RESUMO
Guerra cibernética / guerra eletrônica – conceitos, desafios e espaços de interação

A conceituação do que é guerra cibernética não se consolidou como uma categoria de análise da Ciência Política e das Relações Internacionais e já apresenta desdobramentos importantes, em relação a outras formas de conflito, que envolvem tecnologia eletrônica de amplo espectro. Normalmente os pesquisadores tendem a divergir da natureza do conceito de guerra cibernética em si, que se confundem com ativismo, crimes comuns, espionagem e atos de guerra. No bojo desta discussão, um fato novo surge, interceção entre ações cibernéticas e a guerra eletrônica "convencional". Ambas partem dos mesmos fundamentos estratégicos (roubar informações, enganar e inviabilizar a ação do inimigo) de tal forma, que já podemos falar de um espaço de conflito "ciber-eletrônico", que envolve a utilização de tecnologia de guerra eletrônica e diversos tipos de malware utilizando a tecnologia wifi como modo de transmissão. Este trabalho tenta discutir o quanto a evolução da tecnologia tem tornado as fronteiras de guerra eletrônica e cyberwar tênues, de tal forma que, num futuro talvez haja uma nova área de interseção, a da guerra centrada em redes e sistemas sem fio.

Palavras-chave: Guerra, Tecnologia, Cibernética, Guerra Eletrônica, Guerra Centrada em Redes.

ABSTRACT

The conceptualization of what is cyber warfare has not consolidated as a category of analysis of Political Science and International Relations and already presents important developments, in relation to other forms of conflict, involving electronic technology of wide spectrum. Usually researchers tend to disagree with the nature of the concept of cyber warfare itself, which is confused with activism, common crimes, espionage, and acts of war. At the heart of this discussion, a new fact arises, interception between cybernetic actions and the "conventional" electronic warfare. Both start from the same strategic foundations (stealing information, deceiving and making enemy action unfeasible) in such a way that we can already speak of a "cyber-electronic" conflict space, involving the use of electronic warfare technology and various types of Malware using wifi technology as the transmission mode. This paper attempts to discuss how the evolution of technology has made the frontiers of electronic warfare and cyberwar tenuous, such that in the future there may be a new area of intersection, that of war centered on wireless networks and systems.

Keywords: War, Technology, Cybernetics, Electronic Warfare, Networked Warfare.

Guerra cibernética / guerra eletrônica – conceitos, desafios e espaços de interação

Ricardo Borges Gama Neto[1]

INTRODUÇÃO

Este texto vai discutir de forma preliminar e descritiva o processo de convergência entre dois tipos de tecnologias materializadas nos conceitos de guerra cibernética[2] e guerra eletrônica[3] dentro de uma nova abordagem de interação estratégica entre as diferentes forças de defesa estatais que têm sido convencionalmente denominada guerra centrada em rede. O objetivo deste trabalho não é descrever em pormenores o impacto que este novo approach tem tido nas últimas décadas no desenvolvimento do conflito militar moderno, mas sim demonstrar que a evolução da tecnologia da internet e da microeletrônica tem promovido uma forte convergência entre aquelas duas formas de ação.

Apesar de não ter pretensões mais sofisticadas de análise teórica, este texto parte de dois pressupostos realistas para entender as relações causais que envolvem a questão do desenvolvimento da tecnologia e seu uso como instrumento militar: 1) os Estados são os principais atores no sistema político internacional que é intrinsecamente anárquico e externamente estruturado; e 2) os estados buscam a cooperação de forma puramente estratégica, ou seja, para a obtenção mútua, não necessariamente isonômica, de ganhos (WALTZ, 1988)[4].

1 Ricardo Borges Gama Neto, professor do departamento de Ciência Política (DCP) da Universidade Federal de Pernambuco (UFPE)

2 De forma simplificada guerra cibernética "pode ser definida como o conjunto de técnicas que, utilizadas para burlar o sistema de segurança de um computador ou conjunto destes, busca quebrar (to crack) a integridade de informações e/ou tirar do ar um determinado serviço virtual" (GAMA NETO; LOPES, 2014, p. 31). Contudo, deve ser observado que vírus e worms também podem ser utilizados para causar danos em equipamentos físicos, como por exemplo, no caso das centrifugas nucleares do Irã e o Stuxnet.

3 Guerra eletrônica é utilização de emissões eletromagnéticas e eletro-ópticas para detectar, neutralizar e/ou reduzir a capacidade de ação de uma força adversária, inclusive impedindo que o mesmo faça uso de sua capacidade de emissões.

4 A realpolitick não desaparece na Era da Informação. Mas permanece centrada no Estado, numa era organizada em torno de redes, inclusive redes de Estados. (...) Os Estados existem, (...), sua razão de ser continua sendo, em última instância, sua capacidade de exercer a violência em defesa dos interesses que representam - inclusive os seus próprios. Mas a guerra também está sendo transformada por redes de computadores. Em

O trabalho está estruturado da seguinte forma: uma introdução, as explicações do que são guerra cibernética e guerra eletrônica, o processo (ou possível) de convergência entre ambas e uma conclusão. Como a função deste texto é basicamente exploratória (e por sua consequência descritiva) ao tema, não há apresentação de teorias explanatórias ou mesmo de uma metodologia de análise e coleta de dados mais sofisticada. Deixamos de lado também qualquer alusão ao problema da aplicação da alta tecnologia militar contra adversários não assimétricos como grupos terroristas ou exércitos não estatais.

GUERRA E TECNOLOGIA

A relação entre tecnologia e guerra é intensa. A história demonstra que as inovações tecnológicas, de uma forma ou outra, sempre influenciaram o ato de "fazer a guerra" e muitas vezes determinaram perdedores e vencedores. Da Idade do Ferro ao mundo Pós-Industrial, do uso do cavalo com estribos pelos Hunos ao uso de drones com capacidade de ataque por países como Estados Unidos e Israel[5], a criatividade humana no desenvolvimento de novos conhecimentos, métodos, técnicas e produtos usados para resolver os problemas práticos das sociedades forneceram vantagens a seus possuidores. A cada revolução tecnológica e seu aprimoramento no uso militar, surgiam novas armas, atores, táticas e conflitos[6].

