




JOURNAL OF
GLOBAL STUDIES

ISSN 1518-1219

<http://www.meridiano47.info>

Virgílio Caixeta Arraes

Universidade de Brasília, Departamento
de História, Brasília – DF, Brazil
(arraes@unb.br)

 ORCID ID:
orcid.org/0000-0002-6646-1788

Michel Gomes Nogueira

Universidade de Brasília, Departamento
de História, Brasília – DF, Brazil
(michelnog@hotmail.com)

 ORCID ID:
orcid.org/0000-0001-7041-3220

Copyright:

- This is an open-access article distributed under the terms of a Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided that the original author and source are credited.
- Este é um artigo publicado em acesso aberto e distribuído sob os termos da Licença de Atribuição Creative Commons, que permite uso irrestrito, distribuição e reprodução em qualquer meio, desde que o autor e a fonte originais sejam creditados.



A Guerra Russo-Georgiana (2008): a inovação tecnológica em campo

The Russo-Georgian War (2008): the field technological innovation

DOI: <http://dx.doi.org/10.20889/M47e21001>

Recebido em 5 de dezembro de 2019

Aprovado em 5 de março de 2020

Resumo

O presente artigo trata da guerra entre Rússia e Geórgia em 2008 por causa da disputa sobre Ossétia do Sul e Abecásia, territórios secessionistas e russófilos. O conflito teria sido mais um episódio tradicional no sistema internacional, mas a utilização da cibernética em larga escala pelos russos lhe proporcionaria singularidade. Assim, esta guerra foi um exemplo de danos causados a um país como vítima da cibernética como artefato militar.

Abstract

This article deals with the war between Russia and Georgia in 2008 referring to the confrontation in South Ossetia and Abkhazia, russophiles and secessionists territories. The conflict would be another traditional episode in the international system, but the use of cybernetics in large scale by the Russians gave it singularity. Thus, this war was an example of the damage caused to Georgia as a victim of cybernetics as military weapon.

Palavras chaves: Rússia; Geórgia; Internet; Guerra Cibernética; Cáucaso.

Keywords: Russia; Georgia; Internet; Cyberwar; Caucasus.

Introdução

Ciência e tecnologia e emprego (mesmo hipotético) da força caminham no mínimo de forma paralela nas esferas estatais há várias gerações, a despeito do regime político vigente. Mandatários diligentes costumam estimular inovações e, deste modo, financiar centros de pesquisa, em especial os de aproveitamento militar ou de preservação da integridade física e mental dos quadros principais do país. À proporção que o tempo transcorre, os efeitos das descobertas espriam-se aos poucos para a população (CREVELD, 2004, p. 540-547).

Beneficiam-se de tal posicionamento ao longo de gerações as unidades do Estado castrenses e as concentradas em engenharia e medicina, por exemplo, estruturadas de forma separada das universidades até a virada do século dezoito para o dezenove, haja vista a necessidade de aproveitamento imediato das invenções (WALLERSTEIN, 1996, p. 13-19).

A contínua competição entre grandes potências por territórios, riquezas ou matérias primas desencadeou acelerados processos de modernização nas forças armadas, até o desdobrar na centúria passada de um de seus dois componentes – o Exército – em um novo, a Aeronáutica, com poder de destruição bastante amplo – vide os bombardeios de Hiroshima e Nagasaki em agosto de 1945 pelos Estados Unidos.

Em plena rivalidade da Guerra Fria, o advento da III Revolução Industrial – caracterizada pela microeletrônica – descortinou possibilidades incomuns para a atuação militar dos principais países, entre as quais a do uso de computadores e a de veículos aéreos não tripulados em maneiras distintas nas pelejas. Um dos resultados aos governos é a diminuição do número de feridos ou de mortos dos cidadãos engajados.

O combatente usual, moldado em treinamento intensivo no manejo de armas e no embate físico nos campos de batalha, compartilha nos dias de hoje sua atuação com colegas com especialização em manobrar equipamentos às vezes até milhares de quilômetros do cenário de guerra, se considerada a base da operação. Seu treinamento é diferente dos efetivos tradicionais, por causa de suas trajetórias acadêmicas: da matemática e da física até ramos da engenharia ou da computação.

