# A Ciberguerra É Moderna! Uma Investigação sobre a Relação entre Tecnologia e Modernização na Guerra*[1]

**Luisa Lobato** e Kai Michael Kenkel*****

## Introdução

Há certo elã quando nós, sujeitos modernos, falamos sobre tecnologia. Ela não apenas é o fruto do desenvolvimento científico mais recente: a tecnologia povoa e alimenta o imaginário do indivíduo mais cético. E a ciência da cibernética não escapa a este fascínio tipicamente moderno. O exemplo mais cabal disso no âmbito dos estudos de segurança internacional é a projeção adquirida pelo fenômeno da ciberguerra nas últimas duas décadas.

* Artigo recebido em 29 de dezembro de 2014 e aprovado para publicação em 13 de março de 2015. Luisa Lobato reconhece o suporte do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq). Kai Michael Kenkel agradece o generoso apoio do CNPq e da Fundação de Amparo à Pesquisa do Estado do Rio de Janeiro (FAPERJ).

** Mestranda em Relações Internacionais pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio), Rio de Janeiro, RJ, Brasil. E-mail: l.cruzlobato@gmail.com.

*** Professor e coordenador do Programa de Pós-Graduação em Relações Internacionais do Instituto de Relações Internacionais da Pontifícia Universidade Católica do Rio de Janeiro (IRI /PUC-Rio), Rio de Janeiro, RJ, Brasil. E-mail: kenkel.iri@gmail.com.



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

A inserção da ciberguerra como tema de segurança internacional foi impulsionada por ataques cibernéticos, atribuídos à Rússia,[2] responsáveis por tirar do ar serviços de comunicação críticos da Estônia, em 2007, e da Geórgia, em 2008 (CLARKE; KNAKE, 2012). Referidos eventos também tornaram possível a inclusão do tema nas agendas da Organização do Tratado do Atlântico Norte (OTAN) e da Organização das Nações Unidas (ONU), culminando na criação do NATO Cooperative Cyber Defence Centre of Excellence, sediado na Estônia. Em 2010, o assunto ganhou projeção na mídia após a descoberta do *worm* Stuxnet, um *malware* que atingiu os sistemas de uma instalação nuclear iraniana. Embora sem causar perdas significativas, o Stuxnet foi suficiente para reviver os cenários de catástrofes virtuais imaginados ainda na década de 1990 (FARWELL; ROHOZINSKI, 2011).

A preocupação principal do presente artigo é investigar o papel da tecnologia na modernidade a partir desse fenômeno conhecido como ciberguerra. Argumentamos que o processo de modernização tem por característica a conjunção entre guerra, ciência e tecnologia, e que a incorporação da cibernética à guerra é representativa disso. Dar robustez a esse argumento central é o objetivo da primeira seção. A segunda seção concorre para dar consistência ao argumento ao investigarmos as condições de possibilidade e os significados que compõem o atual discurso sobre ciberguerra, procedendo a uma genealogia do instituto. Tal movimento permite compreender o papel da cibernética como alicerce no desenvolvimento das práticas de guerra e como tropo capaz de influenciar o imaginário militar a seu respeito. A terceira e última seção se divide em dois momentos. Inicialmente, a ciberguerra é situada no contexto mais amplo das transformações da guerra na modernidade (BOUSQUET, 2009). Argumentamos que o fenômeno representa uma tensão entre dois regimes de guerra, o cibernético e o caospléxico, ao incorporar concepções importantes sobre as teorias do caos e da complexidade e, paralela-



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

mente, apoiar-se na crença no controle sobre o conflito, tendo sido articulada como um meio capaz de reduzir as perdas em combate. Em um segundo momento, o aludido movimento nos permite destacar o papel central da tecnologia no guerrear moderno e, igualmente, problematizar a forma como a ciberguerra se articula ao imaginário de não violência presente nas teorias da modernização (JABRI, 2007; JOAS, 1999).

## 1. Modernidade e Tecnologia: Breves Considerações

Se desejamos compreender o papel da tecnologia, a partir do fenômeno da ciberguerra, na modernidade, é indispensável que investiguemos a relação entre modernidade e tecnologia. Desse modo, é finalidade desta seção investigar, de maneira breve, e compreender (1) o fenômeno da modernidade; e (2) sua inter-relação com ciência e tecnologia na guerra. Todavia, essa investigação não se restringirá à presente seção: ela nos acompanhará do momento em que procedermos à genealogia da ciberguerra à nossa discussão a respeito dos distintos regimes tecnocientíficos de guerra que tomaram forma no curso da modernidade. Diante da vastidão de pesquisas sobre o tema, uma das limitações do presente trabalho é a brevidade com a qual trataremos o fenômeno da modernidade. Não iremos desenvolver uma indagação exaustiva das diversas significações que o termo carrega consigo. Desejamos estabelecer uma ideia geral acerca do que falamos ao invocar o termo "modernidade" e como, no contexto da guerra, só podemos fazer sentido dela se levarmos em consideração sua relação com o desenvolvimento tecnológico e a centralidade da ciência.

Estabelecidas essas limitações, pode-se afirmar primeiro que a modernidade é marcada por esforços de uniformização. Porém, jamais foi um período uniforme (JOAS, 1999). Zygmunt Bauman (2001) si-



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

tua a existência de dois estágios na modernidade, um "sólido" e outro "líquido". A distinção fundamental entre ambos é a primazia dada ao princípio da territorialidade pelo primeiro, enquanto o segundo é marcado por tendências nômades de fluidez. Bauman, assim, afirma que mudanças substanciais na maneira de encarar a organização da sociedade e de sua atividade representam as distinções entre ambos os estágios. No que tange à guerra, ele também tem algo a nos dizer: em termos de técnicas de poder, hoje prevalece uma efetiva rejeição de qualquer confinamento territorial. Ganham importância a fuga, a astúcia, o desvio e a evitação. A modernidade é, nesse sentido, conduzida a partir da velocidade:

> O poder pode se mover com a velocidade do sinal eletrônico – e assim, o tempo requerido para o movimento de seus ingredientes essenciais se reduziu à instantaneidade. Em termos práticos, o poder se tornou verdadeiramente *extraterritorial*, não mais limitado, nem mesmo desacelerado, pela resistência do espaço (BAUMAN, 2011, p. 19).

Lefebvre (1995) opta por chamar o fenômeno de modernismo, distinguindo a concepção de modernidade enquanto possibilidade de crítica interdependente dele. A concepção de moderno é constituída como uma antítese ao que é antigo, mas logo adquire uma nova característica: o século XIX vislumbraria o modernismo enquanto o culto da inovação por si só. Em Lefebvre, a modernidade enquanto modernismo pressupõe a existência iminente de algo novo em cada setor da prática, conhecimento e consciência – mas essa novidade está longe de se constituir uma consciência genuína. O que é importante destacar da análise de Lefebvre é o caráter do novo e da inovação como sinônimos da ciência e da tecnologia modernas.

Como Gray (1997), Lefebvre (1995) dedica importantes palavras para o papel da cibernética nesse contexto. O autor considera a cibernética – e todas as teorias e técnicas que se sustentam nela – como a



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

forma mais moderna de cientificismo. Esse mesmo cientificismo está imiscuído na estratégia militar dos EUA e alimenta o tropo de guerra que sustenta o atual debate sobre ciberguerra no país e além dele (GRAY, 1997).

