

A Guerra Moderna e suas transformações: da 1ª geração à guerra cibernética e o impacto na segurança internacional ¹

Mariana Maia Ruivo

“Em um momento anterior, um comandante pode ter certeza de que uma futura guerra seria semelhante às passadas e atuais. Isto permitiu-lhe analisar táticas apropriadas do passado e do presente. O comandante da tropa de hoje não tem mais essa possibilidade. Ele sabe apenas que quem não consegue se adaptar as experiências da última guerra certamente irá perder a próxima.” Gen. Franz Uhle-Wetter”

Resumo

Desde a Segunda Guerra Mundial podemos verificar mudanças significativas na natureza da guerra e, forçando as Forças Armadas ocidentais a se adaptarem aos novos paradigmas. Há uma corrente entre os estudiosos da guerra que defendem a ideia do surgimento de um ‘nova guerra’, onde suas características fundamentais estariam sujeitas a mudanças. Mary Kaldor (2006) defende a ideia de que, com o fim da Guerra Fria, chegou ao fim, também, a guerra entre os Estados e surgiu um novo conflito, caracterizado por contendas civis. Clausewitz, além de mostrar que a guerra é a continuação da política por outros meios, apresenta que se a guerra for observada de forma abstrata, como um conflito entre forças ‘que não obedecem a lei alguma que não seja a sua própria’, a natureza recíproca da violência conduz inevitavelmente a extremos, a medida que dois oponentes tentam obter a vantagem. Tomando como base os autores William Lind e Thomas Hammes que desenvolveram uma teoria da ‘nova guerra’, a história da guerra progrediu por várias fases – nomeadas como gerações – distintas e que, atualmente, o mundo estaria vivendo a Guerra de Quarta Geração. Assim, a tecnologia permitiria que os Estados enfrentassem oponentes elusivos e, talvez, materialmente inferiores, como a guerrilha e o terrorismo. Com o advento de novas tecnologias e de novos atores (não –estatais), os autores chineses Liang e Xiangsui (1999), defendem que a guerra cibernética será a forma básica de guerra futura. Assim, o texto a ser apresentado

¹ Trabalho preparado para apresentação no IV Seminário Discente da Pós-Graduação em Ciência Política da USP, de 07 a 11 de abril de 2014.

procurará dar uma breve introdução sobre as gerações da guerra – da 1ª a 3ª geração -, buscando entender o advento da guerra de 4ª geração, principalmente, a ciberguerra.

Palavras – chave: Guerra – Geração – Guerra Cibernética

Introdução

Desde a Segunda Guerra Mundial podemos verificar mudanças significativas na natureza da guerra e, forçando as Forças Armadas ocidentais a se adaptarem aos novos paradigmas. Há uma corrente entre os estudiosos da guerra que defendem a ideia do surgimento de uma ‘nova guerra’, onde as características fundamentais da guerra estariam sujeitas a mudanças. Mary Kaldor (2006) defende a ideia de que, com o fim da Guerra Fria, chegou ao fim, também, a guerra entre os Estados e surgiu um novo conflito, caracterizado por contendas civis.

Clausewitz, além de mostrar que a guerra é a continuação da política por outros meios, apresenta que se a guerra for observada de forma abstrata, como um conflito entre forças ‘ que não obedecem a lei alguma que não seja a sua própria’, a natureza recíproca da violência conduz inevitavelmente a extremos, a medida que dois oponentes tentam obter a vantagem. Segundo ele,

A guerra, então, não é apenas um verdadeiro camaleão, que modifica um pouco a sua natureza em cada caso concreto, mas é também, como fenômeno de conjunto e relativamente às tendências que nela predominam, uma surpreendente trindade em que se encontra, antes de mais nada, a violência original do seu elemento, o ódio e a animosidade, que é preciso considerar como um cego impulso natural, depois, o jogo das probabilidades e do acaso, que fazem dela uma livre atividade da alma, e, finalmente, a sua natureza subordinada de instrumento da política por via da qual ela pertence à razão pura. (2010: 30)

Há 25 anos, quatro oficiais do Corpo de Fuzileiros, juntamente com um analista militar civil escrevem desenvolveram uma teoria da ‘nova guerra’. De acordo com eles, a história de guerra progrediu por várias fases – nomeadas como gerações – distintas e que

o mundo estaria vivendo a Guerra de Quarta Geração. Essa nova guerra daria início a um período em que os exércitos convencionais de Estados-Nação seriam cada vez mais desafiados por atores não estatais, como a guerrilha e grupos terroristas, usando uma combinação de táticas letais e não-letais que seria cada vez mais difícil para as forças convencionais para combater, mesmo com a tecnologia mais avançada.