> Identifying "revolutions in military affairs" is arbitrary, but some inflection points in technological change are larger than others: for example, the gunpowder revolution in early modern Europe, the industrial revolution of the nineteenth century, the second industrial revolution of the early twentieth century, and the nuclear revolution in the middle of the last century.1 In this century, we can add the information revolution that has produced today's extremely rapid growth of cyberspace. Earlier revolutions in information technology, such as Gutenberg's printing press, also had profound political effects, but the current revolution can be traced to Moore's law and the thousand-fold decrease in the costs of computing power that occurred in the last quarter of the twentieth century (NEY JR. 2011, p. 18).

Mesmo que a tecnologia impacte de forma indelével os conflitos militares, seu emprego sobre cada um difere, há uma miríade de variáveis capaz de intervir neste processo. Não há como predeterminar ex-ante de que forma as mudanças na tecnologia ou sua aplicação impactarão nas dinâmicas dos conflitos. A guerra é um animal incrivelmente dinâmico.

Para os objetivos deste texto, destacamos a assimetria de conhecimento tecnológico. Atualmente a revolução tecnológica produzida pelo avanço da microeletrônica e a crescente dependência das economias e sociedades da internet têm produzido uma inflexão nas

primeiro lugar, tecnologicamente: comunicações eletrônicas, sistemas de vigilância, aviões não tripulados e munições guiadas por satélite são as armas decisivas na confrontação militar. Em segundo lugar, estrategicamente. (...). Essa guerra centrada na rede, na terminologia do Pentágono, depende inteiramente de comunicações seguras, robustas, capazes de manter conexão constante entre nós de uma rede. (CASTELLS, p. 132-3, p. 2003).

5 Sobre o uso de Veículos Aéreos Não Tripulados (VANTS), também conhecidos como Drones, na política internacional ver Gregory (2011) e Allinson (2015).

6 "If it is true that every part of war is touched by technology, is it no less true that every part of technology affect war. Indeed, technologies not ordinarily regarded as military, such as roads, vehicles, communications, and timekeepers, have done as much as weapons and weapons systems to shape the face of war" (Van Creveld,2010, p. 311).

táticas da guerra (localizar e identificar o inimigo, processar as informações conseguidas e desenvolver o meio mais eficaz de combater utilizando as armas mais precisas e letais à disposição). A guerra do Golfo, muito provavelmente, foi o primeiro exemplo deste novo tipo de guerra que nasceu nos laboratórios e centros de estudos de defesa (como por exemplo o Air Force Research Laboratory - AFRL/IF - da Força Aérea dos Estados Unidos). Como destaca Amarante (2010, p. 07):

> Na Guerra do Golfo, em presença da avalanche tecnológica, o Iraque se quedou imobilizado a uma distância inofensiva em relação às forças aliadas. Foi uma guerra de stand-off – manutenção do adversário a distância – em que o poder de fogo e o movimento da coalizão preponderaram sobre as vencidas forças iraquianas. Ela também reverteu uma tendência histórica, na qual o fogo tinha sempre contribuído para o sucesso da manobra. Durante a ofensiva terrestre da Guerra do Golfo Pérsico, os papéis inverteram-se e a manobra concorreu para a eficácia do fogo, compelindo a concentração das forças iraquianas para fazer face ao movimento de envolvimento das forças aliadas.

A guerra do futuro será fortemente apoiada em sistemas de vigilância e aquisição de múltiplos alvos, software embarcado, veículos com baixa assinatura eletrônica e térmica, aquisição e processamento de informações em tempo real (C4IRS)[7] uso intenso de emissões eletromagnéticas e da guerra cibernética, dentre outras tecnologias[8]. A guerra moderna parece se centrar em duas dimensões essenciais, a explosão na quantidade/qualidade de informações disponíveis aos estrategistas e comandantes militares (detecção, armazenagem, filtragem das informações disponíveis) do campo de batalha e a utilização crescente de armas dirigidas ou remotamente tripuladas como bombas inteligentes, mísseis de cruzeiro guiados por satélite/GPS e drones. Ambas dimensões teoricamente permitem algo nunca realizado antes, guerras onde o planejamento e as operações acontecerão em tempo real[9], em todas as dimensões (ar, terra, mar).

2. GUERRA CIBERNÉTICA

A data do surgimento do que convencionou-se chamar de guerra cibernética, é quase datada, 27 de abril 2007. Neste dia, sites do governo, bancos e os principais jornais estonianos sofreram uma série de ataques do tipo negação de serviço (Denial of Service - DDoS) através de redes botnets[10]. Ataques deste tipo consistem, basicamente, em enviar pedidos

7 Designa a expressão (em inglês) de centros de comando, controle, computadores, comunicação, inteligência, sobrevivência e reconhecimento.

8 Para ver um pequeno inventário do que o departamento de Defesa dos EUA consideram tecnologias críticas consultar Bellintani e Bellintani, 2014.

9 Para termos uma ideia do avanço da quantidade de informações que poderão ser disponibilizadas aos comandantes que dispuserem de tal tecnologia vejamos o exemplo descrito no site Sistema de Armas: "Durante a Batalha de Trafalgar em 1805, por exemplo, o Almirante Nelson usava apenas três bandeiras táticas para sinalizar e manobrar sua frota. No auge da Operação Tempestade do Deserto, o General Schwarzkopf usava mais de 700.000 chamadas telefônicas e 152.000 mensagens de rádio por dia para coordenar as ações da Coalizão". < http://sistemasdearmas.com.br/ggn/ggn02c4i.html >. Acessado em junho de 2015.

10 Provavelmente o primeiro caso de ataque cibernético tenha ocorrido em 1982. Em junho explodiu o grande gasoduto Trans-Siberiano. A explosão teria sido causada pela introdução, pelo serviço secreto dos EUA, de um bug no software do sistema de gerenciamento e prospeção de gás, roubado pela KGB de uma empresa canadense. A explosão causou "(...) the most monumental non-nuclear explosion and fire seen from space" (REED, 2005, p. 269).

de informação aos servidores num volume muito maior do que sua capacidade de processamento. O ataque foi executado por uma rede de computadores zumbis de praticamente todos os países do mundo[11].

O ataque a Estónia simplesmente alertou a todas as autoridades de defesa do mundo sobre a existência de um fato que estava na agenda política de defesa da maioria dos países, pelo menos desde a última década do século passado, à utilização da internet como arma de guerra e espionagem (ARQUILLA; RONFELD, 1993).

