As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica

The three trends of cyberwarfare: new domain, combined arms and strategic weapon

DOI: 10.21530/ci.v12n3.2017.620

Augusto W. M. Teixeira Júnior[1]
Gills Vilar-Lopes[2]
Marco Túlio Delgobbo Freitas[3]

Resumo

O presente trabalho analisa como a guerra cibernética impacta a conduta da guerra hodierna. Partindo da teoria da guerra de Clausewitz e dos debates sobre revolução dos assuntos militares e poder aéreo, postulam-se três tendências com distintos níveis de modificação das formas de beligerância advindos do ciberespaço. A primeira delas se refere à criação de um *novo domínio*, o cibernético. A segunda vislumbra a incorporação do ciberespaço à guerra enquanto *arma combinada*, ou seja, incorporando-a aos instrumentos de força convencionais para a produção de efeitos cinéticos. A terceira tendência estipula o uso da guerra cibernética como uma *arma estratégica*, em moldes pareios aos da estratégia de dissuasão nuclear. Em termos metodológicos, a pesquisa se baseia, em primeiro plano, na revisão bibliográfica da literatura de segurança internacional e guerra cibernética e, secundariamente, na análise histórica dos seguintes acontecimentos recentes: Rússia-Estônia (2007), Rússia-Geórgia (2008), Stuxnet (2010) e Rússia-Ucrânia (2014). Objetiva-se assim construir um quadro de análise para melhor compreender como o fenômeno da guerra cibernética afeta a conduta da guerra do século XXI.

Palavras-chave: Guerra Cibernética. Ciberespaço. Conduta da Guerra. Segurança Internacional. Tendências.

1 Doutor em Ciência Política (UFPE). Professor do Programa de Pós-Graduação em Ciência Política e Relações Internacionais (PPGCPRI/UFPB) e do Departamento de Relações Internacionais (DRI/UFPB), em João Pessoa/PB, Brasil. Coordenador do Grupo de Pesquisa em Estudos Estratégicos e Segurança Internacional (GEESI/UFPB/CNPq). Contato: augustoteixeirajr@gmail.com.

2 Doutor em Ciência Política (UFPE). Grupo de Estudos de Defesa e Análises Internacionais (GEDAI) do Departamento de Ciências Sociais (DCS) da Universidade Federal de Rondônia (UNIR), em Porto Velho/RO, Brasil. E-mail: gills@gills.com.br.

3 Mestre em Relações Internacionais (UFF). Professor do Instituto Nacional de Pós-Graduação (INPG). Pesquisador do Instituto Pandiá Calógeras e GEESI (CNPq/UFPB). Contato: marcotuliodf@hotmail.com.

Artigo submetido em 07/02/2017 e aprovado em 08/05/2017.

Abstract

This work analyzes how cyberwar impacts the conduct of modern warfare. Departing from Clausewitz Theory of War and the debates on Revolution in Military Affairs and Air Power, three trends are posited in which different levels of modification of the forms of belligerence coming from the cyberspace are attested. The first one refers to the creation of a new domain, the cyber domain. The second trend envisions the development of the cybernetic means combined with conventional weapons able to produce kinetic effects. The last trend stipulates the use of cyberwar as a strategic weapon, like the nuclear deterrence strategy. These trends are based on historical accounts of international security and cyberwar literature, as: Estonia (2007), Russia versus Georgia (2008), Stuxnet (2010) and Russia versus Ukraine (2014). The objective here is to build a framework for a better understanding of how the phenomenon of cyberwar affects the conduct of war in the 21st-century.

Keywords: Cyberwar. Cyberspace. Conduct of War. International Security. Trends.

Introdução

O panorama do pós Guerra Fria trouxe desafios explanatórios e disciplinares às relações internacionais, especialmente aos estudos estratégicos e de segurança internacional. Atualmente, observa-se o crescente interesse por pesquisas em relações internacionais sobre o ciberespaço, especialmente em seu aspecto securitário (PORTELA, 2016, p. 108). Na perspectiva do debate sobre transformações na conduta da guerra, as ideias de "redução da fricção" e "distanciamento do *front*" (PERON, 2016) são a ponta de lança da chamada revolução dos assuntos militares (RAM), ou *revolution in military affairs* (RMA), da qual a guerra cibernética é caudatária. No plano contextual, alguns países e organizações passaram a considerar o ciberespaço como um domínio combatente, produzindo, assim, mudanças institucionais, estratégicas e doutrinárias. Como exemplos dessa inclinação de pensamento estratégico-militar, citamos o *U.S. Cyber Command* (USCYBERCOM), o *Cooperative Cyber Defence Centre of Excellence* (CCD COE) da Organização do Tratado do Atlântico Norte (OTAN) e a nova arma — ou ramo (*branch*) — chinesa para combater no ciberespaço[4].

Pode-se definir guerra cibernética como um estado de coisas em que o poder militar utiliza meios, estratégias e ferramentas no ciberespaço para alcançar seus objetivos. Tal definição ampara-se na concepção mais ampla de poder cibernético,

4 Cf. Estados Unidos da América (2016), Minárik (2016) e SPUTINIK (2016), respectivamente.

ou *cyber power* (SHELDON, 2013), que diz respeito ao uso estratégico do ciberespaço. Nessa perspectiva, a guerra cibernética é uma modalidade beligerante de uso e atuação predominantes do ambiente cibernético para obter informações privilegiadas e/ou desestabilizar sistemas computadorizados de um país[5].

Este trabalho pretende demonstrar como, no limiar do século XXI, atores estatais — e terceiros a seu mando — utilizam tais meios de força em ações político-estratégicas. Nesse sentido, o problema de pesquisa indaga: como a tecnologia cibernética pode transformar a conduta da guerra?

Acreditamos que essa reflexão impõe três grandes problemas aos estudos estratégicos e de segurança internacional, no sentido de que o ciberespaço:

1. revolucionaria a conduta da guerra, mitigando a relevância dos domínios clássicos da terra, mar, ar e espaço sideral;
2. permitiria alcançar a vitória militar sem dispêndio de muita energia cinética; e
3. faria emergir uma mudança paradigmática na própria conduta da guerra, semelhante ao emprego dissuasório das armas nucleares.

Ao explanar cada uma dessas questões, analisamos três tendências que englobam os impactos da tecnologia cibernética no pensar e agir militares. A primeira delas diz respeito à assunção doutrinária de que o ciberespaço é um novo domínio (MINÁRIK, 2016), do qual se pode traçar um paralelo com a incorporação do "ar" como nova dimensão da guerra. A segunda tendência vislumbra o desdobramento dos meios cibernéticos, combinados aos instrumentos convencionais de força voltados à conduta da guerra (LANGNER, 2011). E a derradeira tendência estipula a guerra cibernética como uma arma estratégica (KREPINEVICH, 2012), em moldes pareios ao nuclear, para retirar do combate o fulcro da dinâmica bélica.

O percurso teórico deste artigo dialoga com a história da guerra cibernética à luz dos debates sobre transformação militar[6]. Dado que esse tema é recente nas relações internacionais, não é possível afirmar a existência de teorias robustas acerca do fenômeno da guerra cibernética (SHELDON, 2013). Logo, as

5 Nessa definição de guerra cibernética como domínio, seus efeitos e empregos são ligeiramente diferentes, quando considerada enquanto arma combinada ou estratégica.

6 "O termo 'transformação militar' pode simplesmente ser entendido como uma 'profunda mudança' nos assuntos militares. Não seria necessária uma mudança rápida ou de amplo escopo, nem o descarte daquilo que ainda funciona bem. As mudanças, no entanto, deveriam ser dramáticas ao invés de aprimoramentos marginais como melhores aeronaves, carros de combate ou navios. Transformação é um processo sem um ponto final" (DAVIS, 2010, p. 11, tradução nossa).

ferramentas conceituais e analíticas disponíveis encontram-se mais na história e na revisão da literatura do que em um edifício teórico bem consolidado. Por tal razão, focamos a literatura especializada em guerra cibernética, mantendo um diálogo com a teoria política da guerra clausewitziana. Essa opção conduzirá o trabalho a uma preferência por autores representativos do esforço de conexão do fenômeno da guerra cibernética com construtos conceituais e doutrinários dos estudos estratégicos e de segurança internacional[7].

