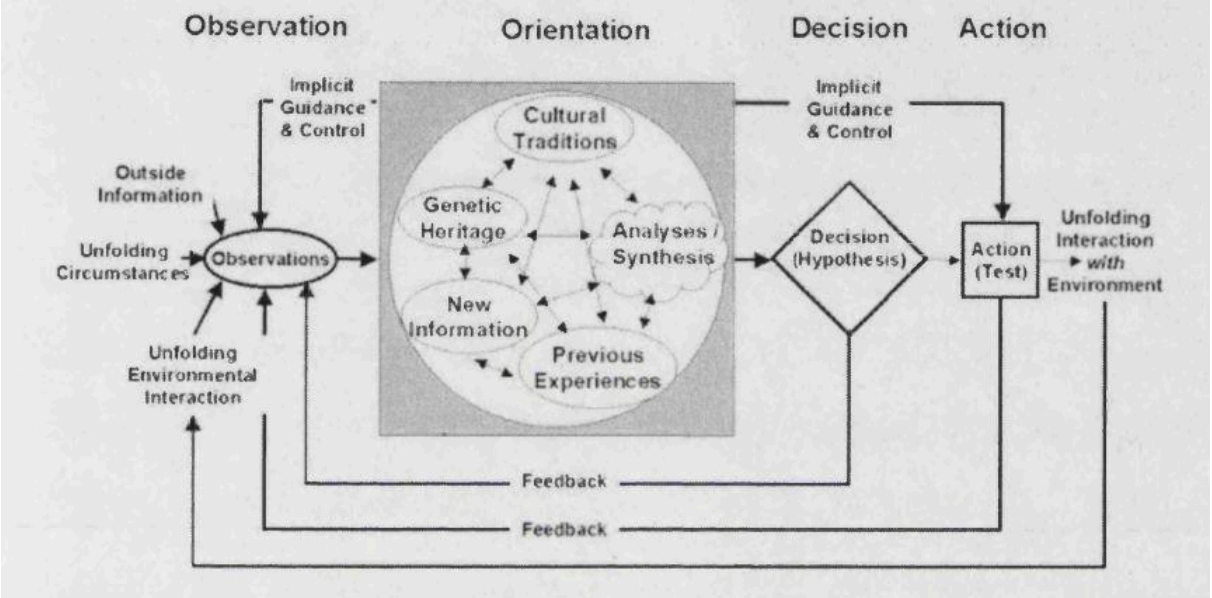
De forma bastante sintética, as ciências não-lineares podem ser definidas como o estudo de sistemas não-lineares, o que é bastante evidente, e que podem se constituir em basicamente qualquer área da ciência (BEYERCHEN, 1992). Sistemas não-lineares podem ser definidos como aqueles que desobedecem, em alguma escala, as leis da proporcionalidade ou da aditividade (ou seja, de que o todo é formado pela soma das partes) (BEYERCHEN, 1992). Sendo definidos por comportamentos muitas vezes imprevisíveis e erráticos, alguns exemplos de sistemas não-lineares são as explosões, o clima global, a evolução biológica e reações químicas (BEYERCHEN, 1992).

Nesse caso, sistemas não-lineares podem ser também descritos, por exemplo, como aqueles em que um pequeno *input* poderá gerar uma mudança desproporcional no *output* daquele sistema (contrariando assim a lei da proporcionalidade). Assim, a análise desse campo científico para o objetivo de estudo dos conflitos armados envolve a consideração de que a Guerra, enfim, pode-se constituir enquanto um sistema não-linear, e que isso poderia se conectar ao pensamento de Clausewitz, especialmente em relação ao pensamento deste relativo à imprevisibilidade e volatilidade dos conflitos (assim contrastando com a antiga noção da cibernética tradicional de que se todas as variáveis de um conflito fossem mapeadas, seria possível calcular exatamente seus resultados) (BEYERCHEN, 1992).

Dessa forma, observamos como os avanços do campo científico dos fenômenos não-lineares passou a desafiar a noção tradicional da cibernética de planejamento absoluto de conflitos. Isso também se observa no pensamento de John Boyd, piloto de caça e estrategista dos EUA, altamente influente no desenvolvimento da NCW, principalmente com a sua teoria de Ciclo OODA (Observe-Orient-Decide-Act) (BOUSQUET, 2008). De forma bastante sintética, esse ciclo resumiria o processo decisório de qualquer ator durante um conflito armado (e, na verdade, em qualquer aspecto da vida), no qual o ator absorve informações de seu ambiente, orienta essas informações de acordo com seu framework de análise

(influenciado por questões culturais, intelectuais etc.), toma uma decisão e por fim a executa (BOUSQUET, 2008). É fundamental observar que Boyd considera nesse processo loops de feedback entre esses diferentes estágios, conforme observado na figura abaixo, que sistematiza essa importante ideia.

Figura 1. Representação gráfica do Ciclo OODA, criado por John Boyd



Fonte: Bousquet (2008)

Ainda que não seja o foco desse trabalho avaliar a influência de Boyd para o Exército dos EUA e tampouco para a formação da NCW, suas ideias são fundamentais para se compreender a transição do pensamento cibernético tradicional (que durante anos imperou nas estratégias militares dos EUA, vide a exposição das dinâmicas computacionais da Guerra do Vietnã) para o pensamento não-linear. A contribuição de Boyd nesse caso é, ainda que com a absorção de diversos conceitos da cibernética (como os ciclos de feedback), a rejeição da consideração de que qualquer teoria ou doutrina pudesse verdadeiramente compreender de forma absoluta a Guerra, justamente pelo processo de constantes revisões, transformações e a verdadeira imprevisibilidade do comportamento humano, restando apenas tentativas de aproximações (BOUSQUET, 2008).

Outros autores influentes para essa transição são John Arquilla e David Ronfeldt, que escreveram e editaram artigos e livros influentes sobre temas como a Revolução Informacional e seus impactos para a Segurança Internacional e estratégias militares. Também de forma bastante sintética, o pensamento desses

autores pode ser descrita como um alargamento do papel que a Informação teria nas Relações Internacionais em comparação ao pensamento cibernético tradicional, o que pode ser observado na seguinte passagem:

> A guerra por muito tempo girava ao redor de quem podia transferir mais massa - como no chamado *levee en masse* da Era Napoleônica, ou as ondas humanas no fronte ocidental da Primeira Guerra Mundial e no fronte oriental durante a Segunda Guerra Mundial. Na Era Nuclear, a ênfase transferiu-se para a transferência de energia, como exemplificado nas ondas de choque e radiação soltas pela divisão dos átomos nas bombas. A vitória dependia não apenas de transferir massa ou energia aos fundamentos do oponente, mas também dependia da capacidade de evitar que seu oponente transferisse energia ou massa para você, e também em ser apto a absorver e recuperar-se dos ataques sofridos. Se a Informação pode ser interpretada como uma propriedade física, então na Era da Informação ganhar guerras torna-se dependente da capacidade de transferir informação ao inimigo e resguardar-se de retaliações (Arquilla; Ronfeldt; 1996.
> Tradução nossa).

Mais uma noção é fundamental para se compreender especificamente como a Network-Centric Warfare foi pensada, e é a própria teoria de Redes. A Rede, enquanto uma forma de organização social, pode ser descrita como um conjunto de indivíduos ou grupos pequenos interligados entre si de forma descentralizada, ao contrário de instituições tradicionais que privilegiam a hierarquia e a centralização (Arquilla; Ronfeldt, 1997).

Munidos desses conceitos, é possível compreender finalmente a gramática dos teóricos da NCW. Factualmente, o primeiro autor a escrever diretamente sobre essa doutrina foi o Vice-Almirante Arthur Cebrowski, em 1998, quando publicou seu influente artigo “Network-Centric Warfare - Its Origin and Future”. Nele, o autor desenvolve suas percepções acerca do impacto da tecnologia informacional na economia e na sociedade, sendo necessário que o aparato militar dos EUA também se adaptasse a esse novo mundo (CEBROWSKI, 1998). Como em um reflexo do espírito animal, ou o *zeitgeist,* da década de 90, em que intelectuais de inúmeros campos buscavam comparar seus avanços com termos econômicos (ou seja, um predomínio direto dos economistas na produção do pensamento), Cebrowski compara essa necessidade de adaptação operacional com um investimento econômico, que poderia trazer vantagens diretas aos EUA (CEBROWSKI, 1998).

Entre esses alardeados ganhos, o autor afirma que a NCW poderia incrementar a velocidade de comando e organização da cadeia militar, assim em direção a uma sincronização em tempo real dos acontecimentos e distribuição

imediata de novas ordens de comando (CEBROWSKI, 1998). Esse incremento na velocidade de combate se refletiria em uma maior superioridade informacional, maximização dos efeitos e minimização das forças empregadas e uma maior facilidade na previsão e disrupção das estratégias inimigas (CEBROWSKI, 1998).

Outro ponto de relevância de seu artigo é a constante referência ao arcabouço científico e intelectual analisado anteriormente, que inclui a análise de teorias de complexidade e do Ciclo OODA de John Boyd, demonstrando uma continuidade de pensamento entre esses diferentes autores e campos científicos.

Trazendo para seu estudo o arcabouço da teoria da complexidade, Cebrowski enxerga que operações militares (um fenômeno por definição bastante complexo) se organizaria melhor de forma “bottom-up”, ao contrário do militarismo tradicional organizado de forma “top-down” (CEBROWSKI, 1998). Em bom português, as forças armadas dos EUA seriam mais eficientes caso operadas de “baixo para cima” do que de “cima para baixo”. Através dessa nova organização das forças, que sincroniza a comunicação das unidades de forma descentralizada e contribui para o aceleramento do processo decisório e a difusão de informações, seria possível desequilibrar o Ciclo OODA do oponente, que teria sua pausa operacional negada, ou seja, com menos tempo para processar informações (CEBROWSKI, 1998).

De forma bastante evidente, percebe-se como a utilização do espaço informacional através de uma lógica de Redes é então percebida como uma fonte de vantagens competitivas no palco de batalha, em que o lado capaz de disseminar informação de forma mais eficiente (e também capaz de confundir o Ciclo OODA do oponente) deverá ser o vitorioso. De antemão, pode-se perceber como o pensamento de Cebrowski sobre conflitos armados está ligado a uma perspectiva que pode ser interpretada como determinística, que passa a considerar o fator tecnológico e operacional como basicamente o grande decisor do resultado desses processos, ao contrário de autores de outras tradições que privilegiam, por exemplo, o fator humano e psicológico dos conflitos.