> Durante a crise do Kosovo, a NATO enfrentou os seus primeiros incidentes sérios de atentados cibernéticos. Entre outros, a conta de correio electrónico da Aliança ficou bloqueada para visitantes externos durante vários dias e houve perturbações repetidas do website da NATO.
>
> Porém, típico à época, a dimensão cibernética do conflito foi considerada apenas um entrave à campanha de informação da NATO. Os atentados cibernéticos eram vistos como um risco, mas um risco limitado tanto em termos de âmbito como de potencial para causar prejuízos, para o qual era apenas necessária uma reacção técnica limitada, acompanhada por esforços de informação pública de pequena dimensão.
>
> Foram necessários os acontecimentos de 11 de Setembro para mudar essa percepção. Mas ainda foram precisos os incidentes na Estónia, no Verão de 2007, para que esta crescente fonte de ameaças à segurança pública e à estabilidade estatal merecesse finalmente toda a atenção política. Uma onda de atentados cibernéticos maciços que durou três semanas veio demonstrar que as sociedades dos países membros da NATO, extremamente dependentes das comunicações electrónicas, também eram extremamente vulneráveis na frente cibernética[12].

Contudo, em face da natureza e novidade do fenômeno, à existência de uma ciberguerra não é unanimidade entre os especialistas, Hamadoun Toure, secretário geral da União Internacional das Telecomunicações (UTI) é cristalino ao afirmar que a guerra cibernética está chegando, e, "just like a conventional war, there are no winners, only destruction"[13], outros por exemplo, como Howard Schimidt, conselheiro da Casa Branca para questões de segurança cibernética do governo Barack Obama, afirma categoricamente que "there is no cyberwar"[14].

Geers (2011) observa que a guerra cibernética não é um fim em si mesma, mas um meio para atingir uma variedade de outros fins. Desta forma, além da questão da natureza mil-

11 O país ficou com problemas nas comunicações e nos negócios durante semanas. "Os dez maiores ataques lançaram fluxos de 90 megabits de dados por segundo nas redes da Estônia, durando até 10 horas cada ataque. Esse volume de dados equivale a fazer o download do sistema operacional Windows XP inteiro a cada seis segundos durante 10 horas". <http://g1.globo.com/Noticias/Tecnologia/0,,MUL45961-6174,00.html>. Acessado em junho de 2015.

12 THEILER, Olaf. "Novas Ameaças Cibernéticas". Revista da NATO, setembro de 2011 < http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/PT/index.htm >. Acessado em junho de 2015

13 Cyberwar is reality world must fight: UN official. <http://phys.org/news/2013-07-cyberwar-reality-world.html>. Acessado em junho de 2015.

14 SINGEL, Ryan. "White House Cyber Czar: There is no Cyberwar". Wired. 04 de março de 2010. Acessado em maio de 2013

itar do conflito, ataques cibernéticos são facilmente confundidos com outros tipos de ação como crime ou ativismo político[15], como por exemplo caso de roubos a sistemas bancários ou famosos casos Wikileads e Eduard Snowden. Um outro caso interessante é o do grupo de hackers Dragonfly, aparentemente situados no leste europeu, que tem desenvolvido uma extensa rede de espionagem contra empresas nos EUA, Canadá e Europa Ocidental, especialmente de energia[16].

Clarke e Knake (2010) defendem que a capacidade de um país num conflito deste tipo, deve ser medida como consequência de três dimensões: a) ofensiva - atacar outros atores estatais; b) defensiva - bloquear e/ou reduzir o estrago derivado do ataque e c) dependência, a extensão em que o sistema de computadores de um país é vulnerável a ciberataques. No entender daqueles os EUA têm a maior capacidade ofensiva, mas a China e a Coréia do Norte possuem maior capacidade de defesa, pois podem desligar sua internet e isolar-se do mundo.

Mesmo que a possibilidade de mortes em um ataque cibernético seja baixa, um ataque a sistemas de computadores pode ser maciçamente disruptivo e deixar um país impotente vis-à-vis a ação de um adversário tanto militar quanto economicamente. Além disto, a internet pode ser utilizada para o roubo de segredos industriais e militares. Há um vasto cabedal de suspeita que a China (Unidade 61398 do Exército Popular)[17] e Coréia do Norte (Gabinete 121) têm realizado espionagem e ataques cibernéticos contra os EUA, Coréia do Sul, Japão e outros países. Existem fortes suspeitas que Israel (Unidade 8200) e EUA (National Security Agency/Central Intelligence Agency) desenvolveram, através de suas agências de segurança, malwares como Stunex, Flame com o objetivo de atacar as centrífugas de enriquecimento de urânio do Irã e espionar outros países do Oriente Médio. A Rússia foi o país que provavelmente mais utilizou a internet como arma de ataque contra adversários em conflito, Estônia (2007), Georgia (2008) e Ucrânia (2014).

É reconhecida a utilização de softwares maliciosos e outras técnicas invasivas com objetivos de adquirir informações confidenciais, implantar falsas, derrubar sites e sistemas e danificar instalações civis e militares. Contudo, "outra categoria de ataques deste tipo, e menos divulgada, é a que resulta da utilização de hardware adulterado, nomeadamente circuitos que utilizam milhares de transístores e de reduzidas dimensões (chips) e de

15 Carr (2010) observa que sites israelenses têm sido uma vítima constante do ciberativismo político de origem palestina e simpatizantes. Durante a operação militar contra o Hamas, no final de 2008 e início do ano posterior, houve uma forte campanha de ataque cibernético contra o país. "The exact number of Israeli or other websites that have been disrupted by hackers is unknown, but the number is well into the thousands. According to one estimate, the number reached 10,000 by the first week of January 2009 alone. Most attacks are simple website defacements, whereby hackers infiltrate the site, leaving behind their own graffiti throughout the site or on the home page. The hackers' graffiti usually contains messages of protest against the violence in Gaza, as well as information about the hackers, such as their handles and country of origin" (p. 19)

16 A empresa CyActive (http://www.cyactive.com) identificou em 2014 pelo menos cinco grandes grupos de hackers que utilizam malwares para ação criminosa contra empresas e bancos ocidentais.: Snake, Black-PoS, Gyges, Dragonfly e Zberp.

17 Dados de quatro milhões de funcionários do governo norte-americano foram roubados via internet. a suspeita cai sobre hackers chineses. De acordo com Duda Teixeira (2015), "A China é o país que mais agressivamente tem coletado informações dos americanos. Os setores mais procurados são os de tecnologia e pesquisas espaciais, que podem turbinar a competitividade das estatais chinesas. A maior parte deles em Xangai. Em maio, cinco membros do Exército Popular da China fora indicados por espionagem industrial nos Estados Unidos". (p 68).

quase impossível controlo de qualidade e funcionamento. Utilizados a ritmo crescente, por exemplo, em sensores e sistemas de segurança em aeronaves, crescem os receios sobre a sua fiabilidade e a confiança nas suas origens" (SANTOS, 2010).