Teórico e historiador militar Martin Van Creveld foi ainda mais longe em 1990, quando ele previu que os atores não estatais armados acabariam com o monopólio da violência apreciado por Estados-nação desde a Paz de Westphalia, que pôs fim à Guerra dos Trinta Anos. Este correu em face dos resultados da Primeira Guerra do Golfo (Operação Tempestade no Deserto) em que a tecnologia se tornou um papel dominante e foi anunciado como dando início a uma revolução nos assuntos militares que prometiam ser a verdadeira próxima geração de guerra centrada em maravilhas tecnológicas, tais como ataque de precisão e vigilância aérea.

Com o advento de novas tecnologias e de novos atores (não –estatais), os autores chineses Liang e Xiangsui (1999), defendem que a guerra cibernética será a forma básica de guerra futura. Assim, esse texto procura dar uma breve introdução sobre as gerações da guerra – da 1ª a 3ª geração -, buscando entender o advento da guerra de 4ª geração e a ciberguerra.

A Guerra e suas gerações: da 1ª a 3ª geração

A Guerra de 1ª Geração teve início no Tratado de Paz de Westphalia², em 1648 e vai até 1860. Tem como principal característica o emprego do “Princípio da Massa”³,

2

Acordo firmado em 1648, designa uma série de tratados que deu fim à Guerra dos Trinta Anos. Além disso, deu início ao Sistema Internacional ‘moderno’, ao acatar – por meio de consenso – noções e princípios como soberania nacional e o de Estado Nação.

3

Para maiores informações, ver: *Introduction to the Principles of War and Operations*, texto publicado pela Universidade de Cincinnati. Disponível em: http://www.uc.edu/armyrotc/ms2text/MSL_201_L02b_Intro_to_Principles_of_War_and_Operations.pdf

onde o intuito é a concentração do potencial de combate no local e na hora decisivos. Além disso, essa foi uma guerra de linha e coluna táticas, com batalhas formais, campos de batalhas lineares em frente e profundas, razoavelmente ordenadas e estruturadas. Há destinação entre ‘militar’ e ‘civil’ era bem clara, como, por exemplo, o uso de uniformes e com um reforço da cultura da ordem. O ápice da Guerra de 1ª Geração fora as campanhas napoleônicas.

De acordo com Lind (1989), em meados do século XIX, o campo de batalha começou a quebrar e se tornou um problema. Exércitos de massa, soldados, mosquetes raiados, e em seguida, carregadores de culatras e metralhadoras, fizeram das táticas de linha e de primeira coluna obsoletas e, então, suicida. Assim, o problema desde então, tem sido uma crescendo contradição entre a cultura militar e a crescente desordem no campo de batalha. A cultura da ordem que já foi coerente com o ambiente em que operava tornou-se cada vez mais em desacordo com ele.

E, foi a partir dessa contradição que surge a Guerra de 2ª Geração, no período de 1860 à I Guerra Mundial. Desenvolvido pelo exército francês durante e após a Primeira Guerra Mundial, ele buscou uma solução no poder de fogo em massa, a maioria dos quais era fogo de artilharia indireta. O objetivo principal era o atrito, e a doutrina foi resumida pelos franceses como ‘a artilharia conquista, a infantaria ocupa’. Armas e equipamentos foram criados e/ou aperfeiçoados, em especial o canhão, o fuzil e a metralhadora, resultando numa supremacia do fogo sobre o movimento. O poder de fogo foi centralmente controlado e cuidadosamente sincronizado, utilizando detalhes, planos e ordens específicas, para a infantaria, a artilharia e os tanques, como em uma ‘batalha conduzida’ onde o comandante poderia, de acordo com Lind, ser comparado à um maestro de uma orquestra.