Refletindo um *zeitgeist* em que a tecnologia parecia ser a solução para todo e qualquer problema social, fosse o desenvolvimento econômico, a sustentabilidade ou a guerra, a Network-Centric Warfare é então gestada a partir de uma perspectiva majoritariamente tecnocrática, em que a tecnologia da informação seria a solução para eliminar a névoa da guerra e criar um ambiente de controle e previsibilidade

(BOUSQUET, 2008). Nesse ponto, quaisquer descontroles ou resultados indesejados em batalhas seria apenas consequência da falta de tecnologia, ou da utilização adequada dela.

Conforme será abordado posteriormente, parte majoritária desses aspectos serão verificados nas estratégias e nos discursos empregados pelas lideranças dos EUA em relação aos conflitos no Iraque. Em especial, a ideia reproduzida em discursos sobre o aumento da eficiência da utilização das forças americanas no Iraque através da tecnologia, o que reduziria a necessidade de emprego de mais soldados, será especialmente relevante durante a Guerra do Iraque (e que faz referência direta às ideias verificadas no artigo de Cebrowski).

Muito se deve, evidentemente, ao fato de Cebrowski ter sido chefe do Office of Force Transformation (responsável por indicar e estudar possíveis transformações no aparato militar dos EUA), por indicação do Secretário de Defesa Donald Rumsfeld em outubro de 2001. Assim, verifica-se de imediato que as ideias de Cebrowski, e de outros teóricos que o acompanharam, tiveram não apenas impacto em meios acadêmicos dos EUA, mas também na própria reorganização do Departamento de Defesa do país, tema abordado no próximo subcapítulo.

Cabe destacar, no entanto, que apesar dos teóricos da NCW buscarem alicerçar definições claras em relação aos aspectos técnicos e operacionais da NCW, e sendo também um fato evidente que esses autores influenciaram decisivamente os processos decisórios do Departamento de Defesa dos EUA, não há uma definição única e consensual em relação a essa doutrina (Dahl, 2004). Ainda que seus fundamentos sejam relativamente bem estabelecidos, tendo como elementos principais a utilização extensiva de tecnologias da informação para melhor comunicação e operacionalização de forças ao redor de redes, é bastante comum que a definição dessa doutrina em documentos oficiais seja bastante vaga.

3.2. ABSORÇÃO E REORGANIZAÇÃO DO DEPARTAMENTO DE DEFESA DOS EUA FRENTE À NCW.

Já em seu artigo que define a NCW, Cebrowski elenca três aspectos necessários para o direcionamento das forças armadas dos EUA no sentido apresentado e defendido pelo autor. Demonstrava assim uma aptidão de seu pensamento de não apenas descrever e analisar o que seria da guerra e dos

conflitos armados em um contexto crescentemente informacional e tecnológico, mas há também um sentido direto de incrementar a posição relativa dos EUA nesse contexto.

Em primeiro lugar, ele descreve a necessidade de formação de um capital humano adequado para operações baseadas em informação e redes, sendo necessário a criação de uma nova elite intelectual capaz de compreender esses processos (CEBROWSKI, 1998). Em segundo, o autor elenca o capital financeiro, necessário para atualizar todo o conjunto de sistemas armados em direção aos objetivos elencados, o que demandaria um aumento do orçamento de defesa do país rumo a esse sentido (CEBROWSKI, 1998). Esse aspecto será fundamental, inclusive, para a compreensão das disputas políticas que posteriormente envolveriam o governo Bush em suas tentativas de aumentar o orçamento de defesa do país no sentido de reforma tecnológica das forças armadas do país. Em terceiro, seria necessário iniciar o quanto antes o processo transformador dessas forças, inclusive no sentido doutrinário (ou seja, aquilo que é ensinado aos novos membros das forças), sendo assim preciso coevoluir tecnologia, cultura e doutrina em um único sentido, para assim alterar decisivamente o caráter sistêmico dessas instituições (CEBROWSKI, 1998).

Pode-se interpretar o objetivo de incremento das forças armadas dos EUA descrita no pensamento de Cebrowski a partir da lente neorrealista, em que o autor identifica na tecnologia informacional e em novas formas organizacionais um potencial fator de incremento da posição relativa dos EUA em relação aos demais países e oponentes. E nessa perspectiva, há uma urgência verificada em relação ao perigo de que outros atores iniciassem essa transformação antes dos EUA.

Factualmente, um ponto de inflexão para uma maior absorção do conjunto de ideias da NCW no Departamento de Defesa dos EUA é a eleição de George W. Bush em 2000, haja vista que o presidente trouxe consigo, e com sua equipe no Departamento de Defesa, o discurso de transformação profunda das forças armadas (Mahnken, 2001). Outro nome importantíssimo nesse contexto histórico é o de Donald Rumsfeld, ex-Secretário de Defesa dos Estados Unidos, e que ativamente advogava pela necessária transformação do exército dos EUA no debate intelectual público dos EUA, inclusive através da escrita de artigos quanto ao tema (Czelusta, 2008). E foi através de Rumsfeld que Cebrowski é indicado para o Office of Force

Transformation em 2001, responsável por implementar a visão de Transformação Militar (*military transformation*) de Rumsfeld (Czelusta, 2008).

Ainda que o primeiro mandato de Bush seja fundamental para compreender as políticas de inserção da NCW, como será averiguado, é importante verificar que muitas das ideias de transformação militar já estavam presentes em documentos de defesa anteriores ao mandato de Bush, como o Joint Vision 2010, publicado em 1996 durante o governo Clinton (Czelusta, 2008). Já nesse documento, verifica-se uma orientação de adaptação, reorganização e transformação do aparato militar dos EUA perante os desafios da Revolução Informacional, devendo orientar as políticas de defesa dos EUA para os 15 anos seguintes (JCS, 1996).

Logo em seus primeiros discursos públicos enquanto presidente dos EUA, Bush afirmou que seria seu objetivo suplantar a ortodoxia do Departamento de Defesa do país e criar uma nova arquitetura de defesa para os EUA e seus aliados, descrevendo esse processo de modo a deixar as forças pesadas dos EUA mais leves e que essas armas leves se tornassem mais letais (NY Times, 2001). Em seus discursos, os intelectuais que formulavam a política de defesa de Bush descreviam o atual cenário de conflitos armados como cada vez mais dependentes de fatores informacionais, além de questões de mobilidade e velocidade de comando, descrevendo assim um objetivo de profunda reformulação do Pentágono (Czelusta, 2008).

Como qualquer reformulação profunda de qualquer instituição imaginável, esses objetivos não ocorriam sem resistências, dado a percepção de que Rumsfeld encontrava uma burocracia de difícil maleabilidade do Pentágono e uma estrutura de *lobby* corporativo e político resistente a alterações que pudessem alterar seus contratos de defesa, além de limites orçamentários impostos ao setor de defesa e que resistiam a aumentos súbitos de gastos (NY Times, 2001). Afinal de contas, em meados do ano 2000 e início de 2001, os EUA não estavam envolvidos em conflitos internacionais de proporções que justificassem os pedidos de aumento expressivo do orçamento de defesa defendidos pela administração Bush.

É claro que tudo se alterou no dia 11 de setembro de 2001. Com esse evento (e mais especificamente, com a forma pela qual o evento foi interpretado, securitizado e utilizado politicamente pela administração Bush), o objetivo de reformulação completa do complexo securitário dos EUA foi energizado, e ganhou ares de extrema urgência e celeridade (Dombrowski; Ross, 2008). O próprio

> combate à Al-Qaeda e a Guerra ao Terror ligaram-se intrinsecamente à reformulação do Pentágono, exposto como incapaz de proteger a população dos EUA perante as difusas e incertas ameaças do século 21 (Dombrowski; Ross, 2008).

Ainda que avaliar os impactos desse evento para a formação do orçamento de defesa dos EUA no século 21 não seja o objetivo desse trabalho, é importante salientar que a atualização das forças do país foi um dos pontos de maior acréscimo nesses gastos, principalmente no sentido de atualização de equipamentos e armamentos e investimentos massivos em pesquisa e desenvolvimento (Crawford, 2021). De certa forma, pode-se observar que o desenvolvimento tecnológico (e, mais especificamente, tecnologias ligadas à informação - leia-se: vigilância) foi visto de forma protagonista ao se combater os novos conflitos que se seguiram ao 11 de Setembro, principalmente em relação à invasão ao Afeganistão e ao Iraque.

Modifica-se assim o ritmo e o volume da advogada transformação militar, permitindo um elo fortificado da indústria de tecnologia dos EUA com essa transformação do Pentágono, alavancando companhias dedicadas a suprir a crescente demanda de novos e mais modernos equipamentos militares (Dombrowski; Ross, 2008). Argumenta-se que esse é o momento em que o conjunto de ideias ligadas à NCW se tornou mais preponderante no planejamento estratégico do Pentágono.

Nesse contexto, ainda que o Departamento de Defesa tenha publicado o documento Transformation Planning Guidance em 2003, que será analisado a seguir, sendo assim responsável por guiar os esforços conjuntos de transformação dos serviços armados do país, houveram também publicações e programas específicos de diferentes serviços para delinear essas transformações, demonstrando um certo deslocamento teórico entre diferentes planejamentos institucionais (Czelusta, 2008). A Marinha, por exemplo, discutia o conceito de “FORCENet”, o Exército discutia o “Battle Command”, as Forças Aéreas discutiam o “Air Operations Center as a weapons system”, enquanto o United States Joint Forces Command (USJFCOM) discutia o projeto de “Global Information Grid”.

Ainda que possuíssem certas divergências relativas a conceitos centrais, como a própria ideia de transformação, todos esses projetos-conceito envolviam diretamente uma defesa teórica da Network-Centric Warfare, verificando-se assim a abrangência desse campo teórico no aparato securitário dos EUA nesse contexto

histórico (Czelusta, 2008). Central para esse processo de discussões de reformulações profundas do Pentágono durante a administração Bush, e mais especificamente sob a liderança de Rumsfeld, é o documento Transformation Planning Guidance, publicado em 2003, e que discute aspectos como responsabilidades organizacionais específicas de diferentes instituições, objetivos a serem cumpridos e desafios a serem superados (Czelusta, 2008).

Já no prefácio do documento escrito por Rumsfeld em pessoa, verifica-se a defesa da necessidade da adaptação e modernização das forças armadas do país frente aos desafios globais expostos pelo 11 de setembro, defendendo também uma visão organizacional ligada ao conceito de centralidade de redes (JCS, 2003). Antes de se adentrar especificamente às modificações propostas pelo documento, pode-se verificar em seus preâmbulos a consideração de que os EUA estavam transicionando de uma Era Industrial para uma Era Informacional, e que a transformação militar rumo aos preceitos da NCW seria um imperativo estratégico para a manutenção da paz internacional, isto é, da hegemonia estadunidense do pós-Guerra Fria (JCS, 2003).