No que tange à metodologia, este trabalho pauta-se no estilo qualitativo de pesquisa, em que pesem os métodos da pesquisa bibliográfica — cuja análise busca identificar tendências de um fenômeno a partir da categorização da literatura especializada (VAN EVERA, 1997) — em estudos estratégicos e da análise histórica de acontecimentos emblemáticos ao tema, envolvendo a Rússia — Estônia em 2007, Geórgia em 2008 e Ucrânia em 2014 — e o *worm*[8] Stuxnet em 2010, reconhecido como a primeira arma cibernética. O objetivo aqui não é aplicar a metodologia de estudo de caso (GEORGE; BENNET, 2005) ou de política comparada de *small-N* (LANDMAN, 2008) e, sim, extrair as principais tendências sobre o impacto da guerra cibernética na conduta da guerra e, portanto, na segurança internacional.

Em perspectiva histórica, a primeira seção apresenta a guerra cibernética no contexto do debate sobre RAM. Com base na literatura, a segunda seção explica a função metodológica da analogia entre os espaços cibernético e aéreo enquanto domínios militares. Como resultado dessa base no pensamento estratégico, a terceira seção analisa as três tendências da incorporação do ciberespaço na conduta da guerra, quais sejam: novo domínio, arma combinada e arma estratégica.

Revolução nos assuntos militares e poder aéreo: modelos para a incorporação do ciberespaço à conduta da guerra

Analisamos agora o fenômeno do qual o tema em tela é uma expressão: a guerra. Apesar de quase 200 anos da publicação da *magnum opus* de Clausewitz (2010), sua teoria política da guerra ainda se mostra assaz útil para o pensar estratégico. Segundo ele, a guerra é um ato de força voltado a submeter o inimigo à

7 Por isso, não damos muita atenção ao pensamento estatal sobre o tema. Contudo, dada a relevância da matéria, futuros artigos abordarão tal aspecto.

8 *Worms* são programas de computador que facilitam a intrusão em sistemas de *hardware* e roubam informação desses (LOBATO; KENKEL, 2015, p. 27).

nossa vontade. Para Clausewitz (2010), a guerra é, ao mesmo tempo, um fenômeno político e uma atividade social. Não obstante o combate ser o principal meio da guerra, essa era composta pela interação de distintas instâncias políticas, militares e sociais combinadas a diferentes motivações no tocante ao evento bélico. Essa "trindade" clausewitziana é formada, portanto, por governo, militares e povo, os quais se movem, respectivamente, pela razão, probabilidade e paixão.

Instituições, interesses e paixões contribuíam para estruturar as dimensões materiais e psicológicas da guerra. Seu significado é mediado por idiossincrasias sociais e temporais. Para Clausewitz (2010), tal fenômeno é marcado pelo uso instrumental da violência, direcionada e justificada politicamente. Se o combate é o principal meio da guerra, como reduzir o desgaste humano e material ao longo dos engajamentos? Como apreender em profundidade a realidade do campo de batalha, no sentido de ver além da colina? *Fricção*[9] e *névoa da guerra*[10] são tanto limitadoras do pleno uso da força — guerra absoluta — quanto partes indeléveis dos desafios enfrentados por comandantes militares, desde tempos imemoriais, em sua busca pela vitória. Apesar de considerar importante a evolução tecnológica, Clausewitz (2010) era cético quanto à capacidade de esse vetor afetar a natureza da guerra. Por outro lado, entendia que avanços tecnológicos poderiam, sim, ser fundamentais para alterar a conduta da guerra. É nesse sentido que a conexão entre tecnologia e mudanças dos assuntos militares apresenta-se útil para pensar transformações referentes ao uso político da força, que, neste caso, referem-se ao advento da era da informação e da guerra cibernética. Considera-se que a RAM seja um importante ponto de partida para entender como mudanças tecnológicas — evolutivas ou revolucionárias —, sociais e políticas afetam as formas de se fazer a guerra.

Antes mesmo da popularização do tema RAM nos Estados Unidos da América (EUA), Brzezinski (1989) já destacava o papel da dianteira tecnológica estadunidense como fundamental para a vitória na confrontação bipolar. A leitura de Brzezinski (1989) sobre o colapso da União das Repúblicas Socialistas Soviéticas (URSS) dialoga com uma transformação profunda nas relações internacionais, a saber: a revolução da informação.

9 Em analogia à física, Clausewitz (2010) afirma que a fricção na guerra é a força que torna coisas fáceis, difíceis. Fatores físicos — como clima e relevo — e psicológicos — a exemplo de moral e medo — competiam para diferenciar a "guerra real" da "guerra no papel".

10 Definida por Clausewitz (2010), "névoa da guerra" — *nebel des kriegs* — caracteriza-se pelas incertezas das reais intenções inimigas, ou seja, é a falta de conhecimento dos planos adversários que podem gerar grande desperdício de recursos.

Com a substituição de sistemas analógicos por digitais, a incorporação da computação nos sistemas de comando e controle (C^2) e a eficiência produtiva do capitalismo ocidental, a nova revolução tecnológica empurrava o mundo à era da informação, com profundos impactos também na arte da guerra. Por exemplo, a internet, surgida no contexto da Guerra Fria, passa ao domínio público ainda nos anos de 1980 e se populariza nos de 1990, quando a luta contra as ameaças cibernéticas toma dimensões políticas (LOBATO; KENKEL, 2015, p. 38). Emergia lentamente um novo paradigma de combate, característico dessa nova era, a *information warfare* (BELLAMY, 2001).

No marco dos debates sobre transformação militar (SLOAN, 2012), a *information warfare* é um paradigma de beligerância em que os antagonistas "combatem" em um ambiente de informação, no qual as dinâmicas ofensivas e defensivas se caracterizam sobretudo pela busca de aquisição e degradação de informações e pelo uso de sistemas inimigos e negação de acesso. É nesse contexto que se tornam possíveis a inserção do ciberespaço nas doutrinas militares e o surgimento de novas formas de combate, a exemplo do previsto pela ideia de "guerra de terceira onda" (PERON, 2016), na qual a supremacia da informação seria primordial para a vitória.

Diante desse quadro, podemos contextualizar o surgimento da tecnologia cibernética no âmbito da RAM. Porém, cabe diferençar "evolução" e "revolução" em assuntos militares. De acordo com Andrews (1998), a diferença reside na maturação da tecnologia na condução da guerra. A evolução militar ocorre, segundo o autor, quando se aplicam novas tecnologias na guerra, que levam gerações para atingir o seu ápice. Em contraste com essa leitura gradualista, surgiu na União Soviética o entendimento de que a introdução de tecnologias poderia provocar *mudanças drásticas* na forma de guerrear (PROENÇA JR; DINIZ; RAZA, 1999). Historicamente, a gênese da ideia da RAM[11] é atribuída ao marechal soviético Nikolay V. Ogarkov, o qual sugere, em 1980, que a revolução[12] tecnomilitar em curso nos anos de 1970-80 se explicava pelo desenvolvimento de munições guiadas com precisão, pelos avanços tecnológicos na área de vigilância e pelos sistemas de distribuição de informações (PROENÇA JR; DINIZ; RAZA, 1999). Portanto, uma RAM ocorre

11 Apesar de semelhantes, a expressão *Military-Technical Revolution* (MTR) — de origem soviética — seria substituída nos Estados Unidos pelo conceito de RAM, cunhado por Andrew W. Marshall, diretor do gabinete de aviação do *U.S. Department of Defense* (ANDREWS, 1998).

12 No âmbito da "ciência militar" soviética, a análise do processo da evolução dos assuntos militares ganhou a alcunha de "revolução" devido a uma questão ideológica. Por uma analogia à própria Revolução Russa, eles valorizavam a palavra "revolução" como uma forma essencial de progresso da história.

quando a nova tecnologia é inserida no âmbito doutrinário e organizacional, provacando mudanças revolucionárias (ANDREWS, 1998).