A guerra, malgrado a existência de regras concertadas em tratados, nem sempre ocorre sob a observância dos padrões morais adequados ou aceitos em determinado período da história pelos membros regulares da sociedade planetária.

Com os incontidos avanços tecnológicos, valem-se governos democráticos ou ditatoriais de armas específicas, as quais necessariamente não eliminam de maneira física seus adversários, porém os desgastam ou desmoralizam perante a opinião pública interna ou mesmo global. É uma forma adicional de enfrentar os adversários.

À guisa de demonstração, sob custo baixo, ‘bombardeiam-se’ de modo anônimo os oponentes nas redes sociais digitais até fatigá-los na arena diplomática ou militar. Nem sequer há a necessidade de desfrutar do trabalho de arregimentados no alvor da idade; no século vinte e um, até ‘robôs’ executam o envio incessante de mensagens com conteúdo fantasioso, distorcido ou fragmentado, de acordo com a classificação tradicional – chamam-nas os veículos de comunicação de *Fake News*.

Outra possibilidade de que dispõem países bem estruturados é a interferência em sistemas civis, privados ou públicos, ou castrenses, por meio de códigos ‘maliciosos’ tais como malwares ou vírus, de sorte que há o acesso a arquivos digitais de terceiros ou a perspectiva de destruir ou adulterar tais bases de dados. Desta sorte, a espionagem, visualizada em filmes populares na fase da bipolaridade, perde aos poucos a importância tática de outrora na disputa de poder.

Portanto, no contexto de temas contemporâneos, não poderia o analista menoscar a importância da tecnologia da informação, amparada esta em lógica binária, a ser resumida do seguinte modo:

existe o registro de descargas elétricas, negativas ou positivas, tratadas como zero ou um. Utiliza-se, pois, a série de números binários para representar entes observados de forma simplificada.

Destarte, a letra A é representada por 01000001. Em sendo ela minúscula, por outro, é 01100001. Dispõe-se esta sequência de números em linguagem de máquina que, por seu turno, é administrada por um código de computador extraído dentre várias linguagens tais quais Basic, C++ e Java, conforme aponta Friedman (2009, p. 82).

Toda potência necessita de preocupar-se com o desenvolvimento material das tropas e do arsenal – aviões, submarinos, drones, equipamentos de comunicação, navios, tanques, mísseis e quejandos dependem cada vez mais da aceleração dos processos de atualização científica. Entre as novas maneiras de atuar, há a ciber guerra ou a guerra cibernética sintetizada. Segundo Teixeira (2017), são “(...) iniciativas empreendidas por um Estado-nação para invadir computadores ou redes de informação com o propósito de causar danos ou distúrbios”.

Ela em si não se encaixa no critério tradicional de conflito interestatal, até pelo alcance do uso por organizações privadas (ilegais) também. Em função disso, amplia-se a gama de possíveis danos a aeroportos, centrais elétricas, portos, escolas, hospitais etc. Nem todo potencial agressor precisa ser ator estatal – terroristas ou mesmo criminosos comuns podem agir.

Os Estados Unidos como primeira potência mundial lidam com esta questão em tal grau “(...) que o Departamento de Defesa criou sua própria divisão de combate cibernético (...) que emprega jovens ligados a essa nova realidade para buscar falhas e formas de minar os sistemas de defesa das potências adversárias” – RUDZIT, *apud* GUEDES, 2012, p. 38.

Ante o exposto, o presente texto aborda a questão da disputa entre Rússia e Geórgia em agosto de 2008 por ascendência política sobre a Ossétia do Sul e a Abecásia, províncias formalmente georgianas, embora integrados no passado ao império russo.

Objetiva-se avaliar o resultado da tática incomum utilizada pelos russos, ou seja, a de empregar um ataque cibernético antes de invadir o território georgiano, ao bloquear os principais canais de comunicação da diminuta nação.

O artigo abarca o relacionamento do Estado, da guerra regular ou irregular e do confronto cibernético, possibilitado pelo avançar da computação e da Internet nas últimas décadas, ao passo que aborda posteriormente o entrevero entre Geórgia e Rússia, avaliado como uma das primeiras representações da cyber guerra.