Mais interessante aos olhos internacionalistas que em relação aos aspectos burocráticos ligados ao Pentágono, é interessante verificar como os autores do documento expuseram suas defesas à necessidade de transformação militar em termos bastante neorrealistas. Entre os argumentos apresentados, há a ideia de que as dinâmicas do *status quo* mundial estaria diminuindo as vantagens militares dos EUA perante outros atores em termos relativos, ou seja, que outros países também estavam incrementando suas capacidades e aproximando-se dos EUA em termos relativos (JCS, 2003).

É presente também a ideia de que fatores tecnológicos e políticos estavam impelindo ameaças assimétricas, em que grupos difusos e menos concentrados passaram a acessar capacidades de ataque nunca antes acessados por esse tipo de grupo, aumentando a necessidade de melhores sistemas de vigilância e superioridade informacional (JCS, 2003). Além disso, a própria transição de uma sociedade industrial para uma sociedade informacional é enxergada como uma possível fonte de vantagens relativas para com outros países, dado também a descrição de uma percepção de capacidades únicas dos EUA para liderar essa transição a nível global em termos militares e tecnológicos (refletindo a incontestável unipolaridade de então) (JCS, 2003).

Em termos de visão organizacional, o documento também descreve quatro pilares de atuação nos quais todo esse processo estaria alicerçado. São eles: fortalecimento de operações conjuntas, aproveitar-se das vantagens de inteligência dos EUA, experimentação de novas formas de combate e desenvolvimento de capacidades de transformação (JCS, 2003). Através do fortalecimento desses pilares, é descrito que os EUA poderiam alcançar os seguintes objetivos:

1) Proteção de bases operacionais críticas;
2) Projetar e manter forças dos EUA em regiões distantes de anti-acesso ou ambientes de negação de área, superando assim ameaças de anti-acesso;
3) Negar santuários aos oponentes através de vigilância, monitoramento e engajamento rápido através de ataques precisos e de alto volume;
4) Garantir sistemas de informação frente a ataques e conduzir operações informacionais ofensivas efetivas;
5) Aumentar a capacidade e sobrevivência de sistemas espaciais e suas estruturas de suporte;
6) Impulsionar tecnologias informacionais e conceitos inovadores para desenvolver uma arquitetura de comando interoperacional (JCS, 2003).

Dessa forma, tem-se acesso à descrição dos principais meios e objetivos preteridos para a transformação das forças armadas dos EUA em direção a modelos orientados a redes, ou seja, diretamente alimentados teoricamente e intelectualmente pelos doutrinários da NCW. Antes de verificar quais os impactos desses preceitos para como os EUA conduziram sua invasão ao Iraque, o próximo subcapítulo tratará do nexo correlacional (não necessariamente causal) identificado entre o objetivo de desenvolvimento de uma superioridade informacional do Pentágono com o estado de vigilância global instaurado por esse departamento e as instituições de inteligência dos EUA, especialmente após o 11 de setembro.

Para tanto, mais um enfoque é brevemente necessário: o segundo pilar do Transformation Planning Guidance, que descreve o imperativo estratégico do Pentágono de explorar as vantagens de inteligência construídas pelos EUA. Através dessa estratégia, o documento descreve como o Pentágono seria capaz de identificar e prever ameaças através de *contínuo monitoramento* de possíveis

adversários através de um “global informational grid” que conectaria todos os sistemas informacionais dos EUA (JCS, 2003). Outro ponto de destaque é a consideração de que o Departamento de Defesa deveria cooperar de forma mais próxima com a comunidade de inteligência do país, incluindo novas prioridades de operações clandestinas (!), inteligência espacial, vigilância, reconhecimento e comunicações (JCS, 2003).

Como se verifica, há uma forte consideração de que o Pentágono deveria ocupar de forma cada vez mais ampla o espaço informacional global, aliado também à comunidade de inteligência dos EUA. Aos incautos, essa ligação aparentemente obscura e quase conspiratória pode parecer surpreendente. Aos leitores desse humilde trabalho que verificaram a história do espaço informacional a partir do complexo industrial-militar dos EUA, tudo há de parecer um tanto *business as usual,* talvez com uma nova roupagem.

3.3. SUPERIORIDADE INFORMACIONAL E VIGILÂNCIA GLOBAL.

Um dos eventos mais significativos para a política internacional do Século 21 foi o vazamento de milhares de documentos secretos da comunidade de inteligência dos EUA em 2013, através de Edward Snowden, um então funcionário da empresa de inteligência Booz Allen Hamilton, contratada pela National Security Agency (NSA). De acordo com Snowden, os documentos revelavam um projeto de vigilância global conduzido pelo Pentágono e agências de inteligência dos EUA em conluio com as de outros países (em especial, do Reino Unido, Canadá, Nova Zelândia e Austrália, membros da aliança Five Eyes), e que tinha como resultado a coleta ilegal de dados de bilhões de pessoas ao redor do mundo (WBUR, 2023).

Os vazamentos foram massivos e suas consequências, extremamente complexas. Diplomaticamente, os vazamentos causaram constrangimento especialmente entre os países deslocados das principais alianças de vigilância, notoriamente os casos da Alemanha (haja vista que a aliança Five Eyes foi criada no contexto da Segunda Guerra Mundial) e do próprio Brasil, que inclusive denunciou publicamente a NSA por espionagem industrial e política contra a Petrobrás e também contra a presidente Dilma Rousseff, além do Ministério de Minas e Energia do país (BBC, 2013) (O Globo, 2013). Verifica-se logo de antemão uma amplitude de alvos nacionais e internacionais desse sistema global de vigilância, teoricamente instaurado para o combate do terrorismo global.

Entre os documentos revelados por Snowden, chama-se a atenção para determinados programas, como o chamado PRISM conduzido pela NSA, responsável por coletar dados de diferentes *websites* (como o Google, Apple e Facebook) e da própria estrutura física da internet, descrevendo-se que a estrutura física construída pelos EUA nesse campo permitiria ao país receber parcela expressiva dos fluxos digitais globais (The Guardian, 2013). Interessante aos olhos latinoamericanos é o fato de que os slides vazados, que descrevem o programa, iniciado em 2007, indicam que quase 100% de todos os fluxos da internet latinoamericana passam diretamente pelos EUA, sendo assim passíveis de interceptação. A materialidade do espaço informacional é também um território em disputa, e que é ocupado através dos interesses dos Estados, como se percebe.

Outro programa que teve parte de seu escopo exposto pelos documentos vazados por Snowden é o X-Keyscore, também responsável por coletar e analisar dados em massa através de vigilância na internet. De acordo com Snowden e Glenn Greenwald, esse sistema permitiria analistas de baixo escalão investigar essencialmente qualquer pessoa ou instituição que estivesse conectada na internet sem qualquer tipo de autorização legal (ABC News, 2013).

De acordo com uma das apresentações vazadas, o programa contaria com mais de 150 instalações físicas ao redor do mundo (por vezes, a invasão ou interceptação de sistemas informacionais deve ser feita de forma próxima ao alvo), inclusive uma delas localizada em Brasília, além de ter disponível mais de 700 servers (The Guardian, 2013). Ainda, é descrito que o programa conta a alimentação de dados de outros programas de vigilância pouco estudados, como o Special Collection Service (seu codinome é F6), que se trata de uma agência de atuação em conjunto entre a CIA e a NSA para atividades de grande sensibilidade, demonstrando assim o caráter de interagência e interoperacionalidade desses programas (Ambinder, 2015).

Parte do sobressalto das revelações expostas por Snowden, e posteriormente por Julian Assange, veio do escopo e da abrangência desses programas, essencialmente globais em seus objetivos de vigilância, não se concentrando exclusivamente em regiões de conflitos nas quais os EUA e seus parceiros estratégicos atuavam. Argumenta-se, todavia, que a criação de um estado global de vigilância em massa, e de concentração de informação (enxergada, como averiguado, como uma fonte indelével de poder nas relações internacionais), não

era exatamente uma novidade teórica e mesmo material, dado a já exposta corrente teórica que passou a considerar o espaço informacional como, talvez, a maior fonte de vantagens relativas nas relações internacionais dos fins do século 20 e do século 21.

Nesse caso, argumenta-se que o estado de vigilância global, instaurado pelos EUA e seus asseclas principalmente após o 11 de setembro, tratou-se de uma prerrogativa estratégica do próprio Estado americano e seus interesses geopolíticos, militares e geoeconômicos, dispostos em alguns de seus documentos de defesa. Em geral, verifica-se um imperativo estratégico que pode ser componente explicativo nesse contexto: o de superioridade informacional.

No documento Joint Vision 2010, publicado em 1996 e que abarca os objetivos estratégicos do Departamento de Defesa ao horizonte de 2010 (ou seja, em um período temporal no qual posteriormente desenvolve-se a pretensa transformação militar de Bush e a difusão dos contratos de empresas de tecnologia e inteligência, no contexto em que se insere Snowden), define a superioridade informacional seria um fator decisivo para os resultados de conflitos no futuro (JCS, 1996). Ainda, o documento define a necessidade de condução de ações ofensivas e defensivas, utilizando-se desse espaço para o ganho de vantagens relativas (JCS, 1996).

Há, todavia, um componente implícito na noção de construção de vantagens informacionais (ou seja, de ter acesso a informações de qualidade que outros atores não detêm, e utilizar-se delas de forma estratégica), que é exatamente por meio de quais ferramentas e técnicas essas informações devem ser obtidas. E por cima de que direitos (como de privacidade) e estruturas sociais tradicionais, como a lógica de distinção entre campos sociais públicos e privados, essa construção de vantagens relacionais deve transpassar.

Levando-se em consideração o aspecto prioritário de questões securitárias no planejamento estatal dos EUA, o que se verifica na composição do orçamento do país, conforme verificado anteriormente, pode-se afirmar que a própria ampliação dos sistemas de coleta, processamento e distribuição de informações posicionam-se frontalmente na própria estratégia de estado do país.

Como de fato se verifica, no período do pós 11 de setembro um conjunto de leis e práticas políticas foram tomadas no sentido de ampliação da capacidade do estado americano de vigiar pessoas ao redor do mundo, principalmente em âmbito

internacional, mas também no sentido doméstico. A aprovação do Ato Patriótico foi o primeiro passo nesse sentido, sendo aprovado seis semanas após os ataques e com apenas três dias para que os congressistas pudessem avaliá-lo e debatê-lo, o que evidentemente não aconteceu, com o projeto assim aprovado em tempo recorde (Goitein, 2021).

Nele, se verifica a possibilidade do Estado de praticar a vigilância em massa, algo até então teoricamente impossível pela lei do país, que considerava a necessidade de mandatos individualizados para essas operações (Goitein, 2021). Dessa forma, permitia-se afinal a coleta essencialmente indiscriminada de dados de indivíduos ao redor do mundo (algo já bastante consolidado na política externa dos EUA anteriormente), e também de seus próprios cidadãos.