A RAM mostra-se, portanto, politicamente atraente no período pós Guerra Fria, pois promete maiores poder de fogo e eficácia militar com menos custos, maior capacidade expedicionária e mais rapidez na condução de operações militares regionais (LILES et al., 2012). O predomínio de guerras caracterizadas pela assimetria das capacidades entre beligerantes e a heterodoxia estratégico-tática introduzem múltiplos desafios para o conflito e as forças armadas que, ao largo dos debates acadêmicos, já incorporam o domínio cibernético à conduta da guerra[13]. No contexto em que o ambiente virtual guarda e protege informações sensíveis e desempenha papel fundamental à gerência de áreas importantes da defesa nacional, o ciberespaço se torna também um novo *front*, meio ou domínio, a partir do qual é possível produzir efeitos estratégicos (SHELDON, 2013).

Independentemente das possibilidades de evolução ou revolução das dinâmicas de transformação militar, persiste a necessidade de influenciar o inimigo, por meio da possibilidade ou do direto uso da força como lógica inerente à guerra (CLAUSEWITZ, 2010). Ao analisar a história militar, percebemos que, apesar das inovações e transformações castrenses, seus protagonistas basicamente perseguiam o mesmo objetivo, a saber: a vitória na guerra, seja ela de tipo ilimitada ou limitada (BIDDLE, 2010; CLAUSEWITZ, 2010). É preciso, pois, compreender como a tecnologia contribui para a contemplação desse objetivo. Consoante Proença Jr (2011, p. 182), "vir a ter vantagens combatentes a partir de promessas tecnológicas é o que anima uma grande parte do projeto de força, e isso depende da exploração do desempenho técnico de artefatos, sistemas e pessoal", ou seja, para a esfera militar, é necessário saber como uma tecnologia será utilizada, e, para isso, deve-se prioritariamente compreender suas promessas e limites. Com o ciberespaço não é diferente. O processo de incorporação de uma nova tecnologia no campo de batalha é normalmente incentivado e saudado por entusiastas que, na tentativa de compreender seu potencial emprego, acabam "hiperdimensionando" suas potencialidades, como possivelmente ocorre com o ciberespaço.

Apesar de a literatura revisada observar impactos estratégicos do ciberespaço nos conflitos armados contemporâneos, alguns autores, como forma de melhor avaliar os desdobramentos dessa nova dimensão da guerra, voltam-se para o

13 Como é o caso do acordo cibernético celebrado entre China e EUA em 2015 (KASPERSEN, 2015).

surgimento de novos vetores de força nos domínios tradicionais[14]. Entre esses, destaca-se o domínio aéreo, cuja comparação histórica mostra-se metodologicamente útil para o estudo do ciberespaço na ótica dos estudos estratégicos.

Apesar de a discussão sobre guerra cibernética ser relativamente recente na academia, pode-se compará-la ao desafio que o surgimento do poder aéreo legou às relações internacionais e aos estudos estratégicos em seu tempo. Se, nos anos de 1950 e de 1960, o desenvolvimento de vetores de entrega de armamento nuclear relativizava a compreensão então acordada sobre os limites geográficos para a projeção do poderio militar, é com a aviação que surge o grande debate sobre revolução militar na primeira metade do século XX[15]. Tanto as guerras no ar quanto no ciberespaço questionam o peso condicionante da geografia sobre a estratégia e a condução de operações militares. Embora criticada, a ideia da "real possibilidade de uma guerra restrita aos domínios adjacentes, como o cibernético" (BOHN; NOTHEN, 2016, p. 90) vem motivando maiores investigações sobre a relação ciberespaço-guerra.

O poder aéreo surge, então, com a promessa revolucionária de perceber, conduzir e vencer guerras. As ideias de que o ar constituiria um domínio novo e que o bombardeio seria a arma definidora da guerra do futuro demonstravam uma clara tendência à hiperestimação (MACISAAC, 2003). Após a Primeira Grande Guerra, o avião, inicialmente uma inovação tecnológica, gera condições para a incorporação de um novo domínio, o ar. Semelhantemente ao debate hodierno acerca da guerra cibernética, as discussões entre a comunidade de estrategistas e planejadores militares sobre essa nova realidade não é conclusiva. Nesse ponto, a evolução patente ao poder aéreo, de uma arma subordinada às demais em direção à constituição de domínio e arma independente — estratégica —, mostra-se útil para ponderar como o ciberespaço afeta a conduta da guerra atualmente. Embora a instrumentalidade da comparação entre, de um lado, domínios aéreo e cibernético e, do outro, o surgimento da guerra no ar e no ciberespaço, seja útil para analisar tendências, apresentamos os limites dessa comparação, em virtude de características peculiares do ciberespaço em relação aos demais domínios.

14 Liles et al. (2012) são representativos dos que adotam a aplicação de princípios tradicionais da guerra terrestre para entender a cibernética. Bohn e Nothen (2016) preferem a analogia do ciberespaço como um "espaço comum", advinda das teorias do poder marítimo. Já Birdwell e Mills (2011) discutem a guerra cibernética tendo em tela o acumulado teórico sobre o poder aéreo.

15 Ao postular as caraterísticas revolucionárias da aviação militar como arma estratégica, Giulio Douhet é um dos teóricos do século XX que melhor representam a articulação entre tecnologia e quebra de paradigmas na conduta da guerra (MACISAAC, 2003).

Ao contrário dos domínios tradicionais, o cibernético é uma criação humana, presente em vários meios: do *pen drive* à "nuvem" (LIBICKI, 2012). Distintamente do que postulam Liles et al. (2012), ao pleitear subordinar as operações cibernéticas de acordo com os princípios da guerra terrestre[16], a capacidade de moldar o ciberespaço torna-se mais importante que o poder de fogo ou de manobra (LIBICKI, 2012). Enquanto os domínios tradicionais impõem diversos custos de operação para atores não estatais, o ciberespaço se caracteriza por: baixo custo de entrada em operação, atuação *multistakeholder* e fluidez extremada (SHELDON, 2013). É, portanto, o domínio em que se cria, armazena, transmite e manipula a informação e em que o poder cibernético converte a informação em efeito estratégico (SHELDON, 2011, p. 306).

De acordo com Libicki (apud Sheldon, 2013), o ciberespaço compõe-se de três camadas:

1. física: *hardware*, cabos, satélites, roteadores e outros componentes infraestruturais;
2. sintática: código/*software* que formata, instrui e controla informação; e
3. semântica: interface ciberespaço-humana em que a informação é dotada de significado/sentido para seres humanos.

O controle, contudo, de uma das camadas do ciberespaço não confere domínio sobre as outras (LIBICKI apud SHELDON, 2013, p. 304). Entretanto, o emprego militar dos vetores cibernéticos contribui para incrementos de força ou acessórios ao seu emprego no campo de batalha, tais como: melhoria da qualidade de coleta de dados dos serviços de inteligência, precisão e rapidez de ataques teleguiados, proteção de estruturas estratégicas de informação[17] e avanço na capacidade de C^2 (BIRDWELL; MILLS, 2011). Essas são tarefas a que o uso da tecnologia cibernética pode contribuir, acarretando possível diminuição da névoa da guerra (COHEN, 2010). Como contraste, o excesso de informação, que dificulta o gerenciamento de dados entre centros de C^2 e forças combatentes, pode, na verdade, aumentar a névoa da guerra. Esse efeito, que reforça o ceticismo clausewitziano quanto à névoa da guerra, é chamado de *digital divide* (BIDDLE, 2010).

16 São estes os nove princípios: objetivo, ofensiva, massa, economia de força, manobra, unidade do comando, segurança, surpresa e simplicidade.

17 Estruturas estratégicas — ou infraestruturas críticas — de informação são componentes necessários a: transmissão de informações, redes de banda larga e satélites; sistemas de comunicação; e computadores, televisores, telefones, rádios e outros produtos que viabilizam o acesso a esses serviços.