O uso de técnicas de guerra cibernética, na situação de guerra declarada, nunca ocorreu (no caso da Georgia e Rússia, apenas este último utilizou a internet como arma). No entanto, em caso de uma situação de conflito militar entre duas forças, técnicas de ataque cibernético seriam as primeiras a serem utilizadas, antes mesmo da ação de forças de combate. Quem for mais capaz de atacar e resistir aos ataques cibernéticos estará em vantagem. Muito provavelmente, a rede mundial de computadores poderá viabilizar a ideia de Sun Tzu, da guerra ser vencida sem o inimigo estar em conflito, pela completa incapacidade de um ator de utilizar sua capacidade econômica e força militar contra seu adversário[18].

3. GUERRA ELETRÔNICA

A guerra eletrônica é uma consequência direta da evolução da tecnologia de detecção e comunicações ocorrida durante e depois da Segunda Grande Guerra Mundial. A invenção dos radares, aperfeiçoamento dos sistemas de interceptação e interferência de ondas de rádio e da criptografia, revolucionou a forma como se fazia a guerra até então[19]. Agora aviões poderiam ser detectados bem antes de chegar a seus alvos, ordens de comandantes poderiam ser enviadas as suas tropas a distâncias muito maiores do que jamais tinha sido feito, ou, serem interceptadas favorecendo forças inimigas[20]. Contudo, todo o avanço tecnológico promovia do outro lado a tentativa de burlar (contra- medidas) aquela evolução. Se havia o radar inglês, os alemães tinham seus rádio-telêmetros para controle de tiro das embarcações e Knickebein para orientação de aviões, etc…

> O campo de batalha da guerra eletrônica é o aspecto eletromagnético. Como a matéria e a gravidade, a radiação eletromagnética é um dos componentes fundamentais do universo. Abrange uma larga faixa de frequências: desde as mais baixas, empregadas em enlaces de longo alcance, passando pelas faixas utilizadas

18 Em 2011 o software de controle de dois tipos de Vants, o Predator e o Reaper, foram infectados por um vírus comum que afeta o sistema operacional Windows chamado Keylogger. Em 2009 os computadores do Ministério da Defesa inglês e de navios de guerra da frota foram contaminados pelo worm Conficker/ Downadup. Neste mesmo ano, a frota de Rafales da Marine francesa foi groundeada por causa do mesmo tipo de malware que afetou os ingleses, impossibilitando os franceses de utilizar os seus sistemas de comunicações, obrigando a força "to return to more traditional forms of communication: telephone, fax and post". < http://www.telegraph.co.uk/ news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html >. Acessado em junho de 2015.

19 A Segunda Guerra Mundial pode ser considerada o ponto inicial da guerra eletrônica, contudo deve se observar que tanto o surgimento do radar (Radio Detection And Ranging) quanto do sonar (Sound Navigation And Ranging) é anterior. O radar evoluiu especialmente durante os anos 1930. Já a invenção do Sonar pode ser datada de antes da I Guerra Mundial. A primeira patente de um dispositivo de ecolocalização submarina (hidrofone) é de 1912. Contudo, com o conflito de 1914-1918, a necessidade de pesquisas para detecção de submarinos foram aprofundadas por ingleses, franceses e alemães. De acordo com Meadowcroft (2006) "the British built the first successful hydrophone in late 1915. (...). The first submarine kill credited to hydrophones occurred on 23 April 1916" (p. 567).

20 A Batalha Naval de Tsushima, em 1905, é reconhecidamente a primeira guerra onde houve a utilização do rádio como meio de comunicação. De acordo com Sakar et all (2006), a comunicação entre os navios de guerra japoneses foi o elemento fundamental para a vitória do país sobre a Rússia. "The wireless telegraph message that the enemy fleet had been sighted was a decisive factor in the Japanese victory" (p. 406).

> em radiodifusão e nas transmissões de televisão, radares e ainda pela radiação infravermelha, incluindo o espectro óptico familiar da luz visível, de vermelho a violeta, até as mais altas, das radiações ultravioleta, raios X e gama (RICHARDSON, 1991, p. 24).

Guerra eletrônica é um termo genérico que engloba todas as ações militares, destinadas a assegurar o uso mais eficaz possível de emissões eletromagnéticas e eletro-ópticas e impedir que o inimigo consiga fazer uso dos seus. Os sistemas que permitem o uso militar e desprendimento desta energia, tanto de forma ofensiva ou defensiva, variam amplamente. Podemos classificar as "ações" da guerra eletrônica em quatro tipos: i. detecção (radares, sonares, receptores de alerta antecipado); ii. coleta de informações (Sigint - Signals Intelligence, Elint - Eletronic Inteligence, Comint - Comunications Inteligence); iii. contramedidas (chaffs, flares, anti-jamming); e iv. interferência intencional (jamming, desvio de sinais/dissimulação e armas do tipo Electo-magnetic Pulse)[21].

Mesmo que a guerra eletrônica seja classificada como o uso ou negação da energia eletromagnética, armas cinéticas como mísseis antiradiação são classificados como instrumentos operacionais desta forma de combate, pois sua função é o de suprimir fisicamente radares, como é o caso dos mísseis MAR-1 e AGM-88C. Além destes, todos os tipos de veículos, navios e aeronaves militares modernos possuem uma suíte de guerra eletrônica integrada (como por exemplo, o israelense Black Fox para tanques de guerra, a Spectra do caça francês Rafale e o sistema LIG NEX1 SLQ-200 das fragatas sul-coreanas da classe Sejong). Existem também equipamentos destinados especificamente para a guerra eletrônica, como aviões radares ou com a missão específica de supressão de defesa (exemplo o EA-F18 Growler).