Gray (1997) sustenta que compreender a guerra do final do século XX é compreender como a racionalidade científica moldou a tecnociência. A guerra moderna, em si, é marcada pelo surgimento de técnicas de governamentalidade (FOUCAULT, 2003) e pela relação entre a tecnologia e a constituição de uma racionalidade pautada na ordem, no progresso e na crença na razão. A tecnologia, crucial no desenvolvimento de práticas de guerra, influencia a forma de pensá-la (CREVELD, 1991; BOUSQUET, 2009). Enquanto isso, a modernidade marca a incorporação de técnicas científicas à lógica da guerra (GRAY, 1997).

Transformações tecnológicas ao mesmo tempo impulsionaram e foram produtos do processo de industrialização e superprodução (TOWNSHEND, 2000). Nesse contexto, o racionalismo, o desenvolvimento de burocracias administrativas e a aplicação sistemática da ciência e da tecnologia à forma de se fazer e pensar a guerra marcam o início da guerra moderna (GRAY, 1997). A crença na capacidade da tecnologia em compensar as incertezas cotidianas foi incorporada por discursos e regimes de guerra desde a aplicação da mecânica ao desenvolvimento de armas e tecnologias de combate (BOUSQUET, 2009).

Aludindo às ideias de Heidegger, Scalercio (2015) atenta para o fato de a essência da tecnologia estar na forma como os seres humanos a concebem e a usam. Ao mesmo tempo em que provém de formas de pensar e compreender o mundo, ela interfere em como nos relacionamos com ele. Enquanto guerra e tecnologia encontram uma associação histórica que precede a Idade Moderna, Scalercio (2015) oferece uma visão complementar àquela feita por Gray (1997): na moderni-



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

dade, a ciência se funde à tecnologia para dar origem ao que este autor denomina de tecnociência. A distinção entre a tecnologia sempre presente e a tecnologia na modernidade reside fundamentalmente no processo de aceleração (GRAY, 1997; BAUMAN, 2001; SCALERCIO, 2015). Dita aceleração guarda relação com três elementos importantes: o pensamento científico moderno, a ascensão do Estado e o desenvolvimento das relações capitalistas, ou, em outras palavras, com o que se convém denominar modernização (SCALERCIO, 2015).

Embora a associação entre guerra e tecnologia preceda a Idade Moderna (CREVELD, 1991), é precisamente com o casamento entre guerra e ciência que meios sem precedentes de destruição foram reunidos em exércitos organizados a partir de estruturas logísticas e que tecnologias e metáforas fazendo alusão a máquinas passaram a ser incorporadas nos vocabulários e práticas de guerra. A tecnociência típica do período moderno passa a permear as estratégias de guerra e, consequentemente, a política na modernidade, enquanto o poder industrial se configura como seu princípio organizador (GRAY, 1997).

Nas breves palavras acima, buscamos situar elementos centrais à modernidade, sem oferecermos uma concepção definitiva de um fenômeno tão complexo. A despeito da ausência de definição global, acreditamos ser perfeitamente possível identificar o que nos permite denominar a modernidade enquanto tal, e podemos listar os elementos aqui trabalhados: pela tecnologia e ciência enquanto inovações, pela inovação alicerçada na tecnociência, pela temporalidade, pela velocidade (aceleração), pela formação de estruturas burocráticas como o Estado, pela consequente tensão entre territorialidade e nomadismo, e pela aplicação disso tudo às esferas da vivência humana, dentre as quais se destaca a guerra.

Havendo procedido a essas considerações, é de suma importância que investiguemos com maior profundidade o fenômeno que nos



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

propusemos a tratar como manifestação dessa inter-relação entre tecnologia e modernidade, qual seja, a noção de ciberguerra. Iremos, portanto, desenvolver uma genealogia do instituto, perpassando brevemente por sua constituição etimológica e concentrando-nos na ciência que o fundamenta – a cibernética – e nos discursos utilizados para construí-lo, após o surgimento do termo na década de 1990.

## 2. Genealogia da Ciberguerra

Compreendemos a genealogia no seu sentido foucaultiano, como fenômeno distinto da busca pelas origens. Trata-se de uma exposição da pluralidade que permite questionar as crenças filosóficas e sociais da ideologia dominante, buscando fazer sentido a respeito de suas condições de possibilidade (FOUCAULT, 1980). Nesse sentido, proceder a uma genealogia do conceito de ciberguerra envolve investigar as significações que constituíram o discurso atual e analisar suas condições de possibilidade.

Contemporaneamente, a ciberguerra é concebida como uma ameaça real (ARQUILLA; RONFELDT, 1993; LYNN, 2011; CLARKE; KNAKE, 2012; SHAHEEN, 2014; GREATHOUSE, 2011), com efeitos potencialmente danosos para se tornar um "Pearl Harbor virtual" (LYNN, 2011) ou ser considerada como inovação militar similar ao que a *blitzkrieg* foi para o século XX (ARQUILLA; RONFELDT, 1993). Como conflito próprio da era da informação, corresponde à guerra conduzida no ciberespaço a partir de ataques cibernéticos e do uso de "armas" cibernéticas (vírus e *worms* projetados para desestabilizar), podendo ocorrer unicamente no domínio virtual ou acompanhar meios convencionais de combate (MELZER, 2011; CLARKE; KNAKE, 2012). Na ciberguerra, está em jogo a capacidade de o agressor danificar os computadores, sistemas ou redes de informações de seus alvos (MELZER, 2011). Qualquer ator estatal ou não estatal pode perpetrar um ataque cibernético, destacan-



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

do-se o papel plural do *hacker* como vândalo, ladrão e terrorista ou "soldado" patrocinado por um Estado (BETZ; STEVENS, 2011). Lynn (2011) caracteriza a ameaça da seguinte maneira:

> Até o presente, as intrusões ocorreram principalmente com a finalidade da exploração: roubar propriedade intelectual de redes comerciais ou espiar o governo. Houve também ciberataques disruptivos, por exemplo contra a Estônia em 2007 e a Geórgia em 2008. É um desenvolvimento de importância extraordinária que agora existam cibertecnologias capazes de destruir redes críticas, causar danos físicos ou alterar o desempenho de sistemas cruciais. No século XXI, bits e bytes são tão ameaçadores quanto balas e bombas (LYNN, 2011).

As tecnologias cibernéticas como ameaças à estabilidade de redes que sustentam infraestruturas críticas dos países são retratadas como novas, resultantes do impressionante desenvolvimento no campo da cibernética nas últimas décadas. Mas a conjunção entre o setor militar, a construção de ameaças e a cibernética precede o discurso ora dominante, incluindo as versões que contestam o exagero existente a respeito da dimensão da ameaça (BETZ; STEVENS, 2011; RID, 2012). A origem e o desenvolvimento da cibernética acompanham a guerra, permitindo sua incorporação não apenas em práticas e tecnologias de guerra, como também afetando substancialmente o imaginário militar desde a Guerra Fria.

O termo ciberguerra é marcado pela união entre "guerra" e "cibernética", correspondendo à guerra deflagrada virtualmente. A raiz etimológica da palavra cibernética remonta ao grego *kybernetikos*, correspondendo à governança, ou à arte de governar (*kybernetike tekhne*). O *ciber* moderno emerge consoante o desenvolvimento das tecnologias da computação e jogos no pós-Segunda Guerra Mundial. Norbert Wiener revolucionou a computação ao conceber a informa-



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

ção como uma quantidade tão relevante quanto energia e matéria. Comunicação e controle são seus elementos constitutivos: "é a finalidade da cibernética desenvolver uma linguagem e técnicas que de fato nos capacitarão para atacar o problema de controle e comunicação em geral" (WIENER, 1989, p. 17).