Outro possível *input* que a guerra cibernética traria à conduta bélica diz respeito à preferência estratégica. O conjunto das características expostas acima apresenta oportunidades expressivas para a ocorrência de operações ofensivas e, em contrapartida, dificulta ações defensivas. Para Libicki (2012, p. 323), as operações cibernéticas desse tipo, que exploram as vulnerabilidades dos sistemas-alvo, evidenciam a capacidade ofensiva que o ciberespaço enseja nos assuntos militares, mundo afora. Distintamente da preferência pela defesa encontrada na leitura clausewitziana, autores como Birdwell e Mills (2011), Liles et al. (2012) e Sheldon (2013) concordam ao enfatizar que a ofensiva é a forma dominante de guerrear no ciberespaço. Ataques mecânicos, eletromagnéticos ou digitais podem originar-se do ciberespaço, oscilando desde a produção de efeitos cinéticos até virtuais.

Apesar dessa euforia, Liles et al. (2012) abordam a questão de a literatura não possibilitar afirmar se a guerra cibernética é o uso do ciberespaço como domínio para o combate (BIRDWELL; MILLS, 2011) ou é o próprio combate no domínio do ciberespaço (LIBICKI, 2012). Como se observa, o fenômeno associado ao surgimento do poder aéreo e sua promessa revolucionária, a hiperestimação retorna contemporaneamente com foco no ciberespaço. Atualmente, grande parte da literatura sobre o uso estratégico-militar do ciberespaço coloca essa nova dimensão do conflito não só como revolucionária, mas igualmente como apocalíptica[18]. Outro aspecto relevante consiste nas perspectivas mais otimistas quanto à incorporação do ciberespaço na conduta das operações militares — tais perspectivas apresentam a guerra como um fenômeno não trinitário. Consoante tal visão, a guerra no ambiente cibernético poderia ser travada sem a interferência de um dos entes da trindade clausewitziana (SLOAN, 2012).

Para melhor analisar os desdobramentos desses debates, expõem-se a seguir as três principais tendências da condução da guerra cibernética.

Três tendências para se pensar a conduta da guerra no ciberespaço

Analisamos as seguintes tendências contemporâneas da guerra cibernética: (1) expressão do predomínio do novo domínio cibernético, operando como arma independente; (2) apenas nova ferramenta para alcançar a vitória em "velhos domínios", na forma de arma combinada; e (3) arma estratégica.

18 Sobre o cenário extremado de *cyber Pearl Harbor,* ver Bumiller e Shanker (2012) e Clarke e Knake (2015).

Primeira tendência: guerra cibernética como novo domínio militar

Desde a primeira Guerra do Golfo, impera no debate estratégico-militar a percepção de que a RAM seria dominada pela supremacia dos vetores aéreos de força e pela integração de sistemas de C^2 nos âmbitos cibernético e material. A Guerra do Iraque, de 1991 a 1992, deixa claro, no que tange à literatura consultada, que importantes transformações na conduta da guerra estavam em curso àquela época (SLOAN, 2012).

Associado ao advento da guerra centrada em redes (GCR), dava-se cabo à revolução do "sistema dos sistemas" (COHEN, 2010). A fim de compreender essas transformações tecnobélicas, Bellamy (2001) formula uma tipologia das formas de GCR[19], a qual pode ser aproveitada também para se pensar prospectivamente modelos de emprego do ciberespaço na guerra contemporânea. Para Liles et al. (2012, p. 172), a GCR aumenta o escopo e a visão do estrategista, haja vista que lhe proporciona a capacidade de utilizar a computação ubíqua para tomar decisões e comunicar-se no campo de batalha. É nesse contexto que se alça o ciberespaço à condição de novo domínio estratégico (BOHN; NOTHEN, 2016; KASPERSEN, 2015). Na era da informação, as infraestruturas de rede fazem parte do repertório de questões estratégicas (BOHN; NOTHEN, 2016), constituindo, possivelmente, um novo *front*.

Novas ferramentas e processos impactam a arte da guerra. Instrumentos, como as chamadas armas cibernéticas, proporcionam aquisição de informação necessária para o campo de batalha. Contudo, suas consequências precisam ser entendidas também na esfera estratégica. Desse modo, Liles et al. (2012, p. 172) salientam que se deve entender a guerra cibernética como um conjunto de operações centradas em informação em que ações ofensivas e defensivas contra centros de C^2 predominam. Assim, a informação é um produto importante no *front*. Com informação precisa, um comandante desdobra suas forças, projeta seus contingentes contra os pontos vulneráveis do inimigo, alcança a vitória. Para o tomador de decisão civil, a informação é igualmente vital, pois, com ela, formula melhor os objetivos para alcançar os fins políticos, via o emprego da força. A informação, portanto, tem o potencial de mudar o comportamento dos atores, violentamente ou não. Eis aí a essência dos que defendem a guerra cibernética como novo domínio de operações militares.

19 São elas: *C^2 warfare*, *software warfare* e *informational warfare* (BELLAMY, 2001).

De forma a testar preliminarmente o uso do domínio cibernético em conflitos contemporâneos, discutem-se três eventos representativos, quais sejam: os impactos dos vultosos ataques cibernéticos sofridos pela Estônia em 2007; a ofensiva militar, precedida por ataques cibernéticos, da Rússia na Geórgia em 2008; e a empreitada bélica russa no ciberespaço ucraniano em 2014.

É ponto relativamente pacífico, na literatura de segurança internacional, que a crise na Estônia em 2007 constitui um marco nos estudos sobre guerra cibernética (CLARKE; KNAKE, 2015; LIBICKI, 2012; NYE JR, 2008). Estopim do conflito cibernético, o governo estoniano removeu uma estátua em homenagem aos soviéticos mortos na Segunda Guerra Mundial, do centro da capital, Tallinn, para um cemitério afastado, culminando com protestos russófonos no país e na Rússia. Ataques virtuais afetaram negativamente o funcionamento das infraestruturas de TIC da Estônia, comprometendo seus serviços derivados. Como frisam Clarke e Knake (2015) e Oppermann (2010), a Estônia detinha uma das mais modernas infraestruturas de TIC do mundo, mas os ataques cibernéticos foram tão impactantes que a OTAN investigou o caso e criou o CCD COE, em Tallinn. Nesse ínterim, o governo estoniano acusou veementemente Moscou pelos atentados à sua "soberania cibernética". Apesar de nunca ter sido provada a atribuição dos ataques, a capacidade de poder cibernético (LIBICKI, 2012) contra a Estônia dificilmente poderia ter sido conduzida sem o auxílio de um grande *player* estatal. Embora Clarke e Knake (2015) apontem para essa direção, Moscou continua negando participação (CROFT; APPS, 2014).

Destacamos duas ponderações sobre esse caso. Primeiro, devido ao tipo de ataque cibernético usado — DDoS[20] —, não se pode concluir acerca da participação do governo russo. Segundo, embora não tenham ocorrido ataques convencionais, com efeitos cinéticos, antes ou depois dos vultosos ataques cibernéticos, esse caso, ainda assim, é emblemático, para os estudos internacionalistas e estratégicos, ao demonstrar como um Estado altamente conectado ao ciberespaço, especialmente à internet, pode ter suas estruturas estratégicas de TIC seriamente danificadas em um cenário de guerra cibernética.

A configuração do ciberespaço como um novo *front*, atrelado a um domínio independente na guerra, tem no caso da Estônia o seu teste inicial. Apesar disso,

20 Conhecido por *distributed denial-of-service* (DDoS), ou negação de serviço, "que ocorre a partir da sobrecarga do sistema[,] e não de uma invasão. Geralmente, um computador[-]mestre comanda milhares de computadores denominados zumbis, que passam a funcionar como máquinas escravizadas" (GAMA NETO; VILAR LOPES, 2014, p. 76).

um ano depois, outro *case* demonstra a progressiva, porém não totalmente comprovada, articulação do ciberespaço com efeitos cinéticos. Em 2008, a república da Geórgia envolve-se em uma onda de ataques virtuais. Diferentemente da Estônia, tais ataques foram o prelúdio de uma guerra convencional. Pela primeira vez, uma ofensiva em domínios tradicionais foi precedida por ataques na dimensão cibernética. Um mês antes dessa ofensiva militar russa, em julho de 2008 (OPPERMANN, 2010), a infraestrutura de TIC georgiana foi severamente danificada. Com o sistema sob ataque, não só serviços *online* nacionais, mas também fornecedores internacionais, receosos, desligam-se do Estado georgiano. Com seus sistemas de informação e comunicação enfraquecidos, ficou ainda mais difícil para a Geórgia mobilizar-se e, consequentemente, defender-se dos ataques convencionais. Sobre tais eventos, Nye Jr (2008) afirma ser esse o evento que abre caminhos sem precedentes para se compreender a guerra cibernética como uma das facetas da conduta da guerra no século XXI.