Estado diante da guerra (ir)regular no alvorecer do século XXI

De acordo com a concepção de Creveld (2004, p. 1 e p. 260), um dos mais importantes estudiosos contemporâneos da teoria da Guerra, Estado, ator de maior representatividade da política global, representa:

uma entidade abstrata que não se pode ver, ouvir nem tocar (...) e após quatro séculos e meio de evolução, que começara por volta de 1300, (ele) talvez seja o mais poderoso construto político de todos os tempos. Contando com forças armadas permanentes – primeiro, os militares, depois a polícia e também o aparato carcerário – impôs ordem à sociedade, chegando ao ponto em que as únicas organizações capazes de enfrenta-lo eram outras do mesmo tipo.

Por seu turno, Duroselle (2000, p. 283) estipula duas condições para o conflito planetário: a primeira se traduz no interesse de considerar um objeto interessante, com a consequente vontade de adquiri-lo. Portanto, ele deverá valer a pena para ser obtido; a outra diz respeito ao fato que essa decisão deverá ser acompanhada “(...) de reação emocional favorável ou desfavorável, pelo menos em uma parte da população que ele controla ou da população do campo adversário”. Na confrontação, entram em jogo, portanto, uma ação e uma reação.

A visão de estratégia de Beaufre (1998, p. 28) difere em certo aspecto da definição clássica de Clausewitz. No entender do teórico francês, ela não trata somente da arte de empregar as forças militares para atingir resultados fixados pela política, porém de “atingir os objetivos fixados pela política, utilizando da melhor maneira os meios de que se dispõe”. Estes podem ser considerados como ofensivos (conquista ou a imposição de condições onerosas), defensivos (proteção do território) ou, por último, mantenedores do *status quo* político.

A despeito da motivação do combate e da forma de participação dos atores – de grupos à sociedade – os conflitos contemporâneos não abrangem apenas desinteligências entre países. Nesse sentido, Lind (2005, p. 12) apresenta um modelo de evolução histórica da confrontação com quatro fases:

A primeira (utilização da massa) é a guerra de linha e coluna (*line-and column*) onde as batalhas eram formais e o campo de enfrentamento, ordenado – ela vigorou entre 1648 e 1860 aproximadamente e estabeleceu uma cultura de ordem em que havia a distinção entre o combatente e o civil, marcada, por seu turno, por rígida hierarquia, uniformes e saudações específicas como as continências;

A segunda (concentração do poder de fogo) desenvolveu-se nas forças armadas da França durante a I Guerra Mundial, com artilharia de conquista e de infantaria de ocupação. Buscava-se a sincronia do poder de fogo, ao valer-se o exército de planos pormenorizados para infantaria, carros de combate e artilharia em batalhas onde seus generais se equivaleriam a maestros;

A terceira (manobra) emergiu na II Guerra Mundial, sendo implementada pelas forças armadas da Alemanha – seria a “*blitzkrieg*” ou a guerra de manobra. Ela se baseava não no poder de fogo e de atrito, mas na velocidade da surpresa do deslocamento. Ao invés de “aproximar e destruir”, a síntese era “passar e causar o colapso”;

A última (conflitos irregulares e assimétricos) caracteriza-se pelo fato de o Estado perder a exclusividade da guerra, de sorte que os contingentes enfrentam oponentes ou milicianos tais como a al-Qaeda, o Hamas, o Hezbollah ou as Forças Armadas Revolucionárias da Colômbia. Em todos os embates, a vitória estatal, quando ocorre, é difícil e custosa.

A dificuldade castrense no Afeganistão e no Iraque decorreu da ausência de Estado, onde não havia governo reconhecido, de maneira que as tropas norte-americanas e aliadas tinham problemas para enfrentar beligerantes não identificados – guerrilheiros ou milicianos sem uniforme oficial, por exemplo, ‘camuflados’ nas populações locais – desprovidos das obrigações com as regras dos tratados internacionais, por não haver a necessidade de subscrição deles por seus líderes ou por suas organizações.

Visacro (2009) enfatiza a existência antiga do fenômeno da guerra irregular, amadurecida havia bom tempo – vide a resistência espanhola durante a ocupação francesa por Napoleão ou a luso-brasileira contra os batavos no seiscentos. Para o autor, ele mesmo militar, terrorismo, guerrilha, insurreição, movimento de resistência, combates não convencionais e conflitos assimétricos são exemplos marcantes.