Há, no cerne da cibernética, uma preocupação com a relação entre comando, controle, comunicação e fluxo de informações em máquinas, em seres vivos e entre ambos. Na Guerra Fria, o desenvolvimento de tecnologias militares de inteligência artificial permitiu um debate comparativo entre indivíduo e máquina, sugerindo a possibilidade de uma convergência entre mente e *software*.

A ciberguerra se insere no contexto da revolução informacional da década de 1980 e difusão das tecnologias da informação (TI) na década de 1990, em meio ao desenvolvimento de tecnologias da informação e inovações organizacionais. Tais transformações afetariam a concepção da natureza dos conflitos e das estruturas, doutrinas e estratégias militares (CAVELTY, 2011). Por exemplo, o modelo da rede, fruto do desenvolvimento das teorias do caos e complexidade, tem servido para fazer sentido acerca das dinâmicas de interconectividade do espaço virtual (JUNIO, 2013; SHAHEEN, 2014; FARWELL; ROHOZINSKI, 2012; RID, 2012), caracterizando também a era da informação (BOUSQUET, 2009).

Embora a ciberguerra, enquanto termo, origine-se da publicação do artigo "Cyberwar Is Coming!", de Arquilla e Ronfeldt (1993), a ideia de computadores protagonizando um cenário de conflito não era exatamente novidade (CREVELD, 1989). Tanto a Guerra do Vietnã quanto a Guerra do Golfo de 1991 representariam duas formas distintas de aplicar essa ideia, uma fracassada e outra relativamente bem-sucedida (BOUSQUET, 2009; CAVELTY, 2011). Arquilla e Ronfeldt escreviam a partir de um contexto no qual a guerra informacional se tornava um tópico "quente" na esfera militar, em particular



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

para uma Revolução nos Assuntos Militares (RMA) em curso desde meados da década de 1980 (ARQUILLA; RONFELDT, 1993; METZ; KIEVIT, 1995).

Nos anos 1990, a esfera militar nos EUA impulsionou a construção da percepção da ameaça virtual devido ao rápido desenvolvimento de sua infraestrutura informacional (CAVELTY, 2009). Para Cavelty (2009), a Estratégia de Segurança Nacional do governo Clinton é manifestação da crescente importância dessa infraestrutura no discurso político do país, e toda uma nova terminologia passou a ser empregada para se referir à "nova ameaça", típica da sociedade da informação. Essa preocupação teria sido alimentada pelo crescente número de ataques de *hackers* às redes e à Internet e pelo uso de armas cibernéticas, como o *Moonlight Maze*, direcionado a arquivos confidenciais do Pentágono (SHAHEEN, 2014).

Cavelty (2011) aduz que a euforia inicial com a ciberguerra levou à formulação de estratégias direcionadas aos sistemas informacionais do oponente. Tal desenvolvimento teórico chamaria a atenção para o percebido grau de vulnerabilidade das sociedades dependentes das redes. Isso também chamaria a atenção para os riscos às redes de dados civis e poria os EUA, por sua condição de superpotência, na condição de alvo de combates assimétricos, categoria na qual a ciberguerra passou a ser incluída.

Uma perspectiva interessante para se vislumbrar a ciberguerra é em termos da interconectividade das infraestruturas em rede como ameaça, precisamente devido à possibilidade de perturbações às redes poderem resultar em efeitos em cascata e, logo, em desastres capazes de escapar ao controle dos administradores da rede ou dos governos. Nesse sentido, "os avanços na tecnologia da informação e da comunicação assim aumentaram o potencial para um desastre maior nas infraestruturas críticas, por ter aumentado enormemente a possibili-



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

dade de riscos locais se transformarem em riscos sistêmicos" (CAVELTY, 2011, p. 13).

Outra perspectiva foca na disposição de atores "maliciosos" para explorar as vulnerabilidades de sistemas sem quaisquer restrições. O ataque às infraestruturas e sistemas críticos se torna integral à lógica moderna de destruição, cujo objetivo é obter um impacto amplo. Essa visão implica em conceber o inimigo como uma entidade genérica, sem rosto, impossível de identificar ou detectar com precisão. Em termos de representação da ameaça, isso torna a capacidade de proteção tradicionalmente atribuída ao território menos relevante e, ao mesmo tempo, torna a ameaça ubíqua precisamente pela possibilidade de vir de qualquer lugar (CAVELTY, 2011).

Uma importante definição sobre ciberguerra a caracteriza amplamente, considerando o seu papel junto aos meios convencionais de guerra, e de forma "estrita", referente a um conflito cujo início, desenvolvimento e fim ocorrem exclusivamente no ciberespaço (ARQUILLA; RONFELDT, 1993). Isso não exclui a possibilidade de ataques cibernéticos afetarem serviços dos quais as pessoas diariamente dependem:

> Ciberguerra se refere a conduzir, e preparar-se para conduzir, operações militares de acordo com princípios relacionados com a informação. Significa perturbar, se não destruir os sistemas de informação e comunicação, definidos amplamente para incluir até a cultura militar, dos quais um adversário depende para "conhecer" a si mesmo [...]. Significa tentar saber tudo sobre um adversário enquanto este não sabe nada sobre nós mesmos. Significa virar o "equilíbrio de informação e conhecimento" ao nosso favor, sobretudo quando o equilíbrio de forças não está. Significa usar o conhecimento para que menos capital e trabalho sejam gastos. Esta forma de guerra pode envolver diversas



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

> tecnologias – notavelmente para C3I; para coletar, processar e distribuir inteligência; para comunicações táticas, posicionamento e a identificação de amigos e inemigos (IFF); e para sistemas de armas "inteligentes" – para dar só alguns exemplos. Também pode envolver o *blinding*, o *jamming*, o engano, o sobrecarregamento e a intrusão eletrônicos dos circuitos de informação e comunicação do adversário (ARQUILLA; RONFELDT, 1993, p. 30).

Mas enquanto a ciberguerra poderia, para Arquilla e Ronfeldt (1993), fazer-se presente tanto em conjunto com meios convencionais de guerra, com o uso de redes digitais para sabotar sistemas de defesa antiaérea, quanto exclusivamente no ciberespaço, como meio de intrusão e ruptura de sistemas de informação e comunicação, ela se distingue dos significados da guerra eletrônica, computadorizada, automatizada ou robótica empregados durante a Guerra Fria. Para os autores, esse tipo de distinção reside em seus impactos na doutrina militar e de guerra, em particular a necessidade de descentralização das estruturas de comando e controle.

Libicki (2009) inicialmente distingue entre ciberguerra estratégica e operacional. A primeira corresponde à "campanha de ciberataques lançada por uma entidade contra um Estado e sua sociedade, primariamente mas não exclusivamente para afetar o comportamento do Estado-alvo" (LIBICKI, 2009, p. 117), ao passo que a segunda é compreendida como "ciberataques em tempos de guerra contra alvos militares e civis relacionados ao esforço de guerra [...] [p]ode ser um multiplicador de forças decisivo se empregado com cuidado, discrição no preciso momento justo" (LIBICKI, 2009, p. 139). Enquanto o autor duvida da efetividade da primeira, entende a segunda apenas como instrumental para a batalha, comparando-a com o que considera ser o papel do poder aéreo para o combate.