Outro evento seria ainda mais elucidativo sobre a tendência do ciberespaço como domínio de operações. Imerso na conjuntura da aguda crise política sobre a anexação da Crimeia, e da posterior guerra civil ucraniana, Moscou toma medidas para controlar a segurança daquele importante espaço geoestratégico de projeção de poder russo, especialmente no Mar Negro. Em março do mesmo ano, a maioria da população da Crimeia vota pela secessão da Ucrânia e unificação à Rússia. O Secretário-Geral da OTAN, à época, classifica isso como uma possível violação ao direito internacional, ocasionando também a ira de *hackers* "ucranianos", a ponto de alguns *sites* da OTAN serem também tirados do ar, por meio do já utilizado — tanto na Estônia quanto na Geórgia — ataque DDoS (CROFT; APPS, 2014).

No âmbito dos estudos estratégicos, a questão se mostra ainda mais complexa quando especialistas em segurança da informação afirmam que as redes de computadores do governo ucraniano foram ocultamente monitoradas pelo Kremlin, anos antes de a crise da Crimeia estourar (JONES, 2014). A descoberta de que um *software* malicioso (*malware*) estaria silenciosamente sabotando sistemas informacionais da Ucrânia foi feita pelo BAE Systems, braço tecnológico das forças armadas britânicas, que cunhou o nome "Snake" para designar esse que é, na verdade, um *kit* de ferramentas de espionagem cibernética (BAE SYSTEMS, 2014, p. 6). Tais análises mostram que o *Snake* infectou máquinas de nove países[21] (BAE SYSTEMS, 2014, p. 6). Com base nos dados fornecidos pela empresa,

21 Bélgica, EUA, Geórgia, Grã-Bretanha, Hungria, Itália, Lituânia, Romênia e Ucrânia.

percebe-se que: (i) a Ucrânia é o primeiro e o mais infectado dos países; (ii) a Rússia, principal alvo de *malwares* no mundo, sequer teve uma única infecção; e é justamente em 2014, na Ucrânia, que o *Snake* mais se manifesta, ou seja, envia informações capturadas para um receptor remoto. As conclusões sobre o *Snake* seguem a mesma lógica das de outras "armas cibernéticas", *i.e.*, a existência de arquitetura e engenharia de *software* bastante robustas e sofisticadas (BAE SYSTEMS, 2014, p. 26), a ponto de ser altamente improvável ser projetado por pessoas sem alto grau de conhecimento e treinamento fora do ordinário (JONES, 2014), habilidades essas vistas nas principais potências cibernéticas. Entretanto, apesar de ser uma arma cibernética, o *Snake* se distingue do *worm* Stuxnet, por exemplo, por não produzir efeitos cinéticos[22].

Como acontece em 2007, mais uma vez, especialistas em computação apontam a Rússia como principal interessada em saber o que determinados ucranianos faziam e como funcionavam suas redes de C² (JONES, 2014). Registre-se também que o acesso à rede de telefonia móvel e internet na Crimeia sofreu fortes ataques durante toda a crise, de acordo com o próprio governo ucraniano (LEE, 2014). Como ocorrido na Estônia e na Geórgia, a maioria dos analistas militares não duvida que a crise ucraniana marca um ponto-chave na história da guerra cibernética (JONES, 2014).

Como síntese da primeira tendência, pode-se dizer que acontecimentos recentes permitem afirmar que crises e guerras entre Estados e atores não estatais têm envolvido o ciberespaço como novo domínio militar e teatro de operações. Contudo, até o momento, apesar da pertinência das ideias de "eliminação da fricção" prometidas pelo ideário da RAM, a materialidade da guerra cibernética não demonstra ainda expressiva capacidade de comprometer os meios de luta do inimigo, muito menos de produzir vetor estratégico de força capaz de proporcionar vantagens expressivas no campo de batalha. A impossibilidade de identificar, na maioria dos casos, os responsáveis pelos ataques cibernéticos mina a capacidade de se averiguar, com precisão, as relações de causalidade entre domínio cibernético e uso da força cinética. Porém, o fato é que Estados estão tirando proveito do ciberespaço para atuar contra seus inimigos, em particular mediante o uso estratégico da informação — acesso ou negação —, o que leva à nossa segunda tendência.

22 Para Sheldon (2013, p. 312), o Stuxnet comprova que uma capacidade cibernética ofensiva pode mirar, de forma mais ou menos precisa, um sistema remoto, comprometê-lo e causar-lhe destruição física.

Segunda tendência: guerra cibernética como arma combinada

Os acontecimentos analisados para formular a primeira tendência não permitem afirmar, categoricamente, que o ciberespaço, como domínio independente, é capaz de vencer, *per se*, batalhas ou produzir vantagens táticas ou estratégicas significativas a quem o usa. Apesar de os relatos de emprego do ciberespaço como domínio em conflitos contemporâneos recaírem majoritariamente na presumida experiência russa, a vantagem central dessa tendência reside em sua conexão com a GCR e com o processo de transformação militar liderada pelos EUA (SLOAN, 2012).

Com isso em mente, buscamos evidenciar aqui a conexão entre ciberespaço e uso da força, em que se destaca a concepção de "armas combinadas". De acordo com House (2008, p. 21) "o conceito de 'combinação das Armas' é a ideia básica de que diferentes Armas combatentes e sistemas de armas devem ser usados em conjunto para maximizar a sobrevivência e a eficácia em combate uma das outras". No cenário contemporâneo, a guerra cibernética é um instrumento de um outro domínio, o ciberespaço, que se destaca como possível campo de afirmação de novas ferramentas no *front,* mas só produz efeitos cinéticos quando somado ou potencializado por meios de emprego militar convencionais.

Como Clausewitz (2010) argumenta, a violência desferida na guerra se dá por meio da aplicação de meios mais ou menos violentos para atingir objetivos militares, visando alcançar os resultados desejados pela política. À luz dessa afirmação, discorre-se como a combinação entre tecnologia cibernética e força convencional possibilita conquistar objetivos militares. Para tanto, analisa-se o primeiro caso evidente de uso de arma cibernética por e contra um ente estatal: o Stuxnet[23].

Nos últimos anos, as relações entre Israel e Irã caracterizam-se por tensões provocadas pela retomada do programa nuclear iraniano, visto com ressalvas por outros países do Oriente Médio e pela parceria histórica entre Irã e Hezbollah (THOMAS; HECKER, 2009). Nesse caso, por se tratar de um Estado, os estrategistas israelenses buscaram promover a dissuasão[24]. Para isso, a opção mais destacada

23 A autoria do Stuxnet nunca foi oficialmente comprovada. Todavia, fortes indícios apontam para EUA e Israel (SANGER, 2012; CLARKE; KNAKE, 2015, p. 229-233; FORSLING, 2016).

24 Dissuasão é a capacidade de fazer com que um oponente B desista de realizar uma ação que não seja do interesse de A, pois os custos e riscos não seriam compensados pelos ganhos (MEARSHEIMER, 1983). No entanto, tomam-se, aqui, dissuasão e coerção como elementos complementares (PAPE, 1996).

foi o uso de uma arma cibernética, sustentada pela possibilidade de recurso a meios de força convencionais.

A dissuasão sempre foi elemento central da política de defesa israelense. Aliada ao que Thomas e Hecker (2009) definem como "excepcionalismo israelense", a dissuasão serviria para "educar" os oponentes nas vezes em que esses tentassem alterar a "regra do jogo". É nesse cenário que a proposta de desenvolvimento de uma arma cibernética se torna atrativa. Em 2010, o governo iraniano torna pública a sabotagem de centrífugas da central nuclear de Natanz (SHAKARIAN, 2011; LOBATO; KENZEL, 2015, p. 27; PORTELA, 2016, p. 94).