Pode-se interpretar essa rápida evolução da vigilância global a partir da visão de Roberto J. González, que descreve como a busca pela automação dos conflitos, a militarização da informação e a predição do futuro são aspectos fundamentais para a compreensão das políticas de tecnologia de segurança dos EUA, em especial no pós Segunda Guerra Mundial (González, 2022). Essa questão já foi verificada no primeiro capítulo desse trabalho, contando-se como ponto fundacional o surgimento da escola cibernética com Wiener.

O aspecto da militarização, ou, ainda, da securitização da informação é especialmente relevante para compreender-se a evolução tamanha da vigilância global. Ao inserir o acesso a informações em todo o mundo como um ponto fundamental para o combate ao terrorismo global, os EUA apostaram mais uma vez em uma visão tecnocentrada (como havia sido na Segunda Guerra Mundial e em sua condução da Guerra do Vietnã), isto é, que enxerga a tecnologia como uma solução aos problemas securitários enfrentados pelo país, que, conforme descrito anteriormente, são descritos como ameaças difusas e descentralizadas que devem ser vigiadas e assim previstas.

O discurso vigente era, nesse contexto do pós 11 de setembro, o de que tecnologia informacional trazia consigo um imperativo de diminuir incertezas e imprevisibilidades através de maior poder de simulação, uma ideia bastante semelhante aos primórdios das ciências cibernéticas, demonstrando uma manutenção de ideologias tecnocentradas no Departamento de Defesa do país (Derian, 2009).

Argumenta-se, todavia, que o espaço informacional internacional ocupado pelo complexo de segurança-inteligência dos EUA perpassa o mero nível de combate às suas ameaças securitárias, mas também escorre a outras esferas.

Não são poucas as denúncias e análises no Brasil, por exemplo, que buscam investigar a utilização dessas ferramentas e prerrogativas informacionais estadunidenses para a espionagem de empresas e ministérios críticos para a economia e a política país, como a Petrobrás e o Ministério de Minas e Energia, informações alegadamente coletadas pela NSA para monitoramento de possibilidades de crises financeiras internacionais (Opera Mundi, 2013). Não deixa de ser relevante nesse caso a tradicional ligação entre a comunidade de inteligência dos EUA com o setor financeiro (*Wall Street*) do país, inferindo-se assim uma possível troca de informações, obtidas pelo aparato de vigilância do país, entre esses setores (fundamentais para a grande estratégia dos EUA) (Bandeira, 2017).

Esse estado de coisas, em que a vigilância, processamento de informações e tecnologias matemáticas de simulação de cenários de conflitos virtuais passam a imperar de forma protagonista no planejamento militar de conflitos armados reais, pode ser descrito como de uma guerra virtual, na qual os espaços geográficos e temporais, além das tragédias e dramas humanos intrínsecos às guerras, tornam-se dissociados através da adição de mais uma camada de mistificação (tecnologia) (Derian, 2009).

Além desse cenário ameaçar a própria relação do ser humano com a guerra em direção à banalidade da prática meramente técnica e dissociada de contato com inimigos humanos reais, pode-se argumentar que a crença ideológica na onipotência da tecnologia para a resolução de conflitos leva os tomadores de decisão a superestimar suas capacidades ofensivas e a subestimar o poder de resistência de oponentes teoricamente incapazes de resistir (por não terem o mesmo acesso à tecnologia militar de ponta). Argumenta-se que esse aspecto explica, em partes, as decisões aparentemente insensatas dos tomadores de decisão dos EUA em suas invasões ao Vietnã (conforme verificado no primeiro capítulo desse trabalho), e posteriormente ao Afeganistão e ao Iraque.

Dessa forma, pode-se observar como o desenvolvimento do espaço informacional por parte da política externa dos EUA seguiu um objetivo notoriamente securitário, mas que também se interliga a outros campos intimamente conectados, como a estratégia econômica do país, na direção da pretendida superioridade

informacional. A obtenção e o processamento da maior quantidade e variedade possível de informações para o desenvolvimento das vantagens operacionais do aparato militar dos EUA, algo previsto na doutrina NCW, será também importantíssimo para a avaliação das estratégias de condução dos EUA em sua invasão ao Iraque, tema do próximo capítulo.

3.4. CONCLUSÕES PARCIAIS.

Nesse capítulo, pode-se observar de forma mais detalhada como os campos científicos da cibernética e dos estudos do caos e da complexidade, abordados no primeiro capítulo, se desenvolvem para a criação efetiva da NCW por Cebrowski, e como essa doutrina incorporou-se ao planejamento securitário dos EUA ao final do século 20. Em especial, esse conjunto de ideias traria consigo influências relevantes para o processo de transformação militar ensejado por Bush e Rumsfeld, que contou com a participação direta de Cebrowski, acelerado consideravelmente após os ataques de 11 de setembro e o aumento dos gastos de defesa dos EUA.

Também se aborda como o processo de reformulação do DOD se relaciona com a expansão do estado de vigilância global exposto pelos vazamentos de documentos secretos dos EUA por parte de Snowden e Assange, além de outros sujeitos. Nesse caso, argumenta-se que há uma relação correlacional (não causal) entre o objetivo de desenvolvimento da superioridade informacional do complexo securitário dos EUA (conceito estratégico encontrado nos documentos de defesa dos EUA desse período) com a expansão da vigilância global por parte desse país e seus parceiros. O espaço informacional não é neutro e é militarizado, efetivamente.

4. A INVASÃO AO IRAQUE E A NETWORK-CENTRIC WARFARE.

Neste capítulo, que finaliza o corpo geral deste trabalho e compõe assim o estudo de caso avaliado, busca-se avaliar de forma mais concreta como a Network-Centric Warfare influenciou de fato a condução da invasão dos EUA ao Iraque em meados de 2003. Além disso, buscará ser avaliado de forma mais ampla as dinâmicas relacionadas à aplicação de diferentes tecnologias militares nessa invasão, e como esse aspecto é fundamental para se compreender, por fim, as consequências da Guerra do Iraque e o futuro da NCW após esse conflito.

4.1. POR TODOS OS MEIOS NECESSÁRIOS: A APLICAÇÃO DA DOUTRINA NCW NA GUERRA DO IRAQUE.

Como verificado ao longo dos capítulos anteriores, o primeiro mandato de Bush foi marcado pela tentativa de reforma e modernização em diversas instâncias do aparato securitário e militar dos EUA, processo orientado ao redor do amálgama da transformação militar e profundamente influenciado pelo corpo teórico da Network-Centric Warfare.

Os eventos do dia 11 de setembro de 2001 e a posterior deflagração da Guerra do Terror, conduzida pelos EUA, aceleraram esse processo de transformação (frente à pressão governista pela expansão dos gastos no setor de defesa nesse sentido), ainda que essa transformação tenha sofrido pressões por uma imediata operacionalização no Afeganistão e no Iraque, o que pode ter alterado o seu sentido, direção e intensidade inicial.

Nesse caso, diante a ampla presença de intelectuais ligados a NCW no Pentágono (como o próprio Cebrowski), é evidente que a NCW estaria frontalmente inserida no planejamento intelectual e teórico do Pentágono em relação ao Iraque (ainda que essa inserção tenha contado com resistências, como será visto), sendo assim necessário verificar como essa doutrina influenciou de fato a condução do conflito.

Serão utilizados principalmente dois estudos para a verificação dessa problemática: o documento The U.S. Army in the Iraq War (dirigido por dois coroneis dos EUA e publicado pela editora do exército do país em 2019) e o estudo Network-

Centric Warfare Case Study (publicado pela U.S Army War College em 2005, e que estuda especificamente a influência da NCW para uma operação do exército americano no contexto da invasão ao Iraque).

Além desses documentos, que evidentemente possuem uma inclinação analítica pelo próprio fato de terem sido escritos por membros do próprio aparato securitário dos EUA, serão complementados pontualmente por outros estudos e reportagens. Destaca-se, entretanto, que em geral as principais fontes disponíveis para esses fenômenos estão ligadas ao corpo securitário do país (direta ou indiretamente).

Anteriormente à invasão dos EUA ao Iraque em 2003, esses dois países já possuíam uma complexa história conjunta de tensões e conflitos, como exemplificado no apoio americano dado ao Iraque na Guerra Irã-Iraque (1980-1988) e o posteriores ataques aéreos dos EUA ao Iraque no contexto da Primeira Guerra do Golfo (1990-1991). Inclusive, o suposto sucesso estrondoso desses ataques ao Iraque (Operação Desert Storm), que se deu quase que exclusivamente por meio de altas tecnologias militares, foi um dos casos preferidos dos defensores do processo de transformação militar (RMA) nos EUA, já que seus resultados positivos se deram a partir da tecnologia militar (USAWC, 2019).

O conjunto de ideias que circundam a RMA, acelerada por Rumsfeld e seus semelhantes, nunca foram aceitas de forma universal e inquestionável no exército dos EUA (USAWC, 2019). Ainda assim, esses ideais foram especialmente utilizados por representantes do Pentágono para explicar o sucesso inicial estrondoso da junta, que derrubou o regime de Saddam Hussein em pouco menos de 3 meses (USAWC, 2019).

Os primeiros meses da invasão ao Iraque, portanto, foram marcados por um grande otimismo em relação às possibilidades estratégicas concretas da tecnologia militar orientada à lógica de redes (NCW), que possibilitou uma rápida vitória sobre as forças convencionais iraquianas (USAWC, 2019). Todavia, o planejamento de inteligência da invasão foi desde o início incapaz de identificar a verdadeira força dos grupos armados irregulares que se fortaleceram logo nos primeiros dias da invasão, como os Fedayeen Saddam e outras milícias ligadas ao Partido Baath e a uma ampla rede de grupos armados transnacionais (USAWC, 2019).

Nesse caso, é destacado que os sistemas tecnológicos que deveriam fornecer às forças armadas um panorama *real-time* das operações acabaram

gerando imprecisões por enfocar demasiadamente nas forças convencionais do Iraque, coletando poucas informações sobre os grupos que se tornariam o verdadeiro desafio tático dos EUA na ocupação do território após a dissolução do já frágil estado iraquiano (USAWC, 2019). Além disso, a própria fragilidade do estado iraquiano, um oponente de fácil identificação e com poucas capacidades defensivas, pode ser um ponto de contestação dos discursos de sucesso imediato e da validação da transformação militar defendida por Rumsfeld (USAWC, 2019).