Para Paiva, essas guerras, que são classificadas como de 2ª geração, “os procedimentos eram rígidos e a disciplina prevalecia sobre a iniciativa” (2010: 82). Ou seja, havia uma preocupação com o método de planejamento e as normas de condução das operações, limitando a criatividade pela busca de soluções diferentes e comprometendo a obtenção dos resultados/objetivos desejados. Assim, continua o autor, a “guerra era estática e de atrito. O atacante ‘empurrava a linha’ e o defensor ‘segurava a

linha’, pois não havia mobilidade para envolver e cercar” (2010:83). Foi, nesse período, também, que começaram a surgir os blindados e a aviação, que levou à uma nova geração da guerra moderna.

Assim, tem início à Guerra de 3ª Geração, e o mundo enfrenta à II Guerra Mundial(além das três primeiras guerras árabe-israelense, Coréia e a *Desert Storm*) . Foi resultado da I Guerra Mundial e foi desenvolvida pelo exército alemão, sendo comumente conhecido como *Blitzkrieg* ou guerra de manobra. Portanto, a força motriz foi principalmente das ideias. Caracterizou-se, principalmente, pelo uso de manobras, tanques, aviões, e poder de fogo pesado. Conscientes de que não tinham uma indústria bélica forte, por causa da I Guerra os alemães desenvolveram táticas radicalmente novas. Esse tipo de guerra tem como base a velocidade, surpresa e o mental, além do deslocamento físico, e não apenas no poder de fogo e do atrito, como anteriormente. Segundo Lind, taticamente, no exército de 3ª Geração, busca entrar na retaguarda do inimigo e, assim, recolhê-lo trás para frente: em vez de ‘ fechar com e destruir’, o lema é ‘desviar e entrar em colapso’.

A guerra deixa de ser um concurso de empurrar, onde as forças tentam segurar ou avançar em uma linha, pois a guerra de 3ª geração não foi linear, buscou-se a aproximação indireta, conforme descrita pelo estrategista Liddell Hart, ao invés de procurar o atrito direto para sua destruição. Assim, a Guerra de Manobra (ao contrário da Guerra de Atrito), visa incapacitar sistematicamente o seu sistema de combate, com a obtenção de uma posição vantajosa e, não mais, buscando ir ao encontro conflito direto. Além das mudanças nas táticas, há também na cultura militar. Um militar dessa geração se concentra para o exterior, sobre a situação, o inimigo e o resultado que a situação exige. Compreender a situação do comandante passou a ser fundamental, o que significava ter liberdade de ação e iniciativa para o subordinado poder adaptar planejamentos e eventuais oportunidades. Ou seja, quando se fala de planejamento e de batalha, a maior preocupação recaía sobre o objetivo e não mais sobre o processo.

Guerra Assimétrica e a Guerra de 4ª Geração

Se o inimigo tiver sua vontade de lutar afetada, então sua capacidade militar, sem importar quão poderosa seja, passa a ser relevante.

Se pensarmos na guerra antes do século XVIII, ficava muito claro que ela ocorria entre dois ou mais estados nacionais, sob o comando de realezas e, normalmente, como bem destacou Maquiavel, eram conduzidas por exércitos de mercenários. Mas, o ato de guerrear mudou muito, principalmente durante o século XX e, inclusive, agora no século XXI. Atualmente, podemos classificar a guerra em quatro tipos diferentes: a guerra convencional; a guerra de destruição em massa; a guerra irregular e a guerra assimétrica.

A guerra convencional ou guerra regular é aquela que é travada entre exércitos, com Estados organizados e estáveis e uma clara separação entre civis e soldados. Sua maior característica é o conflito entre Estados. Após a II Guerra Mundial e durante a Guerra Fria, a grande ameaça eram as armas de destruição em massa. Apesar de ter passado muitos anos, sua imagem – em especial sua vertente nuclear – influenciou na necessidade de requerer diferentes planejamentos estratégicos, armamentos, organizações de unidade e, o que não é menos importante, um diferente treinamento dos oficiais e suas unidades. Porém, hoje, mais do que nunca, fica claro que uma nova guerra com armas de destruição em massa parece ser improvável. Mas, engana-se quem acredite que o que foi apresentado em Hiroshima e Nagasaki tenha colocado fim à ‘arte de guerrear’. Pelo contrário, enfatizou e motivou outros tipos de guerra.