Pós-1945 cada conflito militar significou uma nova revolução na guerra eletrônica. Bastos (2005) afirma que o uso da guerra eletrônica atingiu sua maioridade no conflito entre o Vietnã e os EUA. O uso intensivo de radares, mísseis antiaéreos pelos norte vietnamitas e mísseis antiradiação e o desenvolvimento de uma enorme gama de sistemas de detecção, interferência eletrônica e navegação por parte dos EUA foi uma das características daquele conflito. Outro momento importante, desta vez no Mar, foi a utilização pela Marinha de Israel da combinação de contramedidas, jamming e mísseis antinavio Gabriel durante a Guerra do Yom Kippur (1973) contra navios de guerra da Síria e do Egito[22]. No entanto, nenhum dos conflitos chegou perto do impacto que os dois conflitos com o Iraque (1991 e 2003) demonstraram em termos de evolução da guerra eletrônica. Nestes os EUA e seus

21 O Departamento de Defesa e a NSA no Eletronic Walfare in Operations (FM3-36 - 2009) subdividem a guerra eletrônica em três grupos: a) Ataque eletrônico - Uso de energia direcionada ou armas antiradiação para atacar, destruir e inutilizar a capacidade de combate do adversário; b) Proteção eletrônica - ações para proteger equipamento de qualquer ação ou uso de espectro eletromagnético do inimigo e c) Apoio a guerra eletrônica - ações que permitam ao comandante operacional procurar, localiza e interceptar emissões de energia eletromagnéticas. < http://hosted.ap.org/specials/interactives/_documents/electronic_warfare.pdf>. Acessado em junho de 2015. O site Sistema de Armas apresenta outra divisão. "A GE tem três subdivisões distintas: Medidas de Apoio de Guerra Eletrônica - MAGE, Contramedidas Eletrônicas - CME e Contra-Contramedidas Eletrônica" < http://sistemasdearmas.com.br/ggn/ggn03guerraeletronica1.html >. Acessado em junho de 2015.

22 Não foi apenas no Mar que as forças armadas israelenses demonstraram serem tecnologicamente superiores. No ar Israel utilizou radares doppler, sistemas de supressão de emissão de infravermelho e robustas emissões de contramedidas para reduzir a capacidade dos mísseis antiaéreos soviéticos, especialmente os moderníssimos SAM-6.

aliados apresentaram uma tal superioridade tecnológica, em todas as dimensões do combate, que impressionou o mundo.

> Na Guerra do Golfo, na presença da avalanche tecnológica aliada, o Iraque ficou imobilizado, incapaz de atuar infringindo danos as forcas aliadas. Sensores e atuadores, operando no espectro eletromagnético, interferiram nas comunicações, neutralizando sistemas de defesa e garantindo Uma supremacia eletromagnética, com vistas a anulação de pontos vitais de defesa e do sistema logístico. O resultado foi o envolvimento quadridimensional (caracterizado pelo domínio das três dimensões espaciais e da dimensão eletromagnética) estabelecido pelos aliados, que inibiu o poder militar de Saddam Hussein e que reduziu o Iraque a um contendor cego, surdo, mudo imobilizado e desprovido de vontade de lutar. A consequência foi a rendição incondicional iraquiana (AMARANTE, 2003, p. 03).

Desde o final da última década do século passado, a primeira fase das guerras em larga escala em que os EUA e forças ocidentais atuaram têm sido uma combinação de armas cibernéticas e eletromagnéticas com a função de iludir, enganar, inviabilizar a capacidade de detecção, ataque e de troca de informações do inimigo. Tais ações ocorrem de forma conjunta. Antes do ataque das forças de coalização ao Iraque (1993) foi introduzido nos sistemas da defesa antiaérea iraquiana um vírus que fornecia aos radares informações erradas, depois foram utilizados aviões especializados em guerra eletrônica (EF - F111 Raven) para criar corredores por onde aviões F-16, Tornado, F-15 e F-18 penetraram no que restou das defesas inimigas. O mesmo padrão ocorreu em 2003. O mais importante a constatar é que, em vez de buscarem alvos a serem meramente destruídos, como sistemas de comando e controle, o mais importante passou a ser, em muitos casos, localizar e desativar os eixos fundamentais que ligam os sistemas e torná-los inoperantes[23]. Um exemplo pode ser visto nas redes de eletricidade e de comunicação, em vez de serem destruídos podem ser desligados ou isolados. Depois desta fase, ocorrem ataques cinéticos com mísseis de cruzeiros e ataques aéreos com bombas inteligentes contra alvos específicos, especialmente as tropas inimigas em solo. O avanço dos exércitos aliados somente aconteceu quando as forças terrestres iraquianas estavam virtualmente destruídas, sem capacidade coordenada de reação.

A tática exposta no parágrafo anterior tem a grosso modo, os seguintes objetivos: primeiro, a diminuição de perda de vidas civis (o que evita que oficiais militares destes países possam sofrer processos por violarem o protocolo I da Convenção de Genebra); segundo, redução da exposição dos soldados ao combate, que ocorre somente depois de boa parte da capacidade militar do adversário estar inoperante ou destruída; terceiro, diminuição dos custos com o uso de bombas e mísseis inteligentes (cada vez mais caros), que pode ser direcionada mais efetivamente, contra as forças armadas adversárias; quarto, que as forças ocupantes

23 "A Guerra do Golfo introduziu um novo paradigma de aplicação do poder aéreo: os planejadores operacionais selecionaram como alvos os nós fundamentais de um sistema para alcançar objetivos desejados em vez de visarem todo o sistema para destruí-lo. Por exemplo, ao visarem o Sistema Integrado de Defesa Antiaérea (IADS) do Iraque os planejadores designaram pontos médios de impacto desejados (DMPI) que, quando atingidos, incapacitariam as funções de comando e controle dos centros de operações setoriais (SOS). Como resultado, o objetivo operacional dos combatentes era incapacitar o IADS setorial sem ter de destruir todo o SOS. Os planejadores foram capazes de reduzir de oito para duas o número de PGM de 2000 libras lançadas contra cada SOS na primeira noite da guerra. Não apenas isto conseguiu o efeito desejado, mas liberou uma quantidade gigantesca de poder de fogo para concentrar-se em outros sistemas críticos" (SINE, 2006)

possam recuperar a estrutura danificada e usar a seu favor durante a fase de ocupação e por fim, permitir que o país após o conflito possa retomar "as atividades" o mais rápido possível ao fim do conflito.