De fato, a aparente ingenuidade de Rumsfeld e outros defensores da RMA quanto a uma suposta vitória rápida no Iraque seria quebrada pelo desenrolar do conflito nos meses subsequentes. A insurgência dos grupos paramilitares não convencionais se demonstrou um desafio para o planejamento ofensivo dos EUA, que agora se via diante da necessidade de ocupar partes de um país essencialmente fragmentado.

A partir de dezembro de 2003, as resistências pontuais encontradas pelas forças americanas evoluíram para se tornar uma verdadeira guerra civil, alimentada por motivos diversos (como questões étnicas, religiosas, econômicas e relacionadas ao crime transnacional), e que ameaçou a própria existência de um estado iraquiano frente à fragmentação da sociedade local (USAWC, 2019). Entre 2004 e 2006, a coalizão da Operação Iraqi Freedom buscou estabelecer uma estratégia de transição, buscando alicerçar um novo governo iraquiano legítimo.

Entre as causas que ocasionaram no fracasso dessa tentativa de transição, são elencados o enfoque demasiado no combate ao grupos insurgentes e não ao próprio cenário de emergência de uma guerra civil no país (ou seja, o combate aos efeitos e não às causas), a crença em uma fácil reconstrução das forças armadas legítimas do Iraque (assim dificultando o uso legítimo da violência como parte fundadora desse novo estado), além de políticas de detenção polêmicas (vide o escândalo de Abu Ghraib) e a falta de efetivos de força necessários para a ocupação efetiva de territórios (USAWC, 2019).

A dificuldade de conter os avanços da guerra civil iraquiana, alimentada não apenas por tensões internas, mas também por influência de países vizinhos (como a Síria e o Irã), e também as dificuldades para se estruturar de fato um estado iraquiano soberano, levou a coalizão liderada pelos EUA a conduzir novas estratégias a partir de 2007 (USAWC, 2019). No final de 2006, Rumsfeld é substituído no Pentágono por Robert Gates, e o comandante das forças no Iraque,

George Casey, é substituído por David Petraeus, grande defensor de uma maior ênfase no chamado terreno humano dos conflitos.

Logo em 2007, é iniciado o chamado *surge*, um aumento abrupto das forças deslocadas ao Iraque, que deveriam então ser alocadas para interação efetiva com a população civil do Iraque, com o objetivo assim de diminuir o recrutamento de grupos insurgentes e aumentar o acesso a informações (USAWC, 2019). Ainda que de fato Petraeus apresentasse maior ceticismo em relação às abordagens tecnocentradas da NCW, defendendo estratégicas voltadas ao fator humano dos conflitos, o militar também defendia a reforma do exército americano em direção a sistemas orientados por redes, que seriam fundamentais em determinados contextos (Shachtman, 2007).

As estratégias de contrainsurgência computacional (ou seja, a aplicação da tradição intelectual e militar de parte da academia americana para se estudar como combater insurgências, um certo reflexo do combate aos movimentos anti-coloniais e de guerrilhas comunistas, mas utilizando-se de métodos computacionais), nesse contexto, ganharam relevância no planejamento de Petraeus, como pode ser verificado no desenvolvimento do Humain Terrain System (HTS) (González, 2008).

Essas estratégias iriam guiar, ainda que com contradições, o restante da ocupação dos EUA ao Iraque até sua retirada em meados de 2011. Porém, principalmente após a crise financeira de 2007/2008, as estratégias de contra insurgência de Petraeus foram vistas como demasiadamente custosas em um contexto de crise financeira, acelerando também o próprio processo de retirada das tropas americanas (USAWC, 2019).

Pode-se observar, nesse contexto, como as diferentes gerações da Guerra do Iraque contaram com diferentes abordagens em relação ao papel da tecnologia militar para a manutenção da ocupação ao Iraque. Para exemplificar esse processo de adoção da NCW no contexto do Iraque, expõe-se a seguir os principais resultados encontrados no estudo “Network Centric Warfare Case Study”, que estuda as Network Centric Operations (NCO) a partir da atuação do US V Corps e a 3rd Infantry Division.

Os autores do estudo descrevem que as operações ofensivas do US V Corps e a 3rd Infantry Division foram únicas por conta da utilização de sensores táticos (LRAS3 e o Hunter UAV), pela extensão da conectividade (sistemas de satélite), e sistemas de informação orientados por redes (Cammons et al., 2013). A

combinação desses sistemas orientados a uma lógica de redes e conectado com o poderio bélico tradicional dos EUA permitiu que esses grupos obtivessem uma maior letalidade e precisão, assim confluindo em direção às próprias teorias da NCW (Cammons et al., 2013).

Dentre os resultados encontrados pelo estudo acerca da utilização conjunta dos sistemas informacionais, está o incremento da capacidade de compartilhamento de informações em tempo real e também o incremento de eficiência e sincronia nos níveis de decisão, planejamento e ação (Cammons et al., 2013). Em suma, argumenta-se que a utilização massiva de sistemas informacionais orientados em redes teria permitido aos corpos ofensivos dos EUA incrementar sua eficiência nos primeiros meses de ataque e ocupação ao Iraque.

Dessa forma, pode ser observado como a NCW esteve frontalmente inserida no planejamento militar dos EUA em sua condução à invasão ao Iraque, especialmente em relação ao que se pode chamar de primeira fase do conflito. Nessa fase, marcada predominantemente pelo objetivo de retirar Saddam Hussein e sua base de apoio do estado iraquiano, o rápido sucesso das forças invasoras foi justificado a partir da superioridade tecnológica, informacional e operacional das forças guiadas pelos EUA, conforme verificado nas declarações de Rumsfeld.

Mais especificamente, a primeira fase do conflito foi marcada pelo uso de tecnologias voltadas ao componente cinético dos conflitos, isto é, alinhado à lógica de destruição das principais infraestruturas críticas dos resistentes. A segunda fase da guerra (marcada pelo comando de Petraeus) foi também fortemente baseada em estratégias tecno-centradas, porém em um sentido consideravelmente distinto.

Seria assim um erro analítico considerar que apenas a primeira fase da guerra foi marcada pela influência da NCW, sendo todavia verdadeiro que essa doutrina esteve em maior consideração nesse período. E as dinâmicas relativas à relevância da tecnologia militar na Guerra do Iraque serão justamente o tema do próximo subcapítulo.

4.2. ENTRE O SHOCK AND AWE E O HUMAN TERRAIN SYSTEM: A TECNOLOGIA MILITAR E SEU PAPEL NA INVASÃO E OCUPAÇÃO DO IRAQUE.

Nesse subcapítulo, se pretende apresentar o papel desempenhado pela

tecnologia militar na invasão e ocupação americana do Iraque. Dado o aspecto amplo desse objetivo, foram escolhidos dois contextos para se verificar as diferentes formas pelas quais a tecnologia militar influenciou esse conflito (nesse caso, enfocando-se em aspectos relativos à NCW), sendo escolhidos assim a estratégia Shock and Awe e o Human Terrain System. Esses exemplos foram escolhidos em função de suas diferentes orientações gerais, aplicadas também em diferentes momentos do conflito.

Como visto, os primeiros meses da Guerra do Iraque foram avassaladores e altamente destrutivos para o território iraquiano. A condução desses primeiros ataques se deu a partir da estratégia do Shock and Awe (algo como Choque e Pavor, em português), criado inicialmente por Harlan K. Ullman e que se baseia na criação de um ataque tão repentino e massivo que atordoaria e paralisaria o oponente (Correll, 2003). A ideia principal dessa doutrina seria de atingir uma dominância rápida e até imediata, controlando assim o que o adversário percebe, entende e sabe, desorientando o sistema informacional do oponente e fazendo com que suas resistências sejam destruídas (Correll, 2003).

Os massivos ataques aéreos às principais cidades do Iraque ocorreram nos primeiros dias de março de 2003, inicialmente em Bagdá e então em cidades como Mosul e Basra. No começo de abril, a maior parte do território iraquiano já se encontrava sem qualquer tipo de governo efetivo, entrando essencialmente em um estado anárquico (USAWC, 2019). Nesse caso, o intento de Rumsfeld e seu comando para esses ataques era de entrar de forma rápida e leve no Iraque, possibilitando também uma rápida saída do país, alcançando os objetivos estratégicos dos EUA com o menor custo associado possível (USAWC, 2019).

Esse pensamento é reflexo direto da inserção do pensamento dos autores Harlan K. Ullman e James P. Wade no Pentágono, que defendiam o conceito de dominância rápida, em que um grupo pequeno de soldados seria capaz de dominar um inimigo mais forte e numeroso através de uma rápida demonstração de força, desde que essa ação fosse carregada de alto valor estratégico/tático, tecnologia e inovação (Ullman; Wade, 1996). Poucos meses antes da invasão de fato, Rumsfeld chegara a se desentender seriamente com o Comando Central dos EUA (CENTCOM) em função do número estimado de soldados necessários para a invasão e retirada de Hussein do poder, defendendo assim que pouquíssimas forças seriam necessárias, uma proposta considerada demasiadamente radical e insensata por decisores do CENTCOM (USAWC, 2019).

De acordo com a organização sem fins lucrativos Iraq Body Count, mais de 24.000 civis iraquianos morreram nos primeiros dois anos do conflito (anos iniciais da invasão), sendo que metade dessas mortes se concentrou em Bagdá, a primeira cidade de grande tamanho a ser bombardeada, logo sucumbindo ao caos (IBC, 2024). Nesse caso, é exposto que apesar das primeiras semanas da invasão terem sido inegavelmente favoráveis às forças americanas, que logo desarticularam a resistência armada oficial do governo iraquiano, o objetivo teórico central do Shock and Awe acabou não ocorrendo conforme os especialistas em guerra psicológica da junta planejaram, especialmente quando considerado o médio prazo (USAWC, 2019).

É oportuno salientar, nesse caso, que pouco da doutrina Shock and Awe se orientava à ocupação efetiva de um território, sendo assim dedicada essencialmente ao processo de destruição e dominação rápida. De certa forma, se pode dizer que os pensadores e praticantes da transformação militar encabeçada por Rumsfeld se viram sem qualquer planejamento para o que de fato fazer com todo aquele país e suas inúmeras questões a serem resolvidas. E é muito difícil imaginar que qualquer país que tivesse sua estratégia de invasão intitulada Choque e Pavor fosse recebida como um salvador pela população civil local, conforme previra lamentavelmente o então vice-presidente Dick Cheney.

Assim como a vitória das semanas iniciais foi rápida, logo se tornou veloz a consciência dos desafios a serem enfrentados pelos EUA caso desejassem de fato construir seus objetivos no país, desafios que talvez as teorias de velocidade e dominância do Shock and Awe e dos teóricos da revolução militar não abarcavam em seus arsenais (Derian, 2009). Munidas inicialmente de uma prerrogativa de necessidade e não de opção política (frente à suposta ameaça das armas de destruição em massa iraquianas), o que se expressava em um quase messiânico estado de crença em uma superioridade moral americana, as lideranças dos EUA pareciam encantadas pelo seu próprio sucesso, o que se refletiu em garantias de vitórias rápidas por Rumsfeld, Wolfowitz, Cheney e Tenet (Derian, 2009).