De acordo com Langner (2011), a primeira arma cibernética foi desenvolvida exclusivamente para equipamentos Siemens utilizados no programa nuclear iraniano. Em síntese, a sabotagem cibernética foi planejada para infligir danos físicos em uma peça específica. Outra caraterística desse *malware* é a lentidão em provocar danos, pois não se objetivava parar o programa nuclear iraniano por completo, mas, sim, atrasá-lo.

Descrito como uma arma "atire e esqueça", o Stuxnet foi carregado no sistema operacional das centrífugas de enriquecimento de urânio em Natanz, por meio de *pen drive*. Porém, ao contrário do que entusiastas da guerra cibernética apregoam, a primeira arma cibernética não foi controlada remotamente, pois, para introduzi-la no sistema iraniano, fez-se necessário o recurso humano (LANGNER, 2011), possivelmente por meio da Inteligência israelense.

Além da falta de provas que poderiam responsabilizar Tel-Aviv ou Washington pelos danos causados pelo Stuxnet, havia a preocupação de que a resposta israelense a uma iniciativa iraniana fosse muito custosa (CLARKE; KNAKE, 2015). Embora o resultado da ação do Hezbollah no Líbano em 2006 possa ter corroborado essa percepção, o fato é que a reação de Teerã se restringiu a manifestações públicas de seu presidente.

Novamente, a impossibilidade de afirmar com clareza quem seriam os responsáveis pelo uso de uma arma ou ataque cibernético prejudica a capacidade de realizar inferências seguras. Entretanto, apesar de o ciberespaço, como domínio militar, ainda não produzir efeitos destrutivos em estruturas estratégicas semelhantes ao uso da força convencional, sua combinação com vetores de força materiais potencializa sua capacidade de causar danos. Dessa forma, a interação entre o domínio cibernético e os demais, bem como sua operação no sentido de armas combinadas, apresenta um panorama estrategicamente interessante quanto à sua incorporação à conduta da guerra, para além das missões de observação,

reconhecimento, vigilância e inteligência. Ademais, o caso do Stuxnet aponta para a necessidade de se ter uma estratégia comum que combine armas convencionais e cibernéticas, não apenas no sentido ofensivo, mas também no preventivo. Por isso, nessa tendência, vale recuperar o argumento de Libicki (2012, p. 328) sobre a natureza subsidiária do domínio cibernético em relação aos demais.

Como síntese dessa tendência, afirmamos que considerar o ciberespaço como um domínio combatente pode ser, na maioria dos casos, um equívoco. A guerra cibernética se reforça como auxiliar e combina-se a armas convencionais produtoras de efeito cinético, quando não o faz como domínio de apoio aos tradicionais. Ao considerá-lo como domínio, ao invés de atentar para produzir ou negar efeitos estratégicos advindos desse domínio cujas características intrínsecas o tornam fluído e mutável, o projeto e a estratégia das forças são orientados a buscar a superioridade no ciberespaço. Assim, resta uma terceira tendência da guerra cibernética na conduta da guerra.

Terceira tendência: guerra cibernética como arma estratégica

O terceiro cenário relaciona a compreensão das potencialidades da guerra cibernética à evolução estratégica das nucleares. Apesar de esse campo de investigação ter levado à produção de teorias próprias, em especial às ligadas à dissuasão nuclear, é reconhecida sua origem no âmbito do poder aéreo. Apesar de não vislumbrar um efeito cinético no mesmo nível que o armamento atômico, questiona-se aqui a possibilidade de a guerra cibernética produzir efeitos dissuasórios, tal como as armas nucleares na Guerra Fria. O núcleo dessa lógica é maximizar os benefícios da arma sem usá-la, de forma a prever ou limitar conflitos convencionais.

Em relação ao desenvolvimento da dinâmica de deterrência em torno do campo cibernético, há uma diferença entre o discurso de dissuasão cibernética americano e o israelense (TOR, 2015). No primeiro caso, estadunidenses defendem que dissuadir é influenciar o inimigo mediante uma postura coercitiva, por ser esse um pensamento originário da arma nuclear. Já no segundo, israelenses procuram postergar, limitar e moldar uma série de conflitos, via moderação do inimigo, por meio do emprego limitado da força para controlar o alcance do oponente e adiar a próxima rodada de violência.

Pensar nessa tendência faz sentido se observar-se a evolução do poder nuclear como derivado do pensamento e da teoria do poder éreo[25] (FORSLING, 2016). Similar ao ocorrido com as armas nucleares nos anos de 1940 e de 1950, analistas acreditam que o ciberespaço será o principal teatro de operações da guerra do futuro, retirando do combate físico o mecanismo da vitória (BUMILLER; SHANKER, 2012; CLARKE; KNAKE, 2015). Na prática, a compreensão do ciberespaço como vetor de uma revolução militar, como a nuclear, advoga em favor da reestruturação radical das organizações militares para reacomodar essas "novas armas" (COHEN, 2010, p. 147). O militar deve estar atento à quinta dimensão da guerra, a cibernética, para a qual a informação é um ativo estratégico central, além de relacioná-la com as demais. Desse modo, investiga-se, a partir de agora, o ciberespaço como um novo domínio que, como tal, apresenta seus próprios objetivos e obstáculos; logo, examina-se a guerra cibernética enquanto "arma estratégica" (KREPINEVICH, 2012).

Inicialmente, destaca-se a importância de seu maior objetivo, qual seja: buscar a superioridade da informação, entendida, nesse caso, com o mesmo desdobramento que os conceitos de superioridade naval ou aérea defendem. Em síntese, suas metas principais são: proteger a capacidade de coletar, processar e disseminar um fluxo ininterrupto de informações, negando ao adversário o mesmo e cumprindo, assim, requisitos da chamada *software warfare* (BELLAMY, 2001). Entretanto, para atingir tal fim, deve-se dominar três áreas da guerra na era da informação, a saber: física, informacional e cognitiva. No domínio físico, os elementos de uma força militar devem estar ligados à realização segura e transparente de conectividade e interoperabilidade. No domínio informacional, pessoas e plataformas devem ser capazes de acessar, compartilhar e, mais importante, proteger os dados a um grau que as forças armadas possam estabelecer e manter uma vantagem de informação sobre o adversário. Finalmente, no domínio cognitivo, os militares devem ser capazes de usar essa informação comum para desenvolver a consciência de seu ambiente e compartilhá-la com outros participantes da rede.

Entretanto, a dominância da informação não garante a paralisia estratégica do inimigo, pois a guerra cibernética tem limitações na capacidade de coagir um oponente, caso não seja corroborada por um poder convencional e atuação do espaço físico onde se desdobra força e energia cinética (GARTZKE, 2013; SHELDON, 2011). Como afirmam Thomas e Hecker (2009), esse instrumento não provoca casualidades suficientes para ser considerada *guerra* e, logo, não consegue ser

25 Principalmente da teoria de bombardeio estratégico (TOR, 2015).

uma arma dissuasória, como atestam, por exemplo, Clarke e Knake (2015). Neste prisma, a guerra cibernética, tal como empreendida hodiernamente, não permite falar em *C² warfare*.

O caso mais próximo disso é o Stuxnet, que incidiu ataques, mediante arma cibernética, contra uma usina nuclear, não um centro de C². Assim, por mais que a guerra cibernética e suas armas se desenvolvam em um território submetido às mesmas leis de manobra, velocidade e unidade de comando que regem os outros domínios, sua capacidade de gerar coerção é praticamente inexistente, se não vir acompanhada por um poder convencional capaz de apoiá-la (GARTZKE, 2013). É a partir dessa consideração que Sheldon (2011) apregoa que a proposta de uma estratégia cibernética é ter a finalidade de criar vantagens e influenciar eventos dentro de seu desenvolvimento operacional e por meio das estruturas tradicionais de poder. Nesse sentido, a guerra cibernética se mostra incapaz de produzir efeitos estratégicos atrelados ao campo nuclear, como a dissuasão ou até mesmo a coerção convencionais.