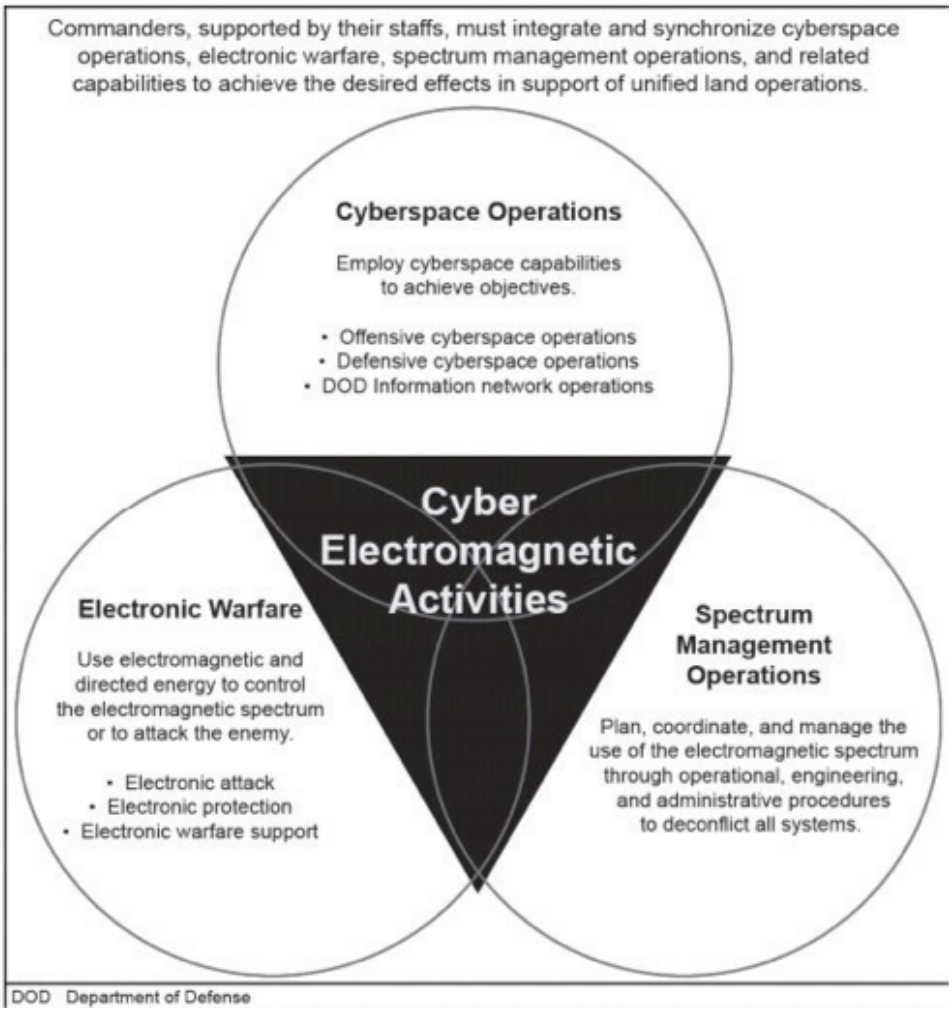
Contudo, a utilização da guerra eletrônica e das armas cibernéticas tem passado por uma forte transformação. Mesmo sendo instrumentos/armas diferentes, sua lógica de ação e o desenvolvimento do padrão da tecnologia e das novas exigências do combate moderno têm tornado sua separação mais tênue, gerando uma nova abordagem chamada "Atividades Ciber Eletromagnéticas".

4. CONVERGÊNCIA

Como observado na introdução, este paper tem como objetivo apresentar de forma preliminar e descritiva a hipótese de que há um processo de convergência entre as atividades de guerra cibernética e guerra eletrônica. Esta aproximação pode ser percebida como consequência da mais nova abordagem de interação entre as diferentes formas de ação militar que sido denominada guerra centrada em rede.

O Exercito Norte Americano em um documento de fevereiro de 2014 define as Atividades Ciber Eletromagnéticas - em inglês Cyber Electromagnetic Activities (CEMA) -, como uma nova direção na forma como as forças terrestres devem operar o ciberespaço e o aspecto eletromagnético. Destacam que as forças armadas americanas operam em um mundo onde as ações militares são fortemente dependentes de redes, desta forma as unificação destas duas formas de guerra tem como objetivo permitir aos EUA tem vantagem sobre os inimigos no ciber espaço e no aspecto eletromagnético, degradando e negando ao inimigo o uso deste mesmo sistema. A figura 01 representa de forma cristalina a abordagem do Exercito americano do problema.

Figura 01 - Atividades Ciber Eletromagnéticas



Fonte: United States Army (2014, secção 1.2).

Apesar de mais limitada que a abordagem que desejamos apresentar, a desenvolvida pelo exército norte americano preconiza, acertadamente, que mesmo sendo atividades conceitualmente diferentes elas, pela sua natureza e meios, tem de serem operacionalizadas de forma conjunta. O CEMA é definido como um esforço unificado onde as operações de ciberguerra e eletrônica devam ser integradas e sincronizadas, percebidas como um ambiente operacional único[24].

> An operational environment is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander . An analysis of an operational environment must consider the five domains and the EMS. The four traditional domains (air, land,

24 Os US Marines no documento Marine Aviation Plane - 2015 afirmam que "one of the fastest evolving portions of Digital Interoperability involves efforts in the Cyber/Electronic Warfare Convergence concept. Airborne networking and the Marine Corps' increased ability to "Maneuver within Spectrum" has enabled the Marine Corps to explore other concepts like advanced Cyber/EW payloads aboard manned and unmanned platforms. With the efforts of the Marine Corps in the digital operability realm, it will be well positioned to move operational control of advanced Cyber and EW payloads down to the tactical edge over the next several years. < http://www.aviation.marines.mil/Portals/11/2015%20Marine%20Aviation%20Plan%20Final_%2010%20Oct%202014_1110%20EDT.pdf >. Acessado em junho de 2015

> maritime, and space) and the EMS exist naturally. The fifth domain, cyberspace, is manmade. Cyberspace and the EMS provide commanders the ability to share information, communicate, integrate, and synchronize operations across all warfighting functions and echelons. Conversely, cyberspace and the EMS provide adversaries and enemies an effective, inexpensive, and anonymous means for recruitment, information activities, training, and command and control. CEMA provide commanders with the ability to gain and maintain an advantage in cyberspace and the EMS. (USAArmy, 2014, secção 1.8 e 1.9).