Os insucessos e escândalos da operação logo se refletiram em queda de popularidade da junta por parte da população civil americana, além de boa parte da opinião pública internacional, refletindo-se assim em maiores demandas desses setores por abordagens menos letais na invasão (González, 2008). Em pouco tempo, as ideias e termos da Revolution in Military Affairs (RMA), Network-Centric

Warfare (NCW) e da rápida vitória no Iraque foram substituídos em termos discursivos e militares por Counterinsurgency (COIN) e operações de estabilização (Derian, 2009). E é nesse contexto de transição que está inserido o Human-Terrain System (HTS).

Entre 2005 e 2006, o exército americano estabeleceu um programa de contrainsurgência experimental chamado de Human Terrain System, que consistia na utilização de pequenos grupos de especialistas em cultura local (no caso, a iraquiana) e outros cientistas sociais para entrar em contato com a população civil local e mapear assim o terreno humano do conflito (González, 2008). Historicamente, o conceito de terreno humano esteve inserido no exército americano em um sentido operacional, já que o conhecimento da cultura do país inimigo seria um importante componente para a previsão do comportamento de sua população em um conflito (Kipp, 2006).

Representado pela mídia ocidental e pelo próprio exército americano enquanto uma tentativa de reconexão com a população civil iraquiana, e como uma tentativa de minimização de baixas através da redução de componentes diretamente cinéticos do conflito, pode-se argumentar que o HTS foi estabelecido como um programa de espionagem e acumulação de informações (González, 2008). Nesse caso, o HTS pode ser comparado com o programa de contrainsurgência computacional CORDS, utilizado na Guerra do Vietnã (exposto no primeiro capítulo desse trabalho), que também se baseava no pressuposto de ganhar os corações e mentes da população ocupada (Cox, 2011).

A comparação também pode ser realizada com o componente clandestino da operação oficial. No caso do conflito no Vietnã, o programa CORDS esteve ligado ao Programa Phoenix (ilegal), que se utilizava das informações coletadas e processadas pelo CORDS para assassinar dissidentes políticos e guerrilheiros dentre a população civil vietnamita (Cox, 2011). No caso do Iraque, é ressaltado que as informações coletadas pelas equipes de campo, como entrevistas, relatórios e bancos de dados, seriam facilmente acessadas pela CIA e por futuros governantes oficiais do Iraque (González, 2008). Essa conexão seria realizada através de um software chamado Mapping Human Terrain, que concentraria as informações e disponibilizaria todas essas informações culturais e antropológicas para os analistas interessados, criando assim teoricamente um panorama cultural abrangente do terreno humano iraquiano (González, 2008).

Novamente, verifica-se a percepção de que a coleta e processamento massivo de informações seria um caminho estratégico para a vitória da ocupação, nesse caso através da coleta e processamento de informações culturais e antropológicas. São verificados estudos de acadêmicos ligados ao exército americano que se dedicavam a simular computacionalmente, por exemplo, como diferentes indivíduos reagiriam a patrulhas armadas ou a uma oferta de chocolates por parte dos militares americanos, buscando assim simular o comportamento humano a partir de um conjunto de centenas de variáveis explicativas (González, 2008).

Esse tipo de modelamento do comportamento humano em situações de conflito a partir de imensos conjuntos de dados e modelos matemáticos complexos resultou, em 2008, na criação do programa de pesquisa Human Social Culture Behavior Modeling por parte do Pentágono, com o objetivo oficial de compreender o comportamento humano em situações de conflito e auxiliar as forças americanas em guerras irregulares e não convencionais (HSCB, 2008).

No caso do HTS, a comparação do aspecto clandestino do programa para com o Projeto Phoenix se dá de forma mais contextual, haja vista que os dados do HTS poderiam ser facilmente inseridos em modelos computacionais do Pentágono e da CIA dedicados a identificação de resistentes e terroristas, o que se confirmou em afirmações encontradas em apresentações secretas vazadas do Pentágono (González, 2009).

Dessa forma, pode-se observar através dos exemplos do Shock and Awe e do Human Terrain System como a tecnologia militar desempenhou um papel fundamental na invasão e ocupação do Iraque por parte da junta liderada pelos EUA. É fundamental notar, nesse caso, que essa utilização não se deu de forma unidirecional, como se nota nas diferentes interpretações e visões estratégicas relacionadas a esses dois programas/doutrinas.

No caso do Shock and Awe, a tecnologia militar superior se configura enquanto um elemento de surpresa e criação de vantagens cinéticas capazes de subjugar o oponente em poucos dias. No caso do HTS, a tecnologia seria um elemento de melhor relação dos invasores para com a população civil (ao menos em sua face oficial), sendo assim uma quase negação teórica da Shock and Awe, que privilegia a rápida subjugação (e não uma ocupação efetiva de um território).

Pode-se afirmar, portanto, que as diferentes fases da Guerra do Iraque contaram com diferentes visões relacionadas ao papel a ser desempenho pela tecnologia militar. A NCW, de forma mais específica, obteve sua consagração teórica e política nos primeiros meses e anos da guerra, mas o termo deixou de ser *sexy* a partir da transição das lideranças militares a partir de Petraeus.

Portanto, a Guerra do Iraque foi pensada, planejada e executada a partir de diferentes visões (oras realistas e sensatas, oras não) do potencial revolucionário da tecnologia informacional e computacional para os conflitos armados. Na verdade, torna-se impossível analisar taticamente e estrategicamente essa invasão sem considerar esses aspectos tecnológicos, informacionais e computacionais.

4.3. A GUERRA DO IRAQUE, SUAS CONSEQUÊNCIAS E O FUTURO DA NETWORK-CENTRIC WARFARE.

Nesse subcapítulo, que encerra o corpo principal desse trabalho, pretende-se avaliar de forma geral as principais consequências da Guerra do Iraque, enfocando-se em questões operacionais, estratégicas e táticas do Departamento de Defesa dos EUA relativas a Network-Centric Warfare. Dessa forma, é do objetivo específico desta seção avaliar de que forma a NCW foi afetada pelos resultados da Guerra do Iraque, e como essa doutrina passou a ser encarada subsequentemente. Adianta-se, de antemão, que há na literatura especializada uma certa lacuna de trabalhos que examinem de forma específica como a NCW foi transformada pelos conflitos no Iraque e Afeganistão.

Em primeiro lugar, os acontecimentos da Guerra do Iraque impingiram sérias dúvidas em relação aos principais pressupostos da NCW, especialmente contra a ideia de que os conflitos poderiam ser modelados e completamente compreendidos através da tecnologia (Oh, 2009). Como foi averiguado nos capítulos anteriores, a NCW e suas ramificações e doutrinas semelhantes (como a Shock and Awe) se demonstraram incapazes de abarcar a complexidade dos conflitos no Iraque, especialmente em um horizonte mais prolongado. Nesse contexto, a disseminação da tecnologia da informação para outros atores é também um ponto relevante.

Um ponto subestimado pelos intelectuais e autores da NCW é o que aconteceria em um contexto de perda da vantagem tecnológica relativa dos EUA em relação a seus oponentes, dado que em algum momento inevitavelmente há de

ocorrer o chamado *spillover* tecnológico, em que as tecnologias civis e militares passam a ser mais acessíveis aos agentes interessados (Oh, 2009). A internet, por exemplo, possibilitou a diversos grupos insurgentes obter e transmitir informações em ampla escala acerca dos ataques americanos, configurando assim uma estratégia de cunho semelhante aos próprios intentos da NCW (Oh, 2009).

Ressalta-se que há pouquíssimo na teoria de Cebrowski acerca de como utilizar suas táticas contra um oponente que também tivesse acesso a sistemas de comunicação em tempo real, concentrando-se assim quase que exclusivamente em confrontos absolutamente assimétricos em termos tecnológicos. De certa forma, pode-se afirmar que os autores da NCW e seus praticantes no Pentágono subestimaram o potencial impacto da disseminação tecnológica em contextos de guerras assimétricas. Em bom português, a disseminação de tecnologias como a internet foi uma faca de dois gumes, complexificando o palco operacional da NCW e compondo um forte desafio a essa estratégia.

Desde o surgimento da cibernética nos anos 40, a tecnologia informacional e computacional foi em geral vista como uma maneira de simplificar, modelar e prever determinados aspectos de conflitos armados. Fosse através das miras automáticas de Wiener ou das simulações antropológicas do Human Terrain System, a tecnologia computacional desenvolveu-se justamente a partir dessa lógica, a da resolução de conflitos armados. No caso do Iraque, viu-se justamente o contrário: a disseminação ainda que desigual da tecnologia informacional entre os players complexificou a guerra, ao invés de simplificá-la.

Do ponto de vista teórico, relembra-se o pressuposto utilizado nesse trabalho de que os Estados-Nacionais e suas agências buscam desenvolver vantagens relativas aos seus rivais. No caso da tecnologia informacional, há uma relação certamente paradoxal em jogo, já que ao mesmo tempo em que o Pentágono dedicou-se ativamente a buscar vantagens relativas através dessas tecnologias, também através destas criou outros desafios e vulnerabilidades a serem exploradas por seus rivais. Ao dispor de uma estratégia de combate inteiramente interconectada em tempo real, conforme previa a NCW, o esforço de guerra americano tornaria-se mais vulnerável a ataques cibernéticos, por exemplo.

Em partes, esse é um dos pontos de destaque para se compreender o essencial fracasso da NCW no Iraque, podendo ser resumido como a subestimação da capacidade das forças resistentes iraquianas de se adaptar a essa guerra

tecnológica e utilizar desse novo cenário a seu favor. Ao enfocar demasiadamente no desenvolvimento de capacidades de simulação e processamento computacional, o planejamento tático dos EUA esqueceu-se de considerar que o fator humano de seus rivais continuaria a inovar e desenvolver novas técnicas de resistência (Oh, 2009).

Outro ponto de impacto da Guerra do Iraque para a NCW foi, enfim, a prova de que essa doutrina não seria infalível ou aplicável a absolutamente todos os conflitos. Em 1999, ou seja, antes da Guerra do Iraque, autores já chamavam a atenção para esse aspecto da NCW, marcada por uma confiança irrestrita em seu pressuposto de superioridade informacional (Barnett, 1999). Uma das marcas indeléveis dessa doutrina, desde sua formação, seria uma confiança excessiva na possibilidade de redução do volume das forças humanas em conflitos através da superioridade informacional, algo que também se verificou nas declarações de Rumsfeld acerca das poucas tropas necessárias para uma invasão ao Iraque (Poduval, 2009).