A maioria dos conflitos após a II Guerra Mundial foi de conflitos armados que geraram uma série de guerras ‘irregulares’, como terrorismo, guerrilha, insurreição, movimentos de resistência e conflitos assimétricos em geral. Interessante ressaltar que esse tipo de guerra não deixa claro das definições de campo de batalha, uniformes ou divisões territoriais, assim como, a diferença entre civis e soldados. Assim, a guerra irregular foi progressivamente substituindo as guerras convencionais.

Após os atentados classificados como terroristas sofridos pelos Estados Unidos em 11 de setembro de 2001, além de mudanças na agenda de política de defesa dos países, há também o surgimento de um novo tipo de guerra, a guerra assimétrica. De acordo com Costa, “Guerra assimétrica,” talvez pudesse ser definida, como foi dito, de guerra irregular em escala mundial, ou como a guerra irregular, que não se cinge a um

espaço nacional.” (s/d: 04) Esse novo tipo de guerra foi denominada de Guerra de Quarta Geração e, pelos coronéis chineses Liang e Xiangsui como a Guerra além dos Limites, onde propõem que para se chegar à vitória nesse tipo de guerras, os meios empregados na condução da guerra transcendem as atividades militares e,

(...) deverá “combinar” todos os recursos de guerra à sua disposição e utilizá-los como meios para a condução da guerra. E até mesmo isso não será suficiente. Ele terá de combinar aqueles recursos de acordo com as exigências das regras da vitória. (1999: 205)

Dessa forma, Liang e Xiangsui afirmam que a Guerra Assimétrica pode se manifestar das seguintes formas: guerra psicológica; guerra econômica; guerra com armamento usual; guerra radiológica, nuclear ou radioativa; guerra biológica, bacteriológica ou virótica; guerra cibernética, eletrônica ou informática; e guerra química. Tendo em vista que nesse tipo de conflito se busca é, também, atingir a moral do adversário, a guerra psicológica é preponderante.

A guerra de 4ª Geração é resultado de uma evolução que visa tirar vantagem das mudanças, ocorridas desde a última grande guerra, política, social, econômica e tecnológica. Junto aos Estados, surgem novos protagonistas, como as organizações não estatais armadas- como a Al-Qaeda, o Hamas, o Hezbollah e, aqui na América do Sul, as FARC -, forças irregulares de diferentes matrizes: separatistas, anarquistas, extremistas políticos, étnicos ou religiosos, crime organizado e outras, sendo a principal forma de atuação tem como base as táticas, técnicas e procedimentos da guerra irregular. Dessa forma, o Estado perde o monopólio da guerra.

A Guerra de Quarta Geração (4GW) exige muito mais inteligência, análise e maior capacidade de disseminação para servir a um sistema de comando altamente flexível. Ela engloba elementos de gerações de guerra anteriores; tal fato exige que nossas forças estejam preparadas para lidar com mais esse aspecto. Neste sentido, é fundamental que os líderes façam uma análise apurada da guerra que estão prestes a entrar. Esta complexa mistura de gerações de guerras e a sobreposição de suas arenas políticas, econômicas, sociais, militares e de meios de massa dificultam, mais

do que nunca, a determinação do tipo de guerra que estamos entrando. (Cel T.X. Hammes, USMC, “The Evolution of War: The Fourth Generation”)

Há quatro ideias centrais para entender a guerra 4ª Geração. A primeira está na dimensão do campo de batalha, que inclui toda a sociedade inimiga. A segunda ideia é uma decrescente dependência na logística centralizada. A terceira é uma maior ênfase na guerra de manobra, em que ‘apenas’ o efetivo da tropa e o poder de fogo não serão mais fatores de vantagem esmagadora. A quarta e última ideia está pautada na destruição da capacidade interna de coesão do inimigo; em vez de destruí-lo fisicamente.

A doutrina militar dos Estados Unidos aponta para quatro formas prováveis de guerra no futuro: Guerra Cibernética, Guerra de Precisão, Operações Combinadas e as *Military Operations Other than War* - MOOTW⁴. Essa última provável guerra abrange uma série de operações em que os militares são empregados, porém, não são, necessariamente, os protagonistas da operação.