A distinção entre a guerra regular e a irregular é ser a primeira travada entre forças armadas nacionais, com distinção entre civis e combatentes, ao passo que a segunda ocorre entre exércitos e grupos, com o propósito de chegar ao poder via revolução ou insurreição.

Objetivos clássicos como destruição de tropas inimigas e conquista ou manutenção de territórios se somam à busca de apoio da opinião pública e, por conseguinte, de ajuda a sua atividade revolucionária ou ideológica. Assim, a luta tem por finalidade também um objetivo psicológico e pode-se aproveitar de atividades como atentados e sequestros (COSTA, 2017, parte 5, p. 2).¹

Consoante ainda Visacro, guerra irregular é o conflito conduzido por força que não dispõe de organização militar formal e, sobretudo, de legitimidade jurídica institucional. O século XXI assiste à atuação de grupos ou de milícias em várias partes do globo, em especial no Oriente Médio. A fraqueza do Estado estimula indiretamente o crescimento de tais agremiações. Nem todas são defensoras de uma doutrina apenas, dado que algumas podem interagir com organizações criminosas.

Quanto à cibernética, a Grã-Bretanha, por causa da II Guerra Mundial, desenvolveu o Colossus Mark 1, estimado como o computador digital programável pioneiro. Seu sucessor, Colossus Mark 2, se tornaria o primeiro em série – dez unidades. No entanto, por ser parte de atividade secreta, seu design não seria aproveitado (MORIMOTO, 2011). Por sua vez, os Estados Unidos construíram o ENIAC (Electronic Numerical Integrator Analyzer and Computer) entre 1943 e 1945, com operação iniciada em 1946, ao atender solicitação do Departamento de Guerra, hoje de Defesa (COPELAND, 2006).

Na década de sessenta, adveio a Advanced Research Projects Agency (ARPA) que tinha como alvo o estabelecimento de uma rede que se mantivesse funcional, mesmo sob intensos bombardeios, e interligasse pontos estratégicos para fins militares, ou seja, centros de pesquisa e tecnologia e serviços de informação nacional. A rede (Arpanet) devia abraçar todas as localidades financiadas pela Agência, ao ligar seus computadores com sistemas de tempo compartilhado, com o fito de reduzir custos de

1 No Brasil, guerra irregular é o confronto armado executado por forças não regulares ou por forças regulares empregadas fora dos padrões normais da confrontação regular contra governo estabelecido ou poder de ocupação com o uso de ações típicas de guerrilhas e a assimétrica sendo o conflito armado que contrapõe dois poderes militares que guardam entre si marcantes diferenças de capacidades e possibilidades. Um enfrentamento onde um dos lados é bem superior ao outro e o mais fraco adota majoritariamente técnicas, táticas e procedimentos típicos da guerra irregular (MINISTÉRIO DA DEFESA, 2007, p. 25).

transmissão e, potencialmente, ampliar os objetivos militares nas pesquisas em torno dessa mesma tecnologia (CARVALHO, p. 12, *apud* NOGUEIRA, 2016).

Em 1990, o Departamento de Defesa a desmantelaria, ao substituí-la pela NSFNET, popularizada em todo o planeta como Internet, a qual permitiria a computadores conectarem-se e assim transferirem dados entre si (BASÍLIO, p. 12, *apud* NOGUEIRA, 2016).

Voltada para a preservação territorial e depois para as atividades civis, a Internet se tornaria logo depois ambiente favorável para a ação também de pessoas mal-intencionadas, direcionadas para crimes individuais, ou de atividades coletivas ilegais como terrorismo. Diante disso, grandes potências passaram a dispor de divisões cibernéticas em prol da segurança nacional.

De acordo com Rudzit (*apud* GUEDES, BRASIL *et al*, 2012, p. 38), a Casa Branca reconhece que atividades bélicas dependem cada vez mais da sofisticação do aparato tecnológico: “Organizações terroristas adorariam quebrar toda a rede de eletricidade da costa leste americana. Imagine o caos? E se for a rede bancária?”.