O ciberespaço é um "ambiente" artificial caracterizado por uma complexa e não centralizada rede de emissões e transmissores de informações, composta não apenas pela Internet (rede mundial de computadores), mas também por redes privadas (intranets) e telecomunicações em geral. Utiliza meios físicos (ex: cabos de fibra ótica), wireless e espaciais (satélites). É redundante destacarmos a importância da internet e das outras redes para as economias nacionais e para os governos. O mais importante agora é destacarmos o aumento incessante das transmissões de rede "sem fio"[25] pelo mundo, especialmente após o surgimento de smartphones e tablets.

Emissões eletromagnéticas para comunicação, não importa se seja por rádio, internet ou data link, em termos físicos é a mesma, diferenciando o nível de frequência (bandas) em que ocorre. O ciberespaço e as emissões eletromagnéticas hoje são os principais meios de transmitir informações e conhecimento, sejam elas individuais, coletivas, civis ou militares. Na realidade podemos afirmar que as redes de computadores e de comunicação, no século XXI, tornaram-se a mesma coisa. Há uma ampla convergência tecnológica entre computadores, comunicações, equipamentos eletrônicos, software e criptografia.

O aumento da importância crescente dos sistemas de wireless para a internet trás consequências óbvias para a guerra eletrônica:

> widespread technological convergence between computers, communications, electronic devices and sensors—convergence at both the device level and the supporting infrastructure level— the iPhone has all of these functions. Over time, the infrastructures used for cyber, EW and EMSO will be come indistinguishable—technological convergence is enabling our network assets to become our EW assets, and vice versa.
>
> (....)
>
> These elements result in operational convergence. CyberOps and EMS ops are increasingly drawing on the same capabilities, e.g. both rely on signals intelligence assets and spectrum managers. Inter- dependence is such that CyberOps is essential for integrated EW and EMSO. EW capabilities have utility for attack and defense of platforms, systems and networks. These capabilities are being employed in concert (in very sophisticated combinations) to attain

25 Poissel (2006, p. 191) observa que "there are currently two variations of mobile wireless network. The first is know as infrastructured network, that is, those networks with fixed and wired gateways. The bridges for the networks are known as base stations. A mobile unit within these networks connects to, and communicates with, the nearest base station thai is within its communication radius. (....) The second type of mobile network, commonly know as an ad hoc network. Infrastructureless netwoks have no fixed routers; all nodes are capable of movement and can be connected dynamically in an arbitrary manner".

> necessary objectives. (TRADOC Combined Arms Center, 2010, apud PORCHE et all, 2013, p. 49).

A convergência[26] entre as armas cibernéticas e o aspecto eletromagnético pode ser centrado em outro conceito fundamental da Revolução dos Assuntos Militares (RAM), a guerra centrada em rede.

A abordagem de guerra centrada em rede é quase uma evolução do conceito de sistemas adaptativos complexos que vem da biologia e da computação, e fundamenta-se na ideia de que a guerra é um sistema complexo, onde os diversos atores devem possuir o máximo de informação possível (aprender e adquirir experiência) para se adaptar a novas situações. A expressão Network Centric Warfare, aparentemente, aparece pela primeira vez em meado dos anos 1990. De acordo com Brewin (1997):

> The concept of network-centric warfare took center stage in the Joint Chiefs of Staff's "Joint Vision 2010" paper released in July 1996 by then-chairman of the Joint Chiefs of Staff Gen. John M. Shalikashvili. The document laid out the department's operational concept of joint warfighting and put networks with their ability to disseminate information quickly at the center of military strategy during the next decade.

Em termos mais simples, podemos definir a guerra centrada em rede como uma abordagem de guerra que busca utilizar toda a tecnologia eletromagnética e de rede para conseguir a maior consciência situacional (domínio de informações) no campo de batalha, permitindo maior conhecimento da evolução do conflito e sincronização das ações, e ao mesmo tempo, impedir que o adversário tenha acesso ao seu arsenal de guerra eletrônica e cibernética. Todos os elementos das forças: soldados, navios, aviões, helicópteros, etc... fazem parte desta rede trocando informações em tempo real. A guerra centrada em rede busca o total domínio informacional e cognitivo. Os elementos centrais desta abordagem são: troca de informações através de rede wireless, computadores, criptografia, data link[27], furtividade, detecção antecipada, comando descentralizado e uso de armas inteligentes. A guerra deixa de ser centralizada e hierarquizada para ser integrada.

Os novos riscos a segurança cibernética, advindos do uso intensivo da tecnologia wireless, trazem à guerra eletrônica ameaças antes impensáveis. Em 2014, cientistas da Universidade de Liverpool conseguiram criar um vírus conceito (Chameleon) que pode ser transferido via redes wi-fi abertas, e não mais apenas entre computadores ou por meio físico. Este malware, depois de conectar- se a um ponto, espalhou-se rapidamente por outras redes atacando roteadores coletando informações de seus usuários[28]. Um vírus deste tipo poderia, se direcionado, atacar sistemas de data link contaminando toda uma rede e inviabilizando

26 Na Austrália a guerra eletrônica e a cibernética estão sob responsabilidade do mesmo órgão do Ministério da Defesa, o Cyber and Electronic Warfare Division. http://www.dsto.defence.gov.au/research-division/cyber-and- electronic-warfare-division.

27 O conceito de data link, provavelmente, é o coração da guerra centrada em rede. Seu objetivo é conectar um ponto da rede a outro (navio, avião, etc...) a outro e pode agir de forma unidirecional (quando um transmissor emite um sinal e uma única direção), semi-duplo (emite mais de um sinal a mais de um receptor, mas apenas por vez) e bidirecional (transmite e recebe comunicações ao mesmo tempo de mais de um emissor). Exemplos de data link são o Link 16 (OTAN) e o Link BR (Brasil).

28 http://www.disclose.tv/news/Scientists_demonstrate_first_contagious_airborne_WiFi_virus/100342.

a troca de informações, negando completamente o conhecimento situacional no campo de batalha[29].

A importância das redes de computadores, softwares, a dependência cada vez maior da comunicação wireless e da criptografia para as forças armadas no mundo tem aumentado bastante a zona cinzenta que separava a guerra eletrônica da guerra cibernética. Conceitos antes visto como ambientes completamente diferentes têm sido percebidos, cada vez mais, como partes de uma mesma forma de conceber a guerra. Além disto, a possibilidade da utilização de técnicas de emissão eletromagnética para permitir o roubo de informações em computadores, através de modens e roteadores wi-fi, abre novos desafios à tecnologia de encriptação de dados como os de data link. É claro que, o fato mais importante é a necessidade dos comandantes terem o máximo de informação possível em tempo real, serem capazes de processar esta avalanche de informações e tomar a decisão que acredita ser a mais correta para chegar ao único objetivo que importa, vencer a guerra.