A Guerra do futuro: Ciberguerra

“Cyberwar está vindo!”, declarou o título de um artigo, de 1993, escrito pelos analistas da Rand Corporation, John Arquilla e David Ronfeldt, que argumentaram que a Internet nascente iria transformar a guerra de forma radical. Na época, a ideia parecia fantasiosa, levando mais de uma década para que os responsáveis pela segurança nacional dos EUA aceitasse a ideia de um novo tipo de guerra. Em fevereiro de 2011, o então diretor da CIA, Leon Panetta, advertiu, em audiência no Congresso, que “o próximo Pearl Harbor poderia muito bem ser um ataque cibernético⁵”. E no final de 2012, Mike

4

Para maiores informações, ver: http://www.bits.de/NRANEU/others/jp-doctrine/jp3_07.pdf e <http://www.operationalstudies.com/mootw/>

⁵ Leon Panetta – Why He Matters - http://www.washingtonpost.com/politics/leon-panetta/gIQAQNAq90_topic.html e <http://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905>

McConnell, que serviu como diretor da inteligência nacional na gestão do presidente George W. Bush, advertiu sombriamente que os Estados Unidos não poderia "esperar o equivalente cibernético do colapso dos World Trade Centers".

Tomando base a ideia de Liang e Xiangsui (1999), a guerra cibernética será a forma básica de guerra futura. A grande revolução tecnológica vem transformando a maneira como as sociedades modernas se inter-relacionam. Num contexto de beligerância entre os Estados ou entre atores estatais e não-estatais, a exploração das redes de computadores constitui uma eficiente maneira para obtenção de vantagens; e, em um contexto militar, a exploração dos sistemas de informação computadorizados pode levar a uma superioridade no 'campo de batalha'.

Há uma falta de consenso entre vários autores para uma definição fechada sobre ciberguerra. O governos dos Estados Unidos define como "o ambiente teórico em que informação digitalizada é comunicada sobre redes de computadores"⁶ (tradução da autora). E, também pode ser definida como

O uso premeditado de atividades perturbadoras, ou ameaça, contra computadores e / ou redes, com a intenção de causar danos sociais, ideológicos, religiosos, políticos ou similares. Ou para intimidar qualquer pessoa em prossecução de tais objetivos."⁷ (tradução da autora)

Dessa forma, a definição que mais deixa clara e concisa o que é uma ciberguerra é de Parks e Duggan, onde, segundos os autores, a guerra cibernética pode ser entendida como

6

Disponível em: <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-023.pdf>

7

Cyber Operations and Cyber Terrorism, Handbook Number 1.02", US Army Training and Doctrine Command, Deputy Chief of Staff for Intelligence, Assistant Deputy Chief of Staff for Intelligence – Threats, Fort Leavenworth, Kansas, 15 August 2005., p. II-2.

(..) o sub-conjunto da guerra da informação que envolve ações realizadas no mundo cibernético. O mundo cibernético é qualquer realidade virtual compreendida numa coleção de computadores e redes. Existem diversos mundos cibernéticos, mas o mais relevante para a Guerra Cibernética é a Internet e as redes a ela relacionadas, as quais compartilham mídia com a Internet. A definição militar mais próxima para o nosso termo, guerra cibernética, é uma combinação de ataque e defesa de redes de computadores, e possivelmente, operações especiais de informação. Nós definimos guerra cinética como sendo a guerra praticada no “mundo real”. Todos os tanques e navios e aviões e soldados tradicionais são os protagonistas da guerra cinética. (2001:122) (tradução da autora)

Dessa forma, um ataque bem-sucedido nas redes dos sistemas que gerenciam e controlam serviços dos Estados e da sociedade civil, gera insegurança, pânico e incerteza em relação à real situação do conflito. Entre os serviços que podem ser atingidos, estão as redes de telecomunicações, de energia elétrica, redes de saúde pública, emergência e água potável e a rede do sistema financeiro.

O poder cibernético é único, pois é feito pelo homem, é recente e está sujeito a mudanças tecnológicas ainda mais rápidas do que outros domínios. O conflito extremo na guerra cibernética também é diferente. No mundo físico, os governos têm quase o monopólio do uso da força em larga escala, o defensor tem conhecimento íntimo do terreno, e os ataques terminam devido ao desgaste ou à exaustão. Porém, no mundo virtual, os atores são diversos, às vezes anônimos; a distância física é imaterial e um único ataque virtual é praticamente, gratuito⁸.