Em termos organizacionais, o conjunto de ideias relacionadas a NCW e a Revolution in Military Affairs (RMA) passaram por fortes contestações institucionais, especialmente pelas rivalidades entre as forças terrestres e as aéreas dos EUA em função de disputas sobre a melhor maneira de conduzir a ocupação do Iraque (Correll, 2019). De fato, como verificado anteriormente, houve em meados de 2007-2008 uma transição de lideranças no Pentágono que levou Robert M. Gates à posição de Secretário de Defesa, trazendo consigo uma maior estima a valores tradicionais das forças armadas americanas (como um maior volume alocado de tropas terrestres) (Correll, 2019).

Portanto, o declínio relativo da RMA no planejamento estratégico dos EUA a partir desse contexto pode ser explicado não apenas como uma consequência direta das complicações encontradas pelo país em suas invasões ao Oriente Médio, mas também como um resultado de disputas institucionais internas entre as forças armadas terrestres e a força aérea do país (Correll, 2019). Nos anos subsequentes à exposição das evidentes falhas operacionais das estratégias tradicionais de contrainsurgência de Petraeus, surgiu ao seio da comunidade de defesa dos EUA uma espécie de fusão entre a RMA e o conjunto de ideias mais tradicionais das forças do país (González, 2022). Essa fusão foi chamada por González de contrainsurgência computacional, em que cientistas sociais, como antropólogos e

internacionalistas, cooperam com cientistas de dados e matemáticos para a criação de técnicas de contrainsurgência intensivamente baseadas em dados coletados em massa (González, 2022).

Dessa forma, pode-se afirmar que o processo da RMA capitaneado por Rumsfeld nunca foi plenamente realizado, tendo sido interrompido por mudanças institucionais e políticas. Ainda assim, o processo de modernização generalizada dos sistemas armados dos EUA nessa direção, ou pelo menos a tentativa de fazê-lo, parece ter sido um resultado inegável desse movimento. Como resultado, parece ser impossível encontrar algum campo específico da comunidade de defesa e mesmo de inteligência dos EUA que não se encontre direta ou indiretamente influenciado por um certo tecno-centrismo, característico da RMA e de forma mais específica da NCW. De forma geral, o termo de contrainsurgência computacional de González parece adequado para explicar o estado de hibridismo que tomou o planejamento dos EUA em sua condução de conflitos, especialmente os mais assimétricos, dado a interação profunda entre a tradicional escola da contrainsurgência ocidental e a evolução da tecnologia informacional e computacional.

Para finalizar esse subcapítulo, considera-se pertinente expor um exemplo específico de um programa que pode ser enquadrado enquanto uma das primeiras tentativas de aplicar esse conceito no Afeganistão. Criado pelo Defense Advanced Research Projects Agency (DARPA), o programa secreto Nexus7 tinha a pretensão de criar um sistema de vigilância que conectasse dados de inúmeras fontes, desde imagens de radares espiões ao preço de frutas para assim medir o coeficiente de estabilidade do Afeganistão (González, 2022). Baseado em um antigo projeto da própria DARPA chamado Real Time Regional Gateway (RTRG), que tinha o objetivo de acumular e analisar o máximo de dados de cidadãos iraquianos obtidos através dos sistemas de vigilância e espionagem dos EUA, o Nexus7 surgiu a partir do momento de transformação desse antigo sistema para também contar com a inserção de dados socioculturais em meados de 2010 (González, 2022). O Nexus7 teria o objetivo de prever ataques terroristas e verificar, por exemplo, se determinada população de um vilarejo seria favorável ao Talibã ou ao governo de Kabul (González, 2022).

Para ressaltar o papel desempenhado por cientistas sociais nesse contexto, verifica-se que um dos grandes defensores desse programa foi David Kilcullen, doutor em estudos antropológicos aplicados à contrainsurgência, e que defendia a

inserção de métricas e metodologias quantitativas para medir a eficácia das estratégias de contrainsurgência americanas no Afeganistão (González, 2022).

Essa breve exposição do Nexus7 é capaz de demonstrar como a contrainsurgência computacional se desenvolveu em termos teóricos e institucionais, unindo assim pressupostos militares tradicionais com o avanço tecnológicos informacionais e computacionais. Fosse este um trabalho mais extenso e específico, poder-se-ia analisar de que forma esse novo pressuposto moldou as estratégias institucionais, políticas e econômicas dos EUA nesses últimos 10 anos, a exemplo da crescente conexão do Pentágono com big techs e o possível papel a ser desempenhado pela inteligência artificial nesse contexto. Mas esses são temas para outros trabalhos, possivelmente de outros pesquisadores.

4.4. CONCLUSÕES PARCIAIS

Nesse capítulo, pode-se verificar de fato como a NCW moldou efetivamente o comportamento e as táticas das forças americanas em sua invasão ao Iraque a partir de 2003, e também como essa doutrina pode ter sido afetada pelos resultados no mínimo controversos desse conflito.

O primeiro subcapítulo busca verificar de forma específica como diferentes tropas e forças dos EUA aplicaram a NCW em suas táticas, além de se verificar uma breve análise mais geral das diferentes fases do conflito.

O segundo subcapítulo explica como a aplicação da tecnologia informacional e computacional nesse conflito não deve ser entendida, entretanto, como um processo unidirecional, evidenciando-se as diferenças fundamentais entre os diferentes momentos do conflito através do Shock and Awe e o Human Terrain System.

O terceiro subcapítulo demonstra os principais questionamentos e resistências desenvolvidas à NCW e a RMA no espaço securitário americano, buscando-se desenvolver brevemente acerca do processo de formação da chamada contrainsurgência computacional aplicada no Afeganistão, entendida como a doutrina que fundiu definitivamente a tradição da contrainsurgência ocidental com os avanços informacionais e computacionais do século 21.

Como conclusão parcial desse capítulo, afirma-se que a Guerra do Iraque resultou em aprendizados ambíguos para as forças armadas americanas e mesmo

para estudiosos de defesa e segurança ao redor do mundo. Os primeiros anos da invasão demonstraram a evidente diferença de capacidades materiais dos EUA para com seus inimigos, que contaram com uma rápida vitória que desestruturou completamente o estado iraquiano e suas forças regulares. Por outro lado, o estado de tecnocentrismo dessas forças foi incapaz de resolver o caos ao qual o Iraque foi jogado, demonstrando também limitações às abordagens *high-tech*.

Em muitos materiais e estudos, autores principalmente de origem nos EUA perguntam se o país teria aprendido sua lição no Iraque e no Afeganistão, isto é, que a tecnologia pode não ser uma solução perfeita para todos os problemas do mundo (especialmente quando se fala de guerra). Esse não parece ser o caso. Há cerca de
60 anos, quando os EUA invadiram o Vietnã, erros muito semelhantes foram cometidos. A presunção e o orgulho, a ignorância acerca do próprio inimigo e uma crença cega na superioridade material e até espiritual de suas forças ocasionaram em duas das piores derrotas militares da história dos EUA. Em ambos os casos, o Vietnã e o Iraque trouxeram profundas transformações na ordem política e econômica global que abalaram a posição relativa dos EUA no sistema internacional. Resta se perguntar se novamente essas lições serão esquecidas.

5. CONCLUSÃO

Este trabalho abordou a histórica intelectual, científica e teórica da Network-Centric Warfare e a aplicação dessa doutrina na Guerra do Iraque, tendo como início do período de análise a Segunda Guerra Mundial e o esforço de desenvolvimento tecnológico dos EUA nesse contexto. Nesse caso, a hipótese principal que guiou o desenvolvimento deste trabalho faz referência ao possível nexo causal da NCW com as estratégias de condução da invasão da junta liderada pelos EUA ao Iraque. Ou seja, buscou-se avaliar se de fato essa doutrina influenciou de forma decisiva a condução dessa invasão.

Como hipótese secundária, buscou-se verificar de que maneira o preceito de superioridade informacional desenvolvido ao seio da NCW se relaciona com o estado de vigilância global estabelecido por instituições da comunidade de inteligência dos EUA. Nesse caso, foi de interesse do autor estabelecer conexões entre o objetivo de desenvolvimento de vantagens relativas dos EUA através do

espaço cibernético e a expansão desse espaço em nível global. Em nível teórico, afirma-se que o neorrealismo é suficiente para explicar parcela expressiva dos principais comportamentos e objetivos perseguidos pelo Departamento de Defesa dos EUA no contexto analisado. A perseguição de vantagens relativas é central no corpo teórico da NCW, que se baseia na utilização da tecnologia e da superioridade informacional para a dominação rápida e eficiente dos inimigos.

Outro achado relevante desse trabalho é a consolidação de um histórico relativamente abrangente do que se pode chamar de tecno-centrismo nas forças armadas dos EUA, isto é, a crença intelectual quase mecanicista de que a tecnologia militar pode resolver todo e qualquer problema enfrentado por essas forças no palco de batalha. Partindo-se da consolidação do complexo industrial-militar e da cibernética no imediato pós Segunda Guerra, passando pela Guerra do Vietnã e pela revolução informacional das décadas de 80 e 90, pode-se verificar como o espaço informacional-computacional cresceu enormemente no planejamento estratégico/militar dos EUA. Argumenta-se que desse processo culminou a NCW e sua aplicação na Guerra do Iraque.

Em um espectro mais amplo, a securitização do espaço informacional por parte dos Estados-Nacionais deve significar na ampliação das rivalidades interestatais nesses ambientes, especialmente quando se considera a crescente relevância estratégica dada a esses campos. Munidos dos pressupostos da Segurança Nacional, será comum observar Estados limitando ou ao menos condicionando o acesso de sua população a serviços como redes sociais.

As exposições de sujeitos como Snowden e Assange revelaram parte dos resultados dessa valorização estratégica dada ao espaço cibernético por parte dos EUA. Ainda que tal fato seja evidente, é necessário afirmar que os objetivos e políticas de Defesa Nacional e de inteligência de um determinado país influenciam decisivamente diversos outros campos sociais em nível global, como o econômico e dos direitos civis, especialmente quando essas políticas são desenvolvidas pela principal potência internacional.

Saber o que acontecerá no futuro é algo precioso à humanidade. Muitas religiões e cultos, inclusive, se baseiam em previsões, visões e profecias. A modelagem matemática e computacional permite ao ser humano prever, analisar e simular acontecimentos com base em informações do passado, sendo assim natural imaginar que a lógica militar logo se interessaria por essa capacidade. Na

verdade, a lógica e o incentivo militar foi propulsor desse campo científico ao longo do século 20, sendo essencialmente impossível separar o desenvolvimento do campo informacional-computacional do Departamento de Defesa dos EUA, haja vista a profunda ligação entre as ciências cibernéticas e computacionais com o estado americano desde o início de seus desenvolvimentos.