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

No século XXI, a projeção adquirida pela ciberguerra após ataques cibernéticos contra a Estônia (em 2007), a Geórgia (em 2008) e o Irã (em 2010) levou à produção de uma série de estudos a seu respeito (FARWELL; ROHOZINSKI, 2011; 2012; KASSAB, 2014; SHAHEEN, 2014; KNOEPFEL, 2014; MEHMETICK, 2014). Os eventos, ademais, contribuíram para generalizar a percepção de que o ciberespaço é um fator de vulnerabilidade para os países. Essa percepção acompanhou o desenvolvimento da ARPANET, rede inicialmente projetada com fins militares que antecede a Internet (KAISER, 2014, p. 13), de modo que os ataques de negativa de serviço que atingiram a Estônia e a Geórgia, e a sabotagem do Stuxnet, são apenas as pontas do iceberg que é o caminho percorrido para o que hoje se tem por ciberguerra.

Recentemente, Libicki (2014) adotou a distinção entre os termos *cyberwarfare* e *cyberwar* para distinguir o que Arquilla e Ronfeldt (1993) categorizaram como um único fenômeno, próprio da era da informação. A terminologia utilizada em seu trabalho mais recente se distingue daquela empregada em sua monografia de 2009:

> A *cyberwarfare*, como a *warfare*, trata da conduta da guerra inevitavelmente para avançar o exercício do combate no domínio físico (também pode ser considerada ciberguerra operacional ou instrumental). A ciberguerra (*cyberwar*) é empreendida para afetar diretamente a vontade do adversário (também pode ser considerada igual à ciberguerra estratégica) (LIBICKI, 2014, p. 29).

Libicki duvida da possibilidade de a categoria *cyberwar* ser verdadeiramente revolucionária. Ele se une ao ceticismo de Rid (2012) e questiona a mudança que ela significaria, mas se distingue ao categorizá-la como mecanismo de guerra (mesmo que limitado), enquanto Rid duvida inclusive de sua inserção nessa categoria. Enquanto não é interesse do presente artigo discutir a possibilidade ou viabilidade da

ciberguerra, é importante notar que muitas categorizações recaem nas definições propostas por Arquilla e Ronfeldt (1993) ou por Libicki (2009; 2014), optando ou por incluir no domínio da ciberguerra tanto operações convencionais quanto exclusivamente digitais ou tratar a ciberguerra apenas na segunda acepção. Esta última tendência tem sido mais recorrente após os ataques cibernéticos contra a Estônia e a descoberta do Stuxnet (KAISER, 2014; FARWELL; ROHOZINSKI, 2012). Outros autores optam por identificar a ciberguerra com ataques cibernéticos a sistemas de informação e considerá-los sem necessariamente fazer alusão a seu impacto imediato no mundo material (DIPERT, 2010).

A preocupação de Arquilla e Ronfeldt com as novas modalidades de conflitos na era da informação acompanha uma mudança no imaginário militar norte-americano influenciada pela Guerra do Vietnã. Uma delas corresponde à política de evitar conflitos em situações similares, enquanto os EUA optam por guerras por procuração ou mediante o uso do poder aéreo, de modo que o país possa gozar de sua vantagem tecnológica de modo absoluto (BUCHANAN, 2006). Influenciada pela aplicação das teorias do caos e da complexidade à cibernética, a nova doutrina militar idealiza conflitos em redes, baseados no uso da tecnologia como meio de reduzir as baixas dos EUA em combate. Uma lição da Guerra do Vietnã incorporada à RMA é a tentativa de evitar embates assimétricos diretos (BUCHANAN, 2006; BOUSQUET, 2009).

Crítico da histeria sobre a ciberguerra, Rid (2013) argumenta que ataques cibernéticos reduzem a violência política. Para o autor, contrariamente à ideia de que tais ataques aumentariam a possibilidade do conflito em função das incertezas características de sua natureza (GOMPERT; LIBICKI, 2014), eles seriam uma forma de reduzir a violência "real" no mundo e poupar o combatente de ataques diretos, uma vez que se utilizam de atos de agressão, como sabotagem e espionagem, que tenderiam a evitar a escalada do conflito.



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

Em suma, a ciberguerra tem grande parte de seu desenvolvimento alocado nos EUA, tendo suas raízes no desenvolvimento da cibernética enquanto ciência (BOUSQUET, 2009). Na década de 1990, o tema foi impulsionado com a difusão da Internet e do ciberespaço no cotidiano e pelo crescente interesse no assunto pela esfera militar e por *think tanks*. Anteriormente, falava-se em guerra computadorizada para fazer referência à penetração do computador na esfera militar-estratégica, sua incorporação na burocracia militar e nas táticas de guerra (CREVELD, 1989). A próxima seção analisa a gradativa transformação dos regimes tecnocientíficos constituídos pelos EUA desde o fim da Segunda Guerra Mundial, de onde muitos elementos constitutivos da ciberguerra nascem, impulsionados pelo processo de "ciberização" da guerra e da mentalidade estratégica. Essa forma de conflito também converge com as transformações na mentalidade militar norte-americana pós-Vietnã, simbolizada pela perspectiva da guerra em redes.

## 3. A Ciberguerra e as Transformações na Guerra no Fim do Século XX

A presente seção visa estabelecer um panorama a respeito de como a ciência e o paradigma da modernização impulsionaram transformações na guerra, a fim de situar a ciberguerra no contexto das transformações da guerra na modernidade. Utilizamos a análise proporcionada por Bousquet (2009), que distingue entre quatro regimes tecnocientíficos de guerra na modernidade. A partir disso, desenvolve-se o argumento de que o fenômeno representa uma tensão entre dois desses regimes, o cibernético e o caospléxico, ao abraçar as noções de caos/complexidade ao mesmo tempo em que é marcada por uma preocupação com o controle. Ademais, compreender a ciberguerra enquanto manifestação desta tensão permite tecermos uma crítica à forma como o fenômeno se articula ao imaginário de não violência pre-



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

sente nas teorias da modernização (JABRI, 2007; JOAS, 1999). Argumenta-se que a "higienização" da guerra, como produto da associação entre tecnologia, ciência e modernidade, é problemática ao sustentar a separação entre guerra e violência, e que a ciberguerra, nesse diapasão, parece se apresentar como solução tecnológica para poupar o combatente da violência inerente ao conflito, a partir da ênfase em uma guerra simulada (REID, 2003; BUCHANAN, 2006; JABRI, 2007).

A relação entre guerra, política e desenvolvimentos tecnológicos tem mudado na modernidade, em particular considerando-se o papel da tecnologia do fim da Segunda Guerra Mundial até o presente. Nesse sentido, o atual discurso em torno da ciberguerra pode ser lido como parte de um processo de transformação dos regimes modernos de guerra. Bousquet (2009) situa a existência de quatro regimes tecnocientíficos que representam as transformações na guerra moderna: o mecanístico, o termodinâmico, o cibernético e o caospléxico. Esses regimes se apoiam em quatro tecnologias distintas, porém centrais ao pensar e fazer a guerra, sendo elas o relógio, o motor, o computador e a rede, correspondentes às respectivas ciências que as envolvem (mecânica, termodinâmica, cibernética e caos/complexidade). Esses desenvolvimentos científicos alteraram a prática e a concepção da guerra e o atual período representa uma tensão entre dois regimes distintos, o cibernético e o caospléxico.

Dois desses regimes antecederam a Segunda Guerra Mundial: o mecanístico e o termodinâmico, apoiando-se respectivamente nas ciências do movimento e da energia. Enquanto o primeiro regime é marcado pela tentativa de imposição de ordem ao campo de batalha a partir da disciplina, do uso do método e da razão científica, o segundo rompe com as certezas antes predominantes, aceitando a existência da desordem física e fundamentando-se na energia enquanto ativo. No universo da guerra, isso implica em reconhecer suas incertezas inerentes, ou a "névoa da guerra" (CLAUSEWITZ, 1989). O período



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

também observou o acelerado desenvolvimento industrial do Ocidente e alimentou a crença moderna no progresso ilimitado (BOUSQUET, 2009).