Porém, apesar de ser referenciada como a grande ameaça do século XXI, Thomas Rid descreve os ciberataques como algo separado da guerra convencional, porque eles não conseguem atender todas as três definições de Clausewitz da guerra como violenta, instrumental, e atribuível a um lado como uma medida tomada para um objetivo político.

⁸ LTC David E. A. Johnson & STEVE Pettit, 2010. P. 17

Por isso, segundo Rid, "ciberguerra nunca aconteceu no passado, não está ocorrendo no presente, e é altamente improvável que ele irá perturbar o futuro." Mas seu argumento é uma representação simplificada das complexas realidades da guerra e segurança hoje e suas ligações inerentes ao ciberespaço.

Hoje, o mundo está tão imerso na tecnologia que as atividades no ciberespaço tornou-se inseparável das operações diárias de negócios, educação, governo e dos militares. Ações *on-line* afetam as ações *off-line*, e vice-versa. Assim, longe de ser separada da guerra convencional, a ciberguerra está profundamente enraizada em práticas militares contemporâneas. De fato, a ciberguerra, faz parte da evolução da guerra convencional, que se está ligado à uma mudança social e político mais ampla. Não é mais fácil imaginar um confronto que não inclui algum elemento de cyber-atividade, como a vigilância ou sabotagem. Perguntar se ciberguerra é real, então, é menos importante do que se concentrar em como conter as ameaças representadas por alguns usos da tecnologia informática. Afinal de contas, um ataque cibernético não precisa matar alguém ou causar grandes danos materiais e, ainda será considerado perigoso.

Em contraponto, o pesquisador finlandês, Jarno Limnéll, argumenta que as atividades no ciberespaço são uma parte inerente da guerra convencional, e que o impacto psicológico, não apenas a violência física, de ciberataques é de extrema importância. Limnéll chama a atenção para uma potencial corrida armamentista no ciberespaço. Se ter um comando cibernético torna-se um símbolo de poder, outros países vão querer ter seus próprios comandos cibernéticos. Alguns países, entre eles o Reino Unido, já estão considerando planos de recursos significativos em ofensivas cibernéticas capacidades, desnecessariamente se preparando para uma guerra cibernética que pode nunca ocorrer.

Finalmente, segundo Limnéll, a ideia de criar um comando independente cibernético ignora o fato de que as capacidades ofensivas não se traduzem em melhores meios defensivos. Muitas armas convencionais podem ser usadas de forma defensiva ou ofensiva. Mas, completa, armas cibernéticas são diferentes; Stuxnet⁹, por exemplo,

⁹ O Stuxnet é um worm de computador projetado especificamente para atacar o sistema operacional SCADA da Siemens, que seria responsável pelo controle das centrífugas de enriquecimento de urânio do Irã. Foi descoberto em 2010, por uma empresa bielorrússia, sendo o primeiro worm que espiona e

poderia ser usado apenas ofensivamente. Outro bom exemplo são os sistemas de computadores dos EUA: é só procurar por Edward Snowden, o ex-empregado NSA quem vazou informações confidenciais sobre essas vulnerabilidades. Os mais sofisticados ciberataques são altamente segmentados e armas cibernéticas são susceptíveis de causar danos colaterais da mesma forma que armas convencionais. Portanto, em muitas situações, a utilização de computadores seria preferível a utilização de armas convencionais: um ataque virtual pode ser menos violento, menos traumatizante, e mais limitada.

Essas transformações cibernéticas extremas ainda são estranhas, mas uma nova Revolução da Informação está mudando a natureza do poder e aumentando sua difusão. De acordo com Nye, "os Estados continuarão sendo os atores dominantes no palco mundial, mas encontrarão o palco bem mais povoado e difícil de controlar" (2012: 152). Além disso,

(...) o espaço cibernético não vai substituir o espaço geográfico nem abolir a soberania do Estado, mas, como os mercados das cidades nos tempos feudais, vai coexistir e complicar muito o conceito de Estado soberano ou de país poderoso no século XXI. (2012: 161)

Considerações finais

"Uma guerra furiosa pelo futuro da sociedade está em andamento. Para a maioria, essa guerra é invisível". Julian Assange

As ideias e a tecnologia forçaram mudança ao longo da história, como os caminhos humanos e o ato de guerrear. Essa mudança perpétua acelerou grandes mudanças geopolíticas e, com a queda da União Soviética, pôs fim a um mundo bipolar. No contexto da revolução da tecnologia de informação, cada vez mais rápida, surge um novo conceito de guerra, a de 4ª Geração.

reprograma sistemas industriais. Um *worm*, traduzindo para o português como verme, é um programa, autorreplicante que se assemelha a um vírus, mas se diferencia por ser um programa completo e não necessita de outro para se propagar.