Esta é uma preocupação também do Planalto, até pela dependência de programas, aplicativos e sistemas de computadores provindos de empresas multinacionais. A Estratégia Nacional de Defesa (END), de dezembro de 2008, “estabeleceu prioridade em três setores estratégicos: Nuclear, Cibernético e Espacial”. No contexto, observa-se que a mobilização do Brasil para fomentar a END ocorreu após o conflito entre Rússia e Geórgia.

No ano posterior, a Diretriz nº 14 do Ministério da Defesa instituiu ao Exército a responsabilidade de coordenação e de integração cibernética. Em setembro de 2012, o Decreto nº 7.809 incluiu na estrutura regimental do Comando do Exército o Centro de Defesa Cibernética.

A desproporcional disputa entre russos e georgianos

A dissolução formal soviética ocorreu em 1991, expressa com o encerramento do regime comunista e com a desagregação territorial incomum, por não ter havido guerras de independência – entre os novos países derivados no processo de debilidade figuraria no Cáucaso a Geórgia, berço de Joseph Stalin, o mais longo dos dirigentes do período comunista (1922-1953).

Apesar da vasta fragmentação territorial da União Soviética, a Rússia, sua sucedânea natural, continuaria como o país de maior extensão global e como entidade multinacional (BAPTISTA NETTO, 2011).

Relembre-se que um dos motivos de a União Soviética ter sido derrotada de maneira fragorosa na Guerra Fria havia derivado do hiato técnico dos anos oitenta, quando comparada ela com as nações do arco norte-atlântico – Estados Unidos, Alemanha, França ou Grã-Bretanha – e com o Japão.

Esta diferença de desenvolvimento originou-se da chamada “fuga de cérebros”, concretizada pela saída de milhares de cientistas em busca de melhores condições de vida por causa da degradação do ensino, da corrupção, da burocracia excessiva e da insuficiência de investimento crescente em

pesquisa científica e, por conseguinte, da necessária renovação do parque tecnológico diante dos céleres avanços da microeletrônica, por exemplo (MILHAZES, 2009; HALLIDAY, 1999, p. 214-221).

De acordo com Rodrigues (2006, p. 179), durante a década de setenta, o atraso científico da União Soviética não era significativo na ciência com relação a países europeus, Estados Unidos ou Japão, pois “(...) físicos e matemáticos soviéticos destacavam-se entre os melhores do mundo. Os livros de cálculo integral e diferencial russos, por exemplo, eram referências, sendo utilizados em cursos de ciências exatas em todo o mundo”.

O autor se posiciona (p. 181) de maneira contrária, portanto, à perspectiva de Milhazes: não teria sido a ausência de nível cultural e de qualificação técnica dos cientistas soviéticos, nem a falta de pesquisa e de desenvolvimento. Em seu olhar de mundo, a União Soviética não conseguiu acompanhar a revolução tecnológica nos anos oitenta “(...) pois esta pressupunha um grau mínimo de flexibilidade, democracia e liberdade de informação, exatamente aquilo que o sistema negava aos seus cidadãos. E, neste aspecto, demonstrou-se menos flexível que as democracias capitalistas”.

Com a extinção da disputa americano-soviética, o governo russo se empenhou em reduzir a diferença, a ponto de poder ameaçar em tese o cotidiano até dos Estados Unidos, quando da eleição presidencial de 2016, na qual se saiu triunfante o republicano Donald Trump: caso se confirme a interferência cabal no pleito, seria o coroamento da denominada Doutrina (Valery) Gerasimov, marcada por ações destinadas a confundir os adversários por meio do emprego de ferramentas avançadas como a cibernética – ela é uma referência ao atual titular do Estado-Maior das Forças Armadas da Rússia. (ARRAES, 2017).

A Geórgia, ao ter a sua soberania reconhecida em abril de 1991, teria querela diplomática importante com a Rússia em decorrência do destino de dois pequenos territórios: a Ossétia do Sul, incorporada ao regime czarista no final do século dezoito, e a Abecásia, anexada também no terceiro quartel do dezenove, áreas habitadas havia muito tempo por comunidades de ascendência russa, infensas à separação política com Moscou. Escaramuças constantes ocorreriam entre a recém firmada administração georgiana e as lideranças políticas das duas regiões.