O fim da Segunda Guerra Mundial observou novas transformações no regime de guerra, graças à aplicação do eletromagnetismo às telecomunicações. Essa mudança foi impulsionada pela ascensão dos EUA à condição de potência mundial, casando-se com a tecnofilia dos militares norte-americanos. Uma assemblage de telecomunicações apoiadas no eletromagnetismo, tecnologias de miniaturização, transmissão de vídeo e áudio, bem como satélites, convergiria para o computador (BOUSQUET, 2009). O regime cibernético da guerra corresponde ao processo de "ciberização" do aparato militar dos EUA na Guerra Fria, quando tecnologias e conceitos da cibernética passam a ser utilizados para pensar a guerra e o uso da força. Associados à finalidade inicial do computador, esses conceitos e tecnologias, bem como a própria guerra, passam a ser vistos como sujeitos à análise científica, passíveis de controle e previsão com o uso da lógica e da matemática para o processamento de informações e produção de cálculos exatos (CREVELD, 1989; BOUSQUET, 2009).

O controle é internalizado no discurso militar dos EUA, e subsidiando essa racionalidade está o sonho de superar a desordem e a entropia no campo de batalha mediante o uso dos fluxos de informações. O embrião do atual discurso de interoperabilidade possibilitaria colocar o computador e sua função de processamento como elementos centrais de controle no campo de batalha, como elo entre o sensor e o resultado final, o radar e o míssil. A centralidade da informação para o regime cibernético dos anos 1950/60 acompanha a do computador, apresentando-se como solução para a "névoa da guerra" (BOUSQUET, 2009).

A Guerra do Vietnã materializa as racionalidades e tecnologias que tornaram a ciberguerra possível, atestando o fracasso desse regime



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

baseado no controle absoluto, centralização e em operações militares subsumidas a uma racionalidade lógico-matemática (BOUSQUET, 2009). A crença na vitória mediante a superioridade tecnológica gerou a percepção errônea do inimigo como portador de uma racionalidade inferior, e o amplo fluxo de informações não reduziria incertezas, mas as aumentaria (CREVELD, 1989). Eis o paradoxo do regime cibernético: a pressão exercida pela grande quantidade de informações, em vez de levar à certeza e à precisão, produziu incertezas e imprecisões no contexto de um sistema centralizado de comando e controle (ARQUILLA; RONFELDT, 1993; BOUSQUET, 2009).

A ciberguerra reúne elementos desse regime cibernético, a exemplo da informação como conceito organizacional (ARQUILLA; RONFELDT, 1993). Mas também incorpora noções de caos e complexidade baseadas no comportamento de sistemas compostos por múltiplas partes independentes e organizadas de modo não linear. Na teoria da complexidade, a figura da rede é essencial para ilustrar os padrões de interação constituídos a partir das relações entre múltiplas entidades em um sistema (BOUSQUET, 2009).

Bousquet (2009) chama atenção para a organização descentralizada, aberta e adaptável ao ambiente em constante transformação da rede. Para Arquilla e Ronfeldt (1993), a revolução informacional mina as hierarquias em torno das quais as instituições são tradicionalmente desenhadas, tornando o poder difuso e redistribuindo-o para atores até então "menores" ou mais fracos. Os atores capazes de se adaptar a essa nova configuração do conflito estariam em vantagem em relação àqueles ainda apoiados em estruturas mais hierarquizadas, como os exércitos. A ciberguerra é uma das novas formas de conflito cuja dinâmica é a das redes.

A transição para o regime caospléxico de guerra envolve reconhecer a necessidade de descentralizar as estruturas de comando e controle e incorporar a existência de ordem no caos (BOUSQUET, 2009), en-



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

quanto a tecnologia ainda se apresenta como solução para a indisposição de comprometer a própria população na guerra (BUCHANAN, 2006). Nessa transição, há uma tensão entre tendências de centralização e descentralização das estruturas militares (ARQUILLA; RONFELDT, 1993; METZ; KIEVIT, 1995), passando a ser a "névoa da guerra" compreendida como superável a partir de sistemas complexos de comando, controle, computadores, comunicação, informação, inteligência, vigilância e reconhecimento (BOUSQUET, 2009).

Os princípios do caos e complexidade são aplicados ao desenvolvimento de tecnologias sofisticadas para o conflito, como *performance* de computadores, inteligência artificial e robótica. No plano estratégico, isso deu maior espaço ao discurso da guerra centrada em redes (BOUSQUET, 2009; ARQUILLA; RONFELDT, 1993). A resposta à ausência de informação é o uso da tecnologia para aquisição, processamento e distribuição de mais informação, considerada um ativo vital a ser protegido (CLARKE; KNAKE, 2012), do qual dependem as infraestruturas críticas dos países.

A atual discussão sobre ciberguerra se insere no contexto da revolução informacional que tem moldado as percepções de oportunidades e riscos (CAVELTY, 2011), flutuando entre as vantagens da tecnologia cibernética no campo de batalha e preclusão de certezas ou previsões pela natureza inerentemente fluida do ciberespaço. Mas, apesar do chamado para se abraçar as ideias de caos e complexidade no contexto dos conflitos assimétricos (ARQUILLA; RONFELDT, 1993), grande parte da doutrina militar ainda tende a empregar a linguagem do regime cibernético da Guerra Fria (BOUSQUET, 2009).

Na modernidade, os desenvolvimentos tecnológicos tanto alteram a forma de se conceber e fazer a guerra quanto a guerra mimetiza, a partir dos paradigmas científicos, as mudanças de gestão e estratégia que alteram substancialmente suas dinâmicas. Esse contexto, marcado pelo uso da violência pelos Estados e entidades políticas



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

com natureza variada, põe a guerra como instrumento da política (CLAUSEWITZ, 1989; CHAGAS, 2015). A razão de Estado, assim, constitui-se de forma antitética à prática indiscriminada ou cultural da guerra (BOUSQUET, 2009).

Clausewitz nos oferece um ponto de partida interessante para situar a teoria da guerra. De acordo com Chagas (2015), a leitura de Clausewitz permite distinguir entre a natureza da guerra, explorada em seu conceito de guerra absoluta e caracterizada por sua permanência, abstração e pureza – um tipo ideal – e as transformações em sua condução, ou, em outros termos, as diversas formas que a guerra pode vir a adquirir. É dessa forma que podemos considerar o diálogo entre Bousquet e Clausewitz, no momento em que este reconhece que cada período tem seu tipo próprio de guerra, suas condições limitadoras e preconcepções. Porém, Chagas (2015) chama a atenção para um elemento ainda mais central em Clausewitz e natural a todas as guerras, independentemente de sua forma: referimo-nos à trindade violência-razão-oportunidade.

Aludida trindade não é a única idealizada por Clausewitz: uma trindade secundária é composta pelos elementos povo-governo-exército. Chagas (2015) assinala que, distintamente da primeira trindade, esta última tende a ser aplicada na análise da guerra moderna e interestatal. Ela, porém, incorpora a trindade inicial, precisamente em virtude de seu caráter universal. Assim, a violência, também em Clausewitz, surge como elemento constitutivo do fenômeno da guerra fora de seu domínio ideal, sem o qual ela perde seu elo com a realidade.