Além das ciências computacionais e cibernéticas, a instrumentalização militar do conhecimento de ciências sociais qualitativas (antropologia, sociologia etc.) em união com modelos computacionais preditivos pode ser observada ao exemplo do Projeto Camelot (1964), que consistiu de um conjunto de estudos em universidades americanas em conluio com a Defense Advanced Research Projects Agency (DARPA, conhecida como o cérebro do Pentágono) sobre contrainsurgência através de modelos computacionais.

Dessa maneira, vê-se como abordagens tecno-centradas dos conflitos são uma marca do pensamento militar dos EUA, que privilegia em grande medida a superioridade tecnológica em sua estratégia bélica.

Com isso em mente, diversas questões surgem a partir da avaliação dos rumos tomados pela tecnologia informacional e computacional em nível civil e militar a partir da Segunda Guerra Mundial. Indo de Neumann com sua comparação de cérebros humanos a computadores, aos sistemas armados automáticos, aos drones Reaper e a crescente ansiedade global com a inteligência artificial, os caminhos a serem trilhados pela humanidade parecem intimamente conectados com suas próprias criações eletrônicas.

Na política internacional, a interconexão de mercados e Estados através do espaço cibernético deve significar em maior rivalidade interestatal para a liderança nesse setor, ao mesmo tempo em que aumenta a vulnerabilidade dos agentes a possíveis ataques cibernéticos. Do ponto de vista dos direitos individuais, será inevitável perguntar se ainda será possível a manutenção de qualquer nível de privacidade ou de separação entre a esfera pública e privada em um mundo de rivalidades cibernéticas, marcado por uma separação cada vez mais ambígua entre combatentes e civis. Todos nós cuidados e observados por máquinas de graça e amor infinito (e eletrônico).

REFERÊNCIAS

AMBINDER, Marc. **What's XKEYSCORE? The NSA's global metadata search engine**. The Week, 2015. Disponível em: https://theweek.com/articles/461546/whats-xkeyscore. Acesso em: 10 jun. 2024.

ARQUILLA, John; RONFELDT, David. **In Athena's Camp: Preparing for Conflict in the Information Age**. Santa Mônica, RAND: 1996.

ARRIGHI, Giovanni. **Adam Smith in Beijing: Lineages of the Twenty-First Century**. Londres: Verso, 2007.

BANDEIRA, Luiz Alberto de Vianna Moniz. **A desordem mundial**. Rio de Janeiro: Editora Civilização Brasileira, 2017.

BARNETT, Thomas P.M. **The Seven Deadly Sins of Network-Centric Warfare**. US Navy Institute, Virginia, 1999.

BBC News. **EUA espionaram Petrobras, dizem papeis vazados por Snowden**. 2013. Disponível em: https://www.bbc.com/portuguese/noticias/2013/09/130908_eua_snowden_petrobras_dilma_mm.

BEYERCHEN, Alan. **Clausewitz, Nonlinearity, and the Unpredictability of War**. International Security, Vol. 17, No. 3, pp. 59-90. 1993.

BOUSQUET, Antoine James Aimé. **The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity**. London: UMI, 2008.

BOUSQUET, Antoine James Aimé. **A Revolution in Military Affairs? Changing Technologies and Changing Practices of Warfare**. Abingdon: Routledge. 2017.

CAPRA, Fritjof. **The Web of Life: A New Scientific Understanding of Living Systems**. Nova Iorque: Anchor Books, 1996.

CAMMONS, Dave et al. **Network-Centric Warfare case study**. Pennsylvania: CSL, 2013.

CORRELL, John T. **What happened to Shock and Awe?**. Air & Space Force, 2003. Disponível em: https://www.airandspaceforces.com/PDF/MagazineArchive/Documents/2003/November%202003/1103shock.pdf. Acesso em: 10 jun. 2024.

CORRELL, John T. **The Counter-Revolution in Military Affairs**. Air & Space Forces, 2019. Disponível em: https://www.airandspaceforces.com/article/the-counter-revolution-in-military-affairs/. Acesso em: 10 jun. 2024.

COX, Dan G. **Human Terrain Systems and the Moral Prosecution of Warfare**. Parameters 41, Nebrawska, 2011.

CRAWFORD, Neta. **The U.S. Budgetary Costs of the Post-9/11 Wars**. Universidade de Boston, Boston, 2021.

CZELUSTA, Mark G. **Business as Usual: An Assessment of Donald Rumsfeld's Transformation Vision and Transformation's Prospects for the Future.** Marshall Center, 2008. Disponível em: https://www.marshallcenter.org/en/publications/occasional-papers/business-usual-assessment-donald-rumsfelds-transformation-vision-and-transformations-prospects#toc-notes.

DAHL, Erik. **Too good to be legal? Network Centric Warfare and International Law**. 2004. Disponível em: https://jpia.princeton.edu/sites/g/files/toruqf1661/files/2004-3.pdf.

DERIAN, J. D. **Virtuous War: Mapping the military industrial media-entertainment network**. Londres: Routledge, 2009.

DOMBROWSKI, Peter; ROSS, Andrew. **The Revolution in Military Affairs, Transformation and the Defence Industry**. Security Challenges, 2008, Vol. 4, No. 4, pp. 13-38.

EDWARDS, P. N. **The Closed World: Computers and the Politics of Discourse in Cold War America**. Londres: MIT Press, 1996.

Eriksson, J., & Giacomello, G. **The Information Revolution, Security, and International Relations: (IR)relevant Theory?**. 2006. International Political Science Review, 27(3), 221-244.

GOMBERT, D. C. **National Security in the Information Age**. Naval War College Review, v. 51, n. 4. 1998.

GOITEIN, Elizabeth. **Rolling Back the Post-9/11 Surveillance State**. Brennan Center, 2021. Disponível em: https://www.brennancenter.org/our-work/analysis-opinion/rolling-back-post-911-surveillance-state.

GONZÁLEZ, Roberto J. **'Human Terrain' Past, Present and Future applications**. Anthropology Today, Londres, 2008.

GONZÁLEZ, Roberto J. **Seeing into Hearts and Minds**. Anthropology Today, Londres, 2015.

GONZÁLEZ, Roberto J. **War Virtually: The quest to automate conflict, militarize data, and predict the future**. Oakland: University of California Press, 2022.

HEIMS, S. J. **The Cybernetics Group**. Cambridge: The MIT Press, 1991.

HSCB - HUMAN SOCIAL CULTURE HUMAN SOCIAL CULTURE BEHAVIOR MODELING PROGRAM. 2009. Disponível em: https://apps.dtic.mil/sti/tr/pdf/ADA496310.pdf.

HUNT, Ryan. **Project Camelot and Military Sponsorship of Social Science Research: A Critical Discourse Analysis**. Pittsburgh: Duquesne University, 2007.

IBC - Iraq Body Count. **A Dossier of Civilian Casualties in Iraq 2003–2005**. Iraq Body Count, 2005. Disponível em: https://www.iraqbodycount.org/analysis/reference/press-releases/12/. Acesso em: 10 jun. 2024.

JCS - Joint Chiefs of Staff. **Joint Vision 2010.** 1996. Disponível em: https://apps.dtic.mil/sti/pdfs/ADA311168.pdf.

NY Times. **BUSH DETAILS PLAN TO FOCUS MILITARY ON NEW WEAPONRY**. New York Times, 2001. Disponível em: https://www.nytimes.com/2001/02/14/us/bush-details-plan-to-focus-military-on-new-weaponry.html. Acesso em: 10 jun. 2024.

NY Times. **THREATS AND RESPONSES: THE PENTAGON; RUMSFELD ORDERS WAR PLANS REDONE FOR FASTER ACTION**. New York Times, 2002.
Disponível em: https://www.nytimes.com/2002/10/13/world/threats-responses-pentagon-rumsfeld-orders-war-plans-redone-for-faster-action.html. Acesso em: 10 jun. 2024.

NYE, Joseph. **Soft Power: the means to success in world politics**. Toronto: Public Affairs, 2004.

O Globo. **Ministério de Minas e Energia está na mira de espiões americanos e canadenses**. O Globo, 2013. Disponível em: https://g1.globo.com/fantastico/noticia/2013/10/ministerio-das-minas-e-energia-esta-na-mira-de-espioes-americanos-e-canadenses.html. Acesso em: 10 jun. 2024.

Opera Mundi. **Novos documentos vazados afirmam que Petrobras também foi alvo de espionagem norte-americana**. Opera Mundi, 2013. Disponível em: https://operamundi.uol.com.br/politica-e-economia/novos-documentos-vazados-afirmam-que-petrobras-tambem-foi-alvo-de-espionagem-norte-americana/. Acesso em: 10 jun. 2024.

PICKERING, Andrew. **The Cybernetic Brain: sketches of another future**. Chicago: University of Chicago Press, 2010.

RID, Thomas. **Cyber War will not take place**. Oxford: University Press, 2013.

ROCHA, M.; FONSECA, D. F. **A questão cibernética e o pensamento realista**. R. Esc. Guerra Nav., Rio de Janeiro, v. 25, n. 2 p. 517-543. 2019.

SINGER, P.W. **Wired for War: the robotics revolution and conflict in the 21st century**. Nova Iorque: Penguin Press, 2009.

STEVENS, Tim. **Cyber Space and the State: toward a strategy for cyber-power**. Londres: King's College Press, 2011.

Strategic Studies Institute - SSI. **The Information Revolution and National Security**. US. Army War College: Washington, 2000.

TABANSKY, Lior. **Basic Concepts in Cyber Warfare. Military and Strategic Affairs**, v.3 n.1. 2011.

The Guardian. **NSA Prism program taps in to user data of Apple, Google and others**. The Guardian, 2013. Disponível em: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

The Guardian. **XKeyscore presentation from 2008**. The Guardian, 2013. Disponível em: https://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation.

ULLMAN, K. Harlan; WADE, James P. **Shock and Awe: Achieving Rapid Dominance.** Washington: The National Defense University: 1996.

VALENTINE, Douglas. **The Phoenix Program.** Nova Iorque: William Morrow & Co, 1990.

VON NEUMANN, John. **Theory of Self-Reproducing Automata**. London: University of Illinois Press, 1966.

WBUR. **How the Snowden leaks changed government surveillance**. WBUR, 2023. Disponível em: https://www.wbur.org/onpoint/2023/07/05/how-the-snowden-leaks-changed-government-surveillance. Acesso em: 10 jun. 2024.

WIENER, Norbert. **The human use of human being**. Cambridge: The Riverside Press, 1950.