Na anteaurota do século vinte e um, a despeito dos esforços de cessar-fogo, a tensão permaneceu em ambos os lados. Em janeiro de 2004, Mikheil Saakashvili assumiria a presidência da Geórgia e tentaria eliminar os focos de instabilidade através da negociação, não utilização da força;

Assim, ele desejaria unificar o conturbado país e, ao mesmo tempo, assegurar a estabilidade de duas formas, ao aproximar-se da União Europeia (UE), por motivos econômicos, e da Organização do Tratado do Atlântico Norte (OTAN), pela questão castrense, de sorte que pudesse ter auxílio em caso de hipotético choque com a Rússia, comandada sob punho de ferro por Vladimir Putin. Tal aspiração teria derivado da alteração recente de eixo da política externa dos Estados Unidos naquela região.

Em sendo assim, seria possível cogitar que Washington acreditasse que Ancara depois da extinção do regime soviético na década de noventa passasse a ter mais ascendência no Cáucaso e contivesse eventuais pretensões de Moscou de maior influência ou mesmo de recomposição territorial (KARAGIANNIS, 2013, p. 74).

Todavia, Rússia e Turquia se aproximariam ao longo da gestão de Vladimir Putin e da de Recep Erdogan. Naquele momento, a opção plausível ao mandatário George Bush seria a de acenar aos países daquela região o possível alistamento na OTAN – na altura, composta por vinte e seis membros.

Com o passar do tempo, o quadro regional para Tbilisi, ao invés de melhorar o relacionamento diplomático com Moscou, degradou-se bastante: em abril de 2008, o Kremlin aproximar-se-ia mais das duas áreas secessionistas com efeitos deletérios para a administração de Saakashvili.

Excluída de vez a possibilidade de envolvimento multilateral com o propósito do diálogo e, portanto, de distensionar, não restou à Geórgia senão a ingrata opção de ratificar o meio militar, de maneira que em agosto de 2008 ela atacaria a Ossétia do Sul, após acidente com policiais. Consumada a agressão aos ossetos, a Rússia, por solidariedade, responderia no dia seguinte ao gesto bélico: invadiria o território georgiano.

O conflito militar entre a Rússia e a Geórgia abarcaria não só a Ossétia do Sul, mas a Abecásia também. As duas comunidades consideram-se autônomas concernentes a Tbilisi, pela identidade russa, apesar da ausência de reconhecimento da sociedade internacional. (RANDIG, 2008).

De acordo com Ramina (2010, p. 3693), a ofensiva russa na região do Cáucaso poderia ser avaliada por uns como o possível retorno às práticas administrativas da finada União Soviética, ou seja, as da crença na manutenção territorial irrestrita ou mesmo da sua expansão sem amarras, ao valer-se de seu poderio bélico avaliado como desproporcional por países de porte pequeno ou médio lá.

Para Freire e Simão (2014, p. 92), a confrontação com a Geórgia teve como elemento central o fato de a Rússia “(...) se afirmar no espaço pós-soviético perante a ingerência crescente ocidental e acima de tudo perante um conjunto de políticas e ações liderados pelos Estados Unidos em particular”.

Em não havendo contramedida alguma pelo Kremlin, mesmo sob desaprovação da Organização das Nações Unidas (ONU) ou de organismos regionais, isso poderia desgastar a imagem do país de grande potência e incentivar movimentações similares, isto é, governos daquela vasta área da Ásia poderiam aproximar-se de suas contrapartes europeias ou estadunidenses.

A datar da posse de Saakashvili em janeiro de 2004, os laços políticos entre a Geórgia e os Estados Unidos se robusteceram, haja vista a possibilidade de a nação caucasiana figurar nos quadros otanianos de forma permanente e, de modo simultâneo, assegurar o domínio definitivo sobre a Ossétia do Sul e a Abecásia. Diante disso, impulsionar-se-ia o processo de diminuição da influência da Rússia.

O crescente estreitamento diplomático entre os dois governos despertou no Kremlin preocupações geoestratégicas de monta, de maneira que Moscou firmaria oficialmente compromisso com as lideranças dos dois territórios, ao desconsiderar as áreas como parte integrante da Geórgia.