Para Reid (2003), a transformação na cultura militar ocidental é um microcosmo de transformações sociais mais amplas, associadas às tecnologias da informação, à ciência da complexidade e à lógica organizacional da sociedade em rede. A lógica da produção cede espaço para a lógica da informação. Nesse sentido, o autor sugere estar em curso uma reorganização do conhecimento a partir de mudanças



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

epistêmicas associadas à emergência das ciências da complexidade no campo da cibernética: "a influência dessa mudança epistêmica não afeta só a organização social dos estamentos militares; é propriamente definição e entendimento do que é a estratégia e como esta é teorizada" (REID, 2003, p. 6).

Jabri (2007) parte do conceito de matriz global da guerra para fazer sentido a respeito da lógica dos conflitos contemporâneos. Dita ideia chama a atenção para a coconstituição entre guerra e paz, possuindo a primeira o papel de disciplinar o tecido social. A guerra está sempre presente ao exercer um papel específico na organização da sociedade, justificar a si própria e estabelecer um discurso sobre o que deve ser considerado guerra ou paz, delimitando o que é uma forma legítima de guerra. Essa concepção difere substancialmente do que se tem tradicionalmente constituído ao longo da modernidade, quando o desenvolvimento de técnicas de governamentalidade representou a passagem do modelo feudal de guerra para o moderno (REID, 2003). Essa passagem é marcada pela concentração das práticas e instituições de guerra nas mãos de um poder central com legitimidade para fazer a guerra, participar na criação das ameaças e alterar a lógica da relação entre guerra e política no início da modernidade (FOUCAULT, 2009).

Jabri (2007) parte da inversão foucaultiana do aforismo de Clausewitz para elaborar o conceito de matriz global da guerra. A despeito das divergências em torno da aplicabilidade ou não da teoria clausewitziana da guerra (CREVELD, 1989; ECHEVARRIA, 2007) e das tentativas de aplicá-las à ciberguerra (KNOEPFEL, 2014; SHAHEEN, 2014), essa leitura permite contextualizar Clausewitz de acordo com o papel da guerra moderna como estratégia de poder (REID, 2003; FOUCAULT, 2003; 2009). Considerar a política como continuação da guerra por outros meios permite conceber o uso da força como estratégia de poder (FOUCAULT, 2003), permitindo contestar a crença de que o período moderno é fundamental-



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

mente pacífico (JABRI, 2007). Foucault sugere que a inversão permite conceber as relações de poder no tecido social como ancoradas em uma relação de força estabelecida na guerra e a partir dela: "A política [*politics*], em outras palavras, sanciona e reproduz o desequilíbrio das forças manifestado na guerra" (FOUCAULT, 2003, p. 16).

Jabri (2007) amplia essa noção para o âmbito global, compreendendo guerra como prática ilustrativa da relação íntima entre guerra e paz. A autora analisa o contexto das transformações pelas quais a guerra passou na modernidade tardia, em particular no que concerne ao desmantelamento das concepções tradicionais de fronteiras estatais e em sua tendência em operar a despeito de limites espaço-temporais. A autora considera a existência de uma rede complexa de relações que caracteriza uma matriz global da guerra que permeia as relações de poder em um escopo global. E, enquanto estratégia de poder, a guerra tem na violência o seu elemento constitutivo (JABRI, 2007).

A partir disso, a autora critica o sonho moderno de erradicação da violência. Em certo sentido, a ciberguerra não rompe com o projeto da modernidade, muito menos assinala uma transformação na natureza da guerra. Mas o fenômeno torna possível que a crença no domínio sobre a informação subsidie a concepção contemporânea de progresso. A ciberguerra incorpora certa rejeição da violência, presente nas teorias da modernização, cuja base é a crença de que a modernidade é uma época pacífica (JOAS, 1999). Essa premissa é criticada precisamente pelo fato de a rejeição à violência negligenciar sua presença no cotidiano. Jabri (2007) questiona a relação entre a modernização e a redução na probabilidade, com possibilidade de erradicação da guerra.

A experiência da Guerra do Golfo alterou substancialmente o pensamento militar sobre guerra, e a ciberguerra passa a fazer parte de uma nova geração de conflitos na qual a vitória não depende exclusiva-



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

mente do uso da força, mas principalmente da habilidade de vencer a guerra informacional e assegurar o domínio da informação (CAVELTY, 2011). O fenômeno representa um processo de transformação na forma de se fazer e pensar guerra, marcado pela tensão entre a busca pela certeza *versus* a incerteza inerente ao instituto. Essa transformação se relaciona com a centralidade da informação para a estratégia militar e com a percepção de que o mundo é organizado em redes. O discurso sobre a ciberguerra a torna ubíqua, podendo acontecer virtualmente a qualquer momento, em qualquer lugar.

Essa ubiquidade, aliada à concepção da ciberguerra enquanto alternativa tecnológica ao conflito, obscurece o papel da violência na guerra. Se a inversão foucaultiana do aforismo de Clausewitz é válida, a guerra permeia as relações políticas e, com isso, toda ordem política surge e é mantida por um ato de força e pela oposição entre "nós" e "outro" (JABRI, 2007).

A ciberguerra representa uma opção de baixo risco em termos de conflito (GOMPERT; LIBICKI, 2014), em particular ao poupar o combatente por trás da operação do computador de sua violência (JOAS, 1999; BUCHANAN, 2006; JABRI, 2007). Ataques cibernéticos possibilitariam a Estados, grupos e indivíduos empreender atos de agressão que não se elevam ao ato de guerra, como a sabotagem e a espionagem. Rid (2013) sugere que operações de sabotagem computadorizadas permitem o emprego de ataques precisos contra sistemas de adversários sem direta e fisicamente causar danos aos seus operadores. Dessa forma, os discursos sobre a ciberguerra, tais como a teoria da modernização, almejam, implícita ou explicitamente, conflitos sem violência – ou, minimamente, com uma violência "limpa".

Como Scalercio (2015) argumenta, as tecnologias da informação foram amplamente utilizadas na redução do custo humano e político de empreitadas científicas e de guerra – o autor se utiliza dos exemplos do programa espacial americano e da guerra ao terror para funda-



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

mentar seu argumento. Scalercio assinala que a garantia da superioridade das campanhas militares dos EUA depende da conjunção entre produção industrial, ciência e tecnologia e investimentos pesados. Essa tríade também serve ao propósito de reduzir as baixas de soldados e tornar a campanha militar breve.

Esse mesmo fenômeno é destacado por Gray (1997). Sua ênfase concorre com o que se tem discutido até o presente momento ao recair sobre a tecnologia computadorizada. O setor militar nos EUA nutre a esperança de solucionar os próprios problemas a partir do desenvolvimento e uso de sistemas e tecnologias baseadas no computador. O setor parece visivelmente comprometido com a crença na vitória alicerçada na superioridade tecnológica (GRAY, 1997). O autor resume seu argumento a partir de um exemplo:

> Um campo de batalha [em um conflito de baixa intensidade] é um país ou uma região. O campo de batalha nuclear é o mundo. A *netwar* ocorre no ciberespaço. Todas se estendem ao espaço, a ciberguerra mais que as outras. As tropas norte-americanas agora enfrentam a expectativa de combater à noite, no Ártico, no espaço real e simulado. O campo de batalha está fragmentado na realidade e nas mentes dos guerreiros e gerentes. Obter financiamento faz parte do preparo para a guerra tanto quanto planejamento e treinamento. Proteger o complexo militar-industrial é tanto objetivo das forças armadas quanto a proteção do país, se não mais ainda (GRAY, 1997, p. 172).