Apesar das incertezas do amanhã, a guerra continuará a existir e, que provavelmente, os princípios da guerra de 4ª Geração poderão se tornar regra no conflito no século XXI. O mundo já presencia e continuará a presenciar guerras entre atores estatais e não-estatais, guerras assimétricas, sem regras e sem princípios. Em contrapartida, essas guerras da Era da Informação serão marcadas pelo emprego de um novo tipo de Força Armada, possuidora de tecnologias cada vez mais avançadas e com a utilização do ciberespaço. Assim, a guerra cibernética passa a ser considerada como uma variação da guerra assimétrica.

O domínio cibernético é ao mesmo tempo um ambiente novo e volátil criado pelo homem. As características do espaço cibernético reduzem alguns dos diferenciais de poder entre os atores e, portanto, proporcionam um bom exemplo da difusão de poder que caracteriza a política global neste século. É improvável que as maiores potências sejam capazes de controlar esse domínio da mesma maneira que têm controlado outros, como mar ou o ar.

Pouco tem sido escrito a respeito da utilização do ciberespaço em conjunto, por exemplo, com os ataques efetuados pelos drones. A programação dessas armas, a operação a distância e o seu projeto são, todos, permeados pelo espaço cibernético, e não é raro que brote na imprensa especulações de que hackers podem invadir, em algum momento, os sistemas de guiagem e operação dos VANTs (Veículo Aéreo Não Tripulado)

É possível que a guerra cibernética crie alguns deslocamentos de poder entre os Estados, abrindo oportunidades limitadas para grandes saltos por parte de Estados pequenos e por atores não estatais, pelo uso de guerra assimétrica. Entretanto, embora deixando os governos permanecerem como os atores mais fortes, o domínio cibernético pode ver um aumento na difusão de poder para atores não estatais e a centralidade da rede como uma dimensão fundamental do poder no século XXI.

Finalmente, a tecnologia do ciberespaço, em conjunto com outras tecnologias aplicadas ao setor bélico, tem feito com que a discussão em torno da própria guerra tenha sofrido modificações até então impensáveis. No caso norte-americano, Singer observa que o avanço tecnológico tem sido tão intenso que ataques e intervenções com

possibilidades de destruir instalações e países inteiros tem sido possíveis com o pouco emprego de soldados de carne e osso.

Referências bibliográficas

ASSANGE, Julian. **Cypherpunks – liberdade e futuro da internet**. São Paulo: Boitempo, 2013

COSTA, Darc. Visualizações da Guerra Assimétrica. Centro de Estudos Estratégicos. Disponível em: <http://www.esg.br/uploads/2009/03/darc7.pdf>

CLAUSEWITZ, Carl Von. **Da Guerra**. São Paulo: Ed. WMF Martins Fontes, 2010.

CLARKE, Richard. Cyber War: The Next Threat to National Security and What to Do About It. **Kindle Edition. (Amazon)**

CREVELD, Martin Van. **The Changing face of War – lessons of combat, from the marnet to Iraq**. New York: Ballantine Books, 2006

_____. **The transformation of War – the most radical reinterpretation of armed conflict since Clausewitz**. USA: The Free Press, 1991

Cyber Operations and Cyber Terrorism, Handbook Number 1.02”, US Army Training and Doctrine Command, Deputy Chief of Staff for Intelligence, Assistant Deputy Chief of Staff for Intelligence – Threats, Fort Leavenworth, Kansas, 15 August 2005.

ECHEVARRIA II, Antulio J. “ Fourth-generation war and other myths”. United States: Strategic Studies Institute. Novembro 2005.

Introduction to the Principles of War and Operations. Texto publicado pela Universidade de Cincinnati. Disponível em: http://www.uc.edu/armyrotc/ms2text/MSL_201_L02b_Intro_to_Principles_of_War_and_Operations.pdf

HAMMES, T.X. “A Guerra de Quarta Geração evolui, a Quinta emerge”. In: Military Review. Setembro-Outubro, 2007.