Para Sheldon (2013), os defensores dessa terceira tendência consideram a possibilidade de, ao menos, duas modalidades de dissuasão a partir do ciberespaço, quais sejam: estratégias punitivas, como a retaliação por meios cibernéticos e/ou respostas militares convencionais; e negação, a exemplo do *air gap*[26]. Conforme Sheldom (2011) e Gartzke (2013), a dissuasão só pode ser garantida com a combinação de forças convencionais e cibernéticas em torno de um objetivo. Sendo assim, mais uma contradição dos entusiastas que hiperdimensionam tal tendência se destaca: a possibilidade de que nações com poder dissuasório baseado em forças convencionais — em alguns casos, nucleares — possam se ver ameaçadas pela assimetria da guerra cibernética. Tal possibilidade não encontra respaldo diante da incapacidade atual de produção de efeitos dissuasórios ou coercitivos através do ciberespaço. O que ocorre é justamente o contrário, ou seja, países com tal característica reforçam, por meio do uso combinado de forças convencionais e cibernéticas, seu *status quo* na estrutura de poder regional ou global.

26 Medida de segurança que envolve isolar fisicamente um computador ou rede de computadores, inclusive desconectando-os da internet.

Conclusões

O uso estratégico-militar do ciberespaço vem provocando alterações na conduta da guerra. Entretanto, a criação de um novo domínio, o cibernético, não ocorre em desconexão com as dimensões materiais, em que os conflitos armados já se processam. Para melhor avaliar as implicações da guerra cibernética para os estudos estratégicos e de segurança internacional, foram extraídas, da literatura revisada, três tendências que apontam limites e possibilidades para o desenvolvimento desse novo domínio e seu emprego como arma combinada ou vetor estratégico.

O debate hodierno sobre guerra cibernética é caudatário da longa controvérsia que envolve a RAM e seus desdobramentos, ligados à adequação da guerra na era da informação. Em essência, os principais desafios que a guerra cibernética apresenta aos estudos estratégicos na perspectiva clausewitziana são: a eliminação da "fricção" na guerra, a superioridade da ofensiva em detrimento da defesa e, por fim, a guerra não trinitária.

Pode-se afirmar que, até o momento, a literatura não apresenta relatos críveis de que ataques cibernéticos tenham produzido danos em larga escala contra estruturas estratégicas ou centros de C². Entretanto, apesar de não se atestar vínculos causais, os acontecimentos aqui analisados — envolvendo, ainda que hipoteticamente, Estônia, EUA, Geórgia, Irã, Israel, Rússia e Ucrânia — permitem apregoar que as atuais guerras cibernéticas estão ligadas a retaliações ou antecedem, sem efeitos cinéticos comprovados, ofensivas terrestres contra Estados. É possível ainda declarar, em favor da guerra cibernética, que, quanto mais um país estiver "plugado" ao ciberespaço, especialmente no que tange a suas estruturas estratégicas, mais vulnerável estará para ataques originados no ciberespaço.

Outra conclusão expressa o entendimento de que o ciberespaço e a guerra cibernética são matérias do campo tático, não estratégico. Como arma estratégica, por um lado, a guerra cibernética é incapaz de produzir coerção, em razão das características do ciberespaço e seus limites na produção de efeitos cinéticos. Ao permitir, na maioria das vezes, o anonimato de seus agressores, inviabiliza assim a dissuasão, seja por negação, seja por punição. Por outro lado, constata-se, ainda que preliminarmente, que a superioridade cibernética, quando combinada com avanços conquistados pelas armas convencionais, por meio da RAM ou da transformação militar, pode ser um meio eficaz de se promover vantagens no campo de batalha do século XXI.

Apesar da oficialização do ciberespaço como domínio de operações pelos EUA e pela OTAN, inclinamo-nos para a tendência da introdução do ciberespaço e de suas armas na acepção de arma combinada. Tal concepção se justifica pelas limitações características da tecnologia cibernética, as quais, quando para fins coercitivos, implicam a necessidade de recorrer a outros domínios para promover desde efeitos cinéticos até mesmo dissuasórios. À luz da teoria clausewitziana, a guerra cibernética merece esse prefixo quando age no meio físico, convertendo-se em recurso para o uso da força.

Finalmente, em virtudes das limitações expostas nesse artigo sobre o impacto revolucionário da guerra cibernética, chama-se atenção para a importância de se pensar, de forma crítica, a incorporação do ciberespaço como novo domínio. Em contrapartida, argumenta-se aqui que tal ceticismo não deve produzir o efeito de negar a realidade da guerra no ambiente cibernético ou de não levá-lo em conta em suas estratégias, especialmente no que toca as potencialidades de emprego como arma combinada.

Referências

ANDREWS, Timothy D. *Revolution and evolution*: understanding dynamism in military affairs. Washington, DC: NDU Press, 1998, p. 4-40. Disponível em: http://www.iwar.org.uk/rma/resources/rma/98-E-27.pdf. Acesso em: 23 abril 2017.

BAE SYSTEMS. *Snake Rootkit Report 2014*. London: BAE Systems, 2014. Disponível em: http://info.baesystemsdetica.com/rs/baesystems/images/snake_whitepaper.pdf. Acesso em: 11 out. 2016.

BELLAMY, Christopher. What is information warfare?. In: MATTHEWS, Ron; TREDDENICK, John (Org.). *Managing the revolution in military affairs*. New York, NY: Palgrave, 2001.

BIDDLE, Stephen. Iraq, Afghanistan, and American military transformation. In: BAYLIS, John; WIRTZ, James J.; GRAY, Colin S. (Org.). *Strategy in the contemporary world*: an introduction to Strategic Studies. 3. ed. Oxford, NY: OUP, 2010.

BIRDWELL, M. Bodine; MILLS, Robert. War fighting in cyberspace: evolving force presentation and command and control. *Air & Space Power Journal*, p. 26-36, Spring 2011.

BOHN, Eduardo C.; NOTHEN, Maurício R. Considerações sobre o ciberespaço e sua inserção nos Estudos Estratégicos. In: GUEDES DE OLIVEIRA, Marcos A.; GAMA NETO, Ricardo B.; VILAR LOPES, Gills (Org.). *Relações Internacionais Cibernéticas (CiberRI)*: oportunidades e desafios para os Estudos Estratégicos e de Segurança Internacional. Recife: Editora da UFPE, 2016. (Defesa & Muros Virtuais, 3).

BRZEZINSKI, Zbigniew K. *EUA x URSS*: o grande desafio. Rio de Janeiro: Editorial Nórdica, 1989.

BUMILLER, E.; SHANKER, Thom. Panetta warns of dire threat of cyberattack on U.S. *The New York Times*, New York, 11 out. 2012. World, p. A1. Disponível em: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html. Acesso em: 22 dez. 2017.

SPUTINIK. *China cria ramo das Forças Armadas sem análogos no mundo*. Sputnik, 18 jan. 2016. Disponível em: http://br.sputniknews.com/mundo/20160118/3325675/China-tropas-unicas-reforma-militar.html. Acesso em: 7 jun. 2016.

CLARKE, Richard A.; KNAKE, Robert K. *Guerra cibernética*: a próxima ameaça à segurança e o que fazer a respeito. Tradução de: Bruno S. Guimarães *et al*. Rio de Janeiro: Brasport, 2015.

CLAUSEWITZ, Carl von. *Da guerra*. Tradução de: Maria Tereza Ramos. 3. ed. São Paulo: Martins Fontes, 2010. (Clássicos Martins Fontes).

COHEN, Eliot. Technology and warfare. In: BAYLIS, John; WIRTZ, James J.; GRAY, Colin S. (Org.). *Strategy in the contemporary world*: an introduction to Strategic Studies. 3. ed. Oxford, NY: OUP, 2010.

CROFT, Adrian; APPS, Peter. NATO websites hit in cyber attack linked to Crimea tension. *Reuters*, Brussels, 16 mar. 2014. Disponível: http://www.reuters.com/article/2014/03/16/us-ukraine-nato-idUSBREA2E0T320140316. Acesso em: 11 out. 2015.

DAVIS, Paul K. *Military Transformation? Which Transformation, and What Lies Ahead*? Santa Monica, CA: RAND Corporation, 2010.