Isso é sintomático do fenômeno que Jabri (2007) identifica na modernidade tardia e que marca a busca pela otimização da necessidade de autossacrifício, podendo a guerra ocorrer diante da ausência de danos e perdas para o lado que perpetra o ato: "esse anseio para a guerra sem a possibilidade de se ferir é, no contexto da atual conjuntura histórica, um que domina o pensamento estratégico no Ociden-



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

te" (JABRI, 2007, p. 11). A separação entre guerra e violência equivale a conceber aquela sob uma perspectiva higienizada que obscurece a violência como aspecto constitutivo do próprio estado de guerra e, portanto, da política e da sociedade. Muito na ciberguerra nos remete às contradições presentes na teoria da modernização, evidentes na crítica à higienização da guerra: o fato de que a negação da violência leva à negligência de sua presença.

## Conclusão

Se a ciberguerra veio para ficar ou não, não saberemos dizer (tampouco nos cabe fazê-lo). O instituto não é um consenso mesmo entre quem se dedicou a desenvolver a ideia no curso dos últimos vinte anos. Em vez de compreendermos apenas o que é a ciberguerra e seus elementos, é muito mais frutífero compreendê-la como parte de um contexto mais amplo, de uma tendência histórica rica em detalhes e contradições, qual seja, o da relação entre a tecnologia e o processo de modernização que lhes dão efeito. As linhas desenvolvidas neste trabalho buscaram dar conta dessa relação, sustentando que o processo de modernização tem por característica a conjunção entre guerra, ciência e tecnologia, e que a incorporação da cibernética à guerra é representativa disso.

Subsidiando essa inter-relação, a primeira seção buscou estabelecer uma compreensão mais ampla acerca dos elementos em questão na modernidade, sem oferecer um conceito preciso e definido a seu respeito. Essa escolha se deve tanto à ampla variedade de elementos e situações quanto à complexidade que compõe este período da história humana. Assinalamos, apoiados no argumento de Bauman (2001), que a modernidade possui pelo menos mais de um estágio, o que dificulta qualquer esforço de uma definição precisa. Elencamos, porém, os elementos comuns identificados por uma parte robusta da literatura, sendo eles a figura do Estado-nação, tensões entre o princípio da territorialidade e o nomadismo, a importância do tempo, da velocida-



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

de (enquanto aceleração) e da instantaneidade na vivência humana, e, de maneira central, a interdependência entre ciência e tecnologia, por um lado, e ciência, tecnologia e guerra, por outro.

A segunda seção se ocupou de investigar as condições de possibilidade e os significados da ciberguerra, procedendo a uma genealogia da ciência que a alicerça – a cibernética – e das maneiras com as quais o discurso tem sido articulado desde seu surgimento, em 1993. Isso permite lançar a oportunidade para situar o papel da cibernética também como alicerce no desenvolvimento das práticas de guerra e tropo capaz de influenciar o imaginário militar a seu respeito.

A seção final traz uma crítica ao processo de modernização em sua conjunção entre guerra e ciência, tendo sido desenvolvida em dois momentos. Inicialmente, situamos a ciberguerra no contexto das transformações da guerra na modernidade. Com efeito, utilizamo-nos da abordagem de Bousquet (2009), que caracteriza quatro regimes distintos de guerra cuja base reside na conjunção entre guerra e ciência característicos do período moderno. A ciberguerra foi então caracterizada como representante de uma tensão entre dois regimes de guerra, o cibernético e o caospléxico, uma vez que incorpora concepções importantes sobre as teorias do caos e complexidade e, paralelamente, apoia-se na crença no controle sobre o conflito, sendo articulada como um meio capaz de reduzir as perdas em combate.

Em um segundo momento, construímos, a partir de Clausewitz (1989), Foucault (2003) e Jabri (2007), uma crítica à incorporação desse processo de modernização na mentalidade militar-estratégica norte-americana. Nosso argumento reside no fato de a ciberguerra ser dotada de características próprias do processo de modernização, dentre as quais se destaca a fuga da violência ou a tentativa de reduzir as baixas em combate – pelo menos do lado "detentor" da superioridade tecnológica (GRAY, 1997; SCALERCIO, 2015). Nossa crítica ecoa Clausewitz (1989), que, em sua trindade, considera a violência



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

como parte inerente da natureza da guerra, e Foucault (2003) e Jabri (2007), que, a partir da inversão de seu aforismo, consideram-na como parte constitutiva da política. Desse modo, se considerarmos o discurso de ciberguerra tal como ele tem sido construído desde o surgimento do termo, veremos que mesmo os textos mais céticos ao fenômeno não contestam algo inerente à sua natureza, que identificamos ser o sonho, alimentado pelo processo de modernização, de que a tecnologia, de alguma maneira mágica, contribuirá para a erradicação da violência do conflito.

## Notas

**1.** O título do presente trabalho faz alusão a duas importantes publicações sobre ciberguerra: a primeira é o artigo "Cyberwar Is Coming!", de John Arquilla e David Ronfeldt (1993), responsável pela formulação do termo *cyberwar*, traduzido para ciberguerra, para se referir às inovações nos conflitos possibilitadas pela revolução informacional. A segunda publicação à qual o título se refere é o artigo de Thomas Rid (2012), "Cyberwar Will Not Take Place", que sustenta ceticismo com relação à ocorrência do evento descrito pelos autores supracitados como "ciberguerra".

**2.** Devido à dificuldade de atribuição de autoria a ataques cibernéticos, torna-se difícil precisar seu(s) autor(es). A Rússia foi considerada como provável fonte dos ataques em virtude de, nas duas ocasiões, os mesmos ocorrerem durante conflitos contra a Estônia e a Geórgia.

## Referências Bibliográficas

ARQUILLA, John; RONFELDT, David. Cyberwar Is Coming! In: _____ (Org.). **In Athena's Camp**: Preparing for Conflict in the Information Age. Santa Monica: RAND, 1993.

BAUMAN, Zygmunt. **Modernidade líquida**. Rio de Janeiro: Zahar, 2001.

BETZ, David; STEVENS, Tim. **Cyberspace and the State**: Toward a Strategy for Cyber-Power. Londres: IISS, 2011.

BOUSQUET, Antoine J. **The Scientific Way Warfare**: Order and Chaos on the Battlefields of Modernity. Nova York: Columbia University Press, 2009.

BUCHANAN, Ian. Treatise on Militarism. In: _____; PARR, Adrian (Org.). **Deleuze and the Contemporary World**. Edimburgo: Edinburgh University Press, 2006.

CAVELTY, Myriam Dunn. **Cyber-Security and Threat Politics**: US Efforts to Secure the Information Age. Milton Park: Routledge, 2009.

____.Unraveling the Stuxnet Effect: Of Much Persistence and Little Change in the Cyber Threats Debate. **Military and Strategic Affairs**, v. 3, n. 3, p. 11-20, 2011.

CHAGAS [VIANNA BRAGA], Carlos. **Between Absolute War and Absolute Peacekeeping**: Searching for a Theory of the Use of Force on Behalf of the International Community. Tese (Doutorado em Relações Internacionais) – Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio), Rio de Janeiro, 2015.

CLARKE, Richard A.; KNAKE, Robert K. **Cyber War**: The Next Threat to National Security and What To Do About It. Nova York: Ecco, 2012.

CLAUSEWITZ, Carl von. **On War**. Princeton: Princeton University Press, 1989.

CREVELD, Martin van. **Technology and War**: From 2000 B.C. to the Present. Nova York: The Free Press, 1989.