_____. “The Evolution of War: The Fourth Generation”. Setembro 1994.
Disponível em: http://www.zoklet.net/totse/en/politics/us_military/162582.html

HOBSBAWM, Eric. **Era dos Extremos – o breve século XX (1914 – 1991)**. São Paulo: Companhia das Letras, 1995.

HOWARD, Michael. **The causes of wars**. USA: Harvard University Press: 1983.

KALDOR, Mary. **New and Old Wars – organized violence in a global era**. (Second Edition) Cambridge: Stanford University Press: 2006

KOLTUKSUZ, Ahmet. “The Information Warfare, Cyber Warfare and Open Sources Intelligence: An Interdisciplinary Approach”. An Intensive Program Proposal for Spring/Summer of 2012 – Disponível em: <http://tdd.aa.u.gr/sites/default/files/Information%20Warfare%20Open%20Source%20Intelligence.pdf>

LIANG, Qiao & XIANGSUI, Wang. “A Guerra além dos limites: conjecturas sobre a guerra e a tática na era da globalização”. Beijing: PLA Literature and Arts Publishing House. Fevereiro 1999 - Disponível em: <https://www.egn.mar.mil.br/arquivos/cepe/GUERRAALEMLIMITES.pdf>

LIND, William S., The changing face of war: Into the Fourth Generation. 1989. Disponível em: <http://www.mca-marines.org/files/The%20Changing%20Face%20of%20War%20-%20Into%20the%20Fourth%20Generation.pdf>

LTC David E. A. Johnson & STEVE Pettit. “Principles of the defense for cyber networks. Defense Concept, 4, n° 2 (jan.2010). Disponível em: http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf

MILLS, C. Wright. **As causas da próxima guerra mundial**. Rio de Janeiro: Zahar Editores, 1961

Military Operations Other than War – MOOTW – Disponível em:

http://www.bits.de/NRANEU/others/jp-doctrine/jp3_07.pdf e <http://www.operationalstudies.com/mootw/>

NATO – OTAN: Defending the networks. Disponível em:
http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf

NYE, Joseph S. **O futuro do poder**. São Paulo: Benvirá, 2012

OLIVEIRA, Flávio Rocha & WAHL, Bernardo. Cibersegurança e Ciberguerra – o governo Obama e a Política de Defesa no Espaço Cibernético. Trabalho apresentado no VII Encontro da Associação Brasileira de Estudos de Defesa – ABED, 2013.

PAIVA, Luiz Eduardo Rocha. “Guerras de Quarta Geração ou mais uma falácia travestida de sapiência?” In: JOBIM, Nelson; ETCHEGOYEN, Sérgio e ALSINA, João Paulo. **Segurança Internacional: Perspectivas brasileiras**. Rio de Janeiro: Editora FGV: 2010

PANETTA, Leon. Why He Matters. Disponível em: -
http://www.washingtonpost.com/politics/leon-panetta/gIQAQNAg90_topic.html e
<http://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905>

PARKS, R. & DUGGAN, David. “Principles of Cyber-warfare”, Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 5-6 June, 2001. Disponível em:
http://www.periwork.com/peri_db/wr_db/2004_May_11_11_30_41/DOCS%20WEBREVIEW/PrinciplesCYBER%20WARFARE.pdf

PINHEIRO, Alvaro de Souza. “O Conflito de 4ª Geração e a Evolução da Guerra Irregular”. Rio de Janeiro, Padece-me, 3º quadrimestre, 2007. N° 16.

RID, Thomas. “Think again: Cyberwar”. **Foreign Affairs**, 2012. Disponível em:
<http://www.foreignpolicy.com/articles/2012/02/27/cyberwar>

_____. “Cyberwar and Peace”. **Foreign Affairs**, 2013. Disponível em:
<http://www.foreignaffairs.com/articles/140160/thomas-rid/cyberwar-and-peace>

SINGER, Peter. “Interview with Peter Singer”. **International Review of The Red Cross**. Volume 94 / Issue 886 / June 2012, pp 467 481

TOWNSHEND, Charles (ed.) **The Oxford Illustrated History of Modern War**. Oxford: Oxford University Press, 1997.