ESTADOS UNIDOS DA AMÉRICA. *US Cyber Command (USCYBERCOM)*. Washington: United States Strategic Command, 2016. Disponível em: http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom. Acesso em: 31 out. 2016.

FORSLING, Carl. Should cyber warfare have its own branch? *Task and purpose*, 28 jun. 2016. [online]. Disponível em: http://taskandpurpose.com/cyber-warfare-branch. Acesso em: 3 ago. 2016.

GAMA NETO, Ricardo B.; VILAR LOPES, Gills. Armas cibernéticas e segurança internacional. In: MEDEIROS FILHO, Oscar *et al*. (Org.). *Segurança e defesa cibernética*: da fronteira física aos muros virtuais. Recife: Editora da UFPE, 2014. (Defesa & Muros Virtuais, 1).

GARTZKE, Erik. The myth of cyberwar: bringing war in cyberspace back down to Earth. *International Security*, v. 38, n. 2, p. 41-73, Fall 2013. Disponível em: https://www.belfercenter.org/sites/default/files/files/publication/IS3802_pp041-073.pdf. Acesso em: 22 dez. 2017.

GEORGE, Alexander L.; BENNETT, Andrew. *Case studies and theory development in Social Sciences*. Cambridge: MIT Press, 2005.

HOUSE, Jonathan M. *Combinação das armas: a guerra do século XX*. Rio de Janeiro: Biblioteca do Exército Editora, 2008.

JONES, Sam. Kremlin alleged to wage cyber warfare on Kiev. *Financial Times*, 5 jun. 2014. Cyber. Disponível: http://www.ft.com/intl/cms/s/0/e504e278-e29d-11e3-a829-00144feabdc0.html. Acesso em: 11 ago. 2016.

KASPERSEN, Anja. Cyberspace: the new frontier in warfare. *World Economic Forum*, 24 set. 2015. Disponível em: https://www.weforum.org/agenda/2015/09/cyberspace-the-new-frontier-in-warfare. Acesso em: 2 ago. 2016.

KREPINEVICH, Andrew F. *Cyber warfare: a "nuclear option"?* Washington, DC: CSABA, 2012.

LANDMAN, Todd. *Issues and methods in Comparative Politics*: an introduction. 3. ed. New York, NY: Routledge, 2008.

LANGNER, Ralph. Stuxnet: dissecting a cyberwarfare weapon. *Focus*, maio-jun. 2011, p. 49-51. Disponível em: http://wp. vcu.edu/hsep/wp-content/uploads/sites/3338/2013/06/stuxnet.pdf. Acesso em: 6 abr. 2017.

LEE, Dave. Rússia e Ucrânia travam 'duelo cibernético'. *BBC Brasil*, 7 mar. 2014. Disponível em: http://www.bbc.co.uk/portuguese/noticias/2014/03/140307_russia_ucrania_bg.shtml. Acesso em: 11 ago. 2016.

LIBICKI, Martin C. Cyberspace is not a warfighting domain. *I/S: a Journal of Law and Policy for the Information Society*, v. 8, n. 2, p. 321-336, 2012.

LILES, Samuel; et a.. Applying traditional military principles to cyber warfare. In: C. CZOSSECK; OTTIS, R.; ZIOLKOWSKI, K. (Ed.) *4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2012.

LOBATO, Luísa Cruz; KENKEL, Kai M. Discourses of cyberspace securitization in Brazil and in the United States. *Revista Brasileira de Política Internacional*, v. 58, n. 2, 2015, p. 23-43. Disponível em: http://www.scielo.br/pdf/rbpi/v58n2/0034-7329-rbpi-58-02-00023.pdf. Acesso em: 22 abr. 2017.

MACISAAC, David. Vozes do azul: teóricos do Poder Aéreo. In: PARET, Peter (Org.). *Construtores da estratégia moderna*: de Maquiavel à era nuclear. Tomo 2. Tradução de Joubert de O. Brízida. Rio de Janeiro: Biblioteca do Exército Editora, 2003.

MEARSHEIMER, John J. *Conventional deterrence*. Cornell: Cornell University Press, 1983.

MINÁRIK, Tomáš. NATO Recognises Cyberspace as a "Domain of Operations" at Warsaw Summit. *NATO CCDCOE*, Tallinn, 21 jul. 2016. Disponível em: https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html. Acesso em: 28 out. 2016.

NYE JR, Joseph S. Cyber insecurity. *Daily News Egypt*, Cambridge, 14 dez. 2008. Disponível em: http://belfercenter.ksg.harvard.edu/publication/18727/cyber_insecurity.html. Acesso em: 1 out. 2016.

OPPERMANN, Daniel. Virtual attacks and the problem of responsibility: the cases of China and Russia. *Carta int.*, São Paulo, v. 5, n. 2, NUPRI-USP, dez. 2010, p. 11-25. Disponível em: http://citrus.uspnet.usp. br/nupri/arquivo.php?id = 21. Acesso em: 30 mar. 2016.

PAPE, Robert. *Bombing to win*: Air Power and coercion in war. Cornell: Cornell University Press, 1996.

PERON, Alcides E. dos R. Guerra virtual e eliminação da fricção? O uso da cibernética em operações de contrainsurgência pelos EUA. In: GUEDES DE OLIVEIRA, Marcos A.; GAMA NETO, Ricardo B.; VILAR LOPES, Gills (Org.). *Relações Internacionais Cibernéticas (CiberRI)*: oportunidades e desafios para os Estudos Estratégicos e de Segurança Internacional. Recife: Editora da UFPE, 2016. (Defesa & muros virtuais, 3).

PORTELA, Lucas S. Agenda de pesquisa sobre o espaço cibernético nas Relações Internacionais. *Revista Brasileira de Estudos de Defesa*, v. 3, n. 1, jan./jun. 2016, p. 91-113. Disponível em: http://seer.ufrgs.br/index.php/rbed/article/view/62071. Acesso em: 20 abr. 2017.

PROENÇA JR, Domício. Promessa tecnológica e vantagem combatente. *Revista Brasileira de Política Internacional*, v. 54, n. 2, 2011, p. 173-188. Disponível em: http://www.scielo.br/pdf/rbpi/v54n2/v54n2a09.pdf. Acesso em: 22 dez. 2017.

PROENÇA JR, Domício; DINIZ, Eugenio; RAZA, Salvador G. *Guia de estudos de estratégia*. Rio de Janeiro: Jorge Zahar Editor, 1999.

SANGER, David E. *Confront and conceal*: Obama's secret wars and surprising use of American power. New York: Crown: 2012.

SHAKARIAN, Paulo. Stuxnet: Cyberwar Revolution in Military Affairs. *Small Wars Journal*, 15 April 2011. Disponível em: < http://smallwarsjournal.com/blog/journal/docs-temp/734-shakarian3.pdf > . Acesso em: 16 ago. 2016.

SHELDON, John B**.** Deciphering cyberpower strategic purpose in peace and war. *Strategic Studies Quarterly,* Summer 2011, p. 95-112. Disponível em: http://www.au.af.mil/au/ssq/2011/summer/sheldon.pdf. Acesso em: 22 dez. 2017.

SHELDON, John B. The rise of cyberpower. In: BAYLIS, John; WIRTZ, James J.; GRAY, Colin S. (Org.). *Strategy in the contemporary world*: an introduction to Strategic Studies. 4. ed. Oxford, NY: Oxford University Press, 2013.

SLOAN, Elinor C. *Modern military strategy*: an introduction. Oxon, NY: Routledge, 2012.

THOMAS, Rid; HECKER, Marc. War 2.0: irregular warfare in the Information Age. Wesport: Praeger, 2009.

TOR, Uri. 'Cumulative deterrence' as a new paradigm for cyber deterrence. *Journal of Strategic Studies*. Vol. 0, Iss. 0, p. 1-26, 18 dez. 2015. Disponível em: http://www.tandfonline.com/doi/abs/10.1080/01402390.2015.1115975?journalCode = fjss20 Acesso em: 22 dez. 2017.

VAN EVERA, Stephen. *Guide to methods for students of Political Science*. Cornell: Cornell University Press,1997.