____.**The Transformation of War**. Nova York: Free Press, 1991.

DIPERT, Randall R.The Ethics of Cyberwarfare. **Journal of Military Ethics**, v. 9, n. 4, p. 384-410, 2010.

ECHEVARRIA, Antulio J. **Clausewitz and Contemporary War**. Oxford: Oxford University Press, 2007.

FARWELL, James P.; ROHOZINSKI, Rafal. Stuxnet and the Future of Cyber War. **Survival: Global Politics and Strategy**, v. 53, n. 1, p. 23-40, 2011.



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

____. The New Reality of Cyber War. **Survival: Global Politics and Strategy**, v. 54, n. 4, p. 107-120, 2012.

FOUCAULT, Michel. Nietzsche, Genealogy, History. In: BOUCHARD, D. F. (Org). **Language, Counter-Memory, Practice**: Selected Essays and Interviews. Ithaca: Cornell University Press, 1980.

____. **Society Must Be Defended**: Lectures at the Collège de France, 1975-76. Nova York: Picador, 2003.

____. **Security, Territory, Population**: Lectures at the Colle`ge de France (1977-78). Org. de Michel Senellart. Basingstoke: Palgrave Macmillan, 2009.

GOMPERT, David C.; LIBICKI, Martin. Cyber Warfare and Sino-American Crisis Instability. **Survival: Global Politics and Strategy**, v. 56, n. 4, p. 7-22, 2014.

GRAY, Chris Hables. **Postmodern War**: The New Politics of Conflict. Nova York: Guilford Press, 1997.

GREATHOUSE, Craig. Cyber War and Strategic Thought: Do the Classic Theorists Still Matter? In: Kremer, J.-F.; MÜLLER, B. (Org.). **Cyberspace and International Relations**: Theory, Prospects and Challenges. Berlim: Springer, 2011.

JABRI, Vivienne. **War and the Transformation of Global Politics**. Basingstoke: Palgrave Macmillan, 2007.

JOAS, H. The Modernity of War: Modernization Theory and the Problem of Violence. **International Sociology**, v. 14, n. 4, p. 457-472, 1999.

JUNIO, Timothy J. How Probable is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate. **Journal of Strategic Studies**, v. 36, n. 1, p. 125-133, 2013.

KAISER, Robert. The Birth of Cyberwar. **Political Geography**, n. 46, p. 11-20, 2014.

KASSAB, Hanna Samir. In Search of Cyber Stability: International Relations, Mutual Assured Destruction and the Age of Cyber Warfare. In: Kremer, J.-F.; MÜLLER, B. (Org.). **Cyberspace and International Relations**: Theory, Prospects and Challenges. Berlim: Springer, 2014.

KNOEPFEL, Sascha. Clarifying the International Debate on Stuxnet: Arguments for Stuxnet as an Act of War. In: KREMER, J.-F.; MÜLLER, B. (Org.). **Cyberspace and International Relations**: Theory, Prospects and Challenges. Berlim: Springer, 2014.

LEFEBVRE, Henri. **Introduction to Modernity**: Twelve Preludes September 1959-May 1961. Nova York: Verso, 1995.

LIBICKI, Martin C. **Cyberdeterrence and Cyber War**. Santa Monica: RAND, 2009.

____.Why Cyber War Will Not and Should Not Have Its Grand Strategist. **Strategic Studies Quarterly**, v. 8, n. 1, p. 23-39, 2014.

LYNN, William. The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack. **Foreign Affairs**, 2011.

MEHMETICK, Hakan. A New Way of Conducing War: Cyberwar, Is that Real? In: KREMER, J.-F.; MÜLLER, B. (Org.). **Cyberspace and International Relations**: Theory, Prospects and Challenges. Berlim: Springer, 2014.

MELZER, Nils. **Cyberwarfare and International Law**. Genebra: UNIDIR, 2011.

METZ, Steven; KIEVIT, James. **Strategy and the Revolution in Military Affairs from Theory to Policy**. Carlisle Barracks: Strategic Studies Institute, U.S. Army War College, 1995.

REID, Julian. Foucault on Clausewitz: Conceptualizing the Relationship Between War and Power. **Alternatives**, n. 28, p. 1-28, 2003.

RID, Thomas. Cyber War Will Not Take Place. **Journal of Strategic Studies**, v. 35, n. 1, p. 1-28, 2012.

____. Cyberwar and Peace: Hacking Can Reduce Real-World Violence. **Foreign Affairs**, 1º dez. 2013. Disponível em: <https://www.foreignaffairs.com/articles/2013-10-15/cyberwar-and-peace>. Acesso em: 20 jan. 2015.

SCALERCIO, Márcio Antonio. **As armas e as consciências**. Tese (Doutorado em Relações Internacionais) – Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio), Rio de Janeiro, 2015.



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015

SHAHEEN, Salma. Offense-Defense Balance in Cyber Warfare. In: KREMER, J.-F.; MÜLLER, B. (Org.). **Cyberspace and International Relations**: Theory, Prospects and Challenges. Berlim: Springer, 2014.

TOWNSHEND, Charles. The Shape of Modern War. In TOWNSHEND, Charles (Org.). **The Oxford History of Modern War**. Oxford: Oxford University Press, 2000.

WIENER, Norbert. **The Human Use of Human Beings**: Cybernetics and Society. Londres: Free Association Books, 1989.

# Resumo

## A Ciberguerra É Moderna! Uma Investigação sobre a Relação entre Tecnologia e Modernização na Guerra

O presente artigo investiga o papel da tecnologia na modernidade a partir do fenômeno da ciberguerra. Argumenta-se que o processo de modernização tem por característica a conjunção entre guerra, ciência e tecnologia e que a incorporação da cibernética à guerra é representativa disso. Para tanto, procede-se a uma genealogia da ciberguerra, o que permite investigar as significações constitutivas do atual discurso, bem como analisar suas condições de possibilidade. Esse primeiro movimento permite situar a cibernética enquanto alicerce no desenvolvimento das práticas de guerra e como tropo capaz de influenciar o imaginário militar a seu respeito. Finalmente, o fenômeno é situado no contexto mais amplo das transformações da guerra na modernidade, apontadas por Bousquet (2009) e as quais destacam o papel central da tecnologia no guerrear moderno. Isso permite problematizar a forma como a ciberguerra se articula ao imaginário de não violência presente nas teorias da modernização.

**Palavras-chave**: Ciberguerra – Tecnologia – Modernidade – Guerra – Violência

Luisa Lobato e Kai Michael Kenkel

# Abstract

## Cyberwar Is Modern! An Investigation into the Relationship between Technology and Modernization in War

This article investigates the role of technology in modernity based on the phenomenon of cyberwar. We argue that the conjunction of war, science and technology is a defining characteristic of the modernization process and that the incorporation of cybernetics into warfare is representative of this. In doing so, we establish a genealogy of cyberwar, which allows the study to investigate constitutive signifiers within current discourses, as well as analyzing its permissive conditions. This first step situates cybernetics as fundamental to the development of practices of warfare and as a trope capable of influencing the military imaginary. Finally, the phenomenon is situated in the broader context of the changes in warfare in modernity, highlighted by Bousquet (2009), which underscore the central role of technology in modern warfare. This allows for the problematization of the way in which cyberwar relates to the discourse on non-violence that permeates theories of modernization.

**Keywords**: Cyberwar – Technology – Modernity – War – Violence



Contexto Internacional (PUC)
Vol. 37 nº 2 – mai/ago 2015
1ª Revisão: 27/04/2015