CONCLUSÃO

Este é um texto com um caráter exploratório que tenta em poucas páginas discutir questões complexas. Em face da necessidade de simplificação, muitos conceitos e discussões ficaram de fora deste trabalho. Primeiro, procuramos discutir a relação simbiótica entre tecnologia e guerra, depois seguindo os objetivos que havíamos proposto na introdução, discutir os conceitos de guerra cibernética e guerra eletrônica. No fim, destacamos que estes conceitos estão em um processo de convergência e não podem mais ser pensados como dimensões diferentes da guerra. Defende-se que a forma mais clara de demonstrar a necessidade de se repensar esta divisão está no conceito de guerra centrada em rede, provavelmente o fato mais importante do que se tem denominado, apensar de sem muito esclarecimento, de Revolução nos Assuntos Militares (RAM).

29 Talvez das técnicas conceitos mais intrigantes de malware seja o conceito de vírus sônico. Pesquisadores o Instituto Fraunhofer desenvolveram uma técnica capaz de, a partir de ondas sonoras inaudíveis ao ouvido humano, transferir um vírus capaz de a pequenas distâncias transferir pequena quantidade de dados. < http://www.jocm.us/index.php?m=content&c=index&a=show&catid=124&id=600 > Outro fato interessante é o relatado por pesquisadores israelenses de que os computadores "vibram e emitem ruídos" diferentes a cada bit de chave de segurança, o que poderia permitir a quebra da chave privada RSA <https:// nakedsecurity.sophos.com/2013/12/19/the-sound-made-by-your-computer-could-give-away-your-encryption- keys/?utm_source=Naked%2520Security%2520-%2520Feed&utm_medium=feed&utm_content=rss2&utm_campaign=Feed&utm_reader=feedly >. Acessados em junho de 2015

REFERÊNCIAS

AMARANTE, José Carlos A. (2010), "A Batalha Automatizada: um sonho possível?" Cadernos de Estudos Estratégicos, Vol. 09, pp. 03 -19.

. (2003), "O Alvorecer do Século XXI e a Ciência e Tecnologia Nas Forças Armadas". Military Review. Vol. 83, nº 01, pp. 03-18.

ALLINSON, Jamie (2015), "The Necropolis of Drones". International Political Sociology. Vol. 02, pp. 123-127.

ARQUILLA, John e RONFELDT, David (1993). Cyberwar is coming! Santa Monica: Rand Corporation.

BASTOS, Expedito. (2005), "Vietnã - Maioridade da Guerra Eletrônica. < http://www.ecsbdefesa.com.br/fts/Vietn%E3.pdf >, acessado em junho de 2015.

BELLINTANI, Adriana e BELLINTANI, Mauro (2014). A Guerra: do século XIX aos nossos dias. Boa Vista: Editora UFRR.

CASTELLS, Manuel. (2003), A Galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar Editores.

CARR, Jeffrey (2010), Inside Cyber Walfare. Sebastopol: O'Reilly.

CLARKE, Richard e KNAKE, Robert. Cyberwar: the next threat to national security and what to do about it. New York: HarperCollins.

TEIXEIRA, Duda. (2015), "O 7 x 1 dos Espiões Chineses". Revista Veja. Ed. 2340, ano 48.

GAMA NETO, Ricardo e LOPES, Gills. (2014), "Armas cibernéticas e segurança internacional". IN: MEDEIROS FILHO, Oscar; FERREIRA NETO, Walfredo e GONZALES, Selma Lúcia. Segurança e Defesa Cibernética: da fronteira física aos muros virtuais. Recife: Editora da UFPE. GERRS, Kenneth (2011), Strategic Cyber Security. Tallinn: NATO/CCD/COE Publication. GREGORY, Derek (2011), "From a View to Kill: drones and late modern" war. Theory, Cultura & Society. Vol. 28m nº 7-8, pp. 188-215.

MEADOWCROFT, Brian. (2006), "Hydrophones". In: Wordl War I: a student encyclopaedia.

Santa Barbara: ABC-CLIO.

NYE JR, Joseph. "Nuclear Lessons for Cyber Security?" Strategic Studies Quarterly, Vol. 5, nº 04,p 18-37, pp. 18-38.

POISSEL, Richard A. (2006), Information Warfare and Electronic Warfare Systems. Norwood: Artech House.

PORSHE, Isaac et all (2013), Redefining Information Warfare Boundaries for an Army in a Wireless World. Santa Monica: RAND Corporation.

REED, Thomas. (2005), At the Abyss: An Insider's History of the Cold War. Presidio Press. RICHARDSON, Doug (1991), Guerra eletrônica: guia das armas de guerra. São Paulo: Nova Cultural.

SANTOS, Gabriel Augusto. "Novo Ano, Novos Desafios: Ciberataques e Ciberdefesas". Revista Militar. nº 2496, janeiro de 2010. http://www.revistamilitar.pt/artigo.php?art_id=533. Acessado em junho de 2015.

SARKAR, Tapan et all (2006), History of Wireless. New Jersey: Wiley - Interscience.

SINE, Jack. (2006), "Definir 'Arma de Precisão' em Termos de Basear-se em Feitos. Air & Space Power. 4º Trimestre. < http://www.airpower.maxwell.af.mil/apjinternational/apj-p/

2006/4tri06/sine.html >

UNITED STATES ARMY. (2014), Cyber Eletromagnetic Activities. FM 3-38. < http:// armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_38.pdf >, acessado em junho de 2015.

VAN LENTE, Harro e RIP, Arie (1988),. "Expectations in Technological Developments: an example of prospective structures to be filled in by agency". In: DISCO, Cornelis e VAN DER MEULEN, Barend. Getting New Technologies Together: studies in making sociotechnical order. Berlin: De Gruyter.

VAN CREVELD, Martin. (2010), Technology and War: from 2000 BC to the present. New York: Free Press.

WALTZ, Kenneth N. (1988), "The Origins of War in Neorealist Theory". Journal of Interdisciplinary History, vol. 18, nº 04, pp. 615-628.

UNIVERSIDADE
FEDERAL
DE PERNAMBUCO

CFCH

CENTRO DE FILOSOFIA E
CIÊNCIAS HUMANAS

Departamento de
Ciência Política

Programa de Pós-Graduação
em Ciência Política