Em agosto de 2008, Moscou investiu sem freios contra Tbilisi como pronta resposta à tentativa de ela reiterar sua soberania sobre a ‘russificada’ Ossétia do Sul. Sem esperar por negociações bilaterais ou por mediações multilaterais, via Nações Unidas, por exemplo, a gestão de Putin autorizou bombardeios maciços ao país ao tempo em que mobilizou cerca de setenta mil efetivos ao norte do Cáucaso, os quais se somariam aos quase dez mil dos contingentes secessionistas. Contra isso, pouco podiam fazer os vinte e cinco mil soldados georgianos.

Com o desencadear da confrontação, mais de mil e cem habitantes, entre os quais quatro centenas de civis, pereceriam. Cerca de duzentas mil pessoas tiveram de deixar às pressas suas residências. (GIELOW, 2018, A18).

A ausência de intervenção por parte dos Estados Unidos decepcionou a Geórgia. No entanto, recorde-se de que a Casa Branca já se deparava com dois conflitos de médio porte na Ásia: Afeganistão e Iraque. Em ambos, a justificativa oficial conjugava em graus distintos o combate ao terrorismo e a implementação da democracia neoliberal – em nenhum deles lograriam êxito os norte-americanos.

Além das confrontações em andamento, não havia convergência na OTAN sobre qual posição tomar acerca da Geórgia e da Rússia. De um lado, Washington, Londres e Ottawa convictos da importância de expandir a composição otomaniana;

De outro, Paris, Berlim, Roma e Madri céticos quanto ao valor disso por causa do desgaste junto a Moscou. Em suma, não havia consenso sobre qual rumo a ser tomado – nem todos viam com entusiasmo a presença do organismo militar em solo afegão, vez que sua atuação deveria circunscrever-se à Europa (NOETZEL, SCHREER, 2008, p. 17-18).

Se na parte física dos enfrentamentos o desfecho não surpreendeu os membros do sistema internacional, na digital, sim, porquanto teria sido a primeira vez em que ‘ataques’ virtuais de monta se anteciparam aos reais, executados pelo exército ou aeronáutica.

Cerca de duas semanas anteriores aos bombardeios aéreos e da circulação de tropas moscovitas em solo georgiano, a infraestrutura do pequeno país teria sido alvo de significativa ofensiva digital, por meio de barragens coordenadas de milhões de pedidos – conhecidos como ataques distribuídos de negação de serviço (ou DDoS, na sigla em inglês) – que terminaram por sobrecarregar vários servidores oficiais. Embora acusada pela Geórgia, a Rússia negaria a autoria do serviço.

Talvez isso tenha sido um ensaio das forças armadas moscovitas. Kornes e Kastenberg (2009, p. 1) registram que no mesmo dia (8 de agosto) da ofensiva russa àquela nação outro acometimento digital ocorreria. Dois dias mais tarde, as investidas de DDoS tornariam inoperante a maioria dos sítios oficiais da Geórgia. “Durante essa fase, os ataques distribuídos de negação de serviço foram particularmente levados a cabo por botnets”

Tais *botnets* (diminutivo de robot em inglês) são uma rede de computadores conectada com a Internet e infectada por um aplicativo (*malware*) que permite ao servidor o ‘comando e controle’, isto é, o envio de comandos a esses *bots*. Utilizam-nas para lançar mensagens eletrônicas de campanhas publicitárias (*spam*), mas podem ser empregadas para ataques de negação de serviço em larga escala. Estima-se que as *botnets* da investida maciça aos sítios da Geórgia seriam afiliadas a organizações ilegais russas (SHAKARIAN, 2011, p. 67).

De acordo com Handler (2012, p. 224), o objetivo principal da campanha cibernética russa foi o de apoiar a invasão física da Geórgia, ao mirar a parte principal da infraestrutura. A escalada dos ciberataques teria sido assaz significativa: cinquenta e quatro sítios oficiais do governo georgiano ficaram inoperantes ou fora do ar.

Os alvos eram os também os meios de comunicação locais, sem necessidade de destruição real ou ocupação por tropas como teria sido feito outrora. Por meio da denominada negação de

acesso, a população e as forças armadas nacionais tinham menos condições de informar-se sobre o andamento da confrontação, de maneira que se atingiria o moral da sociedade e, por conseguinte, dificultar-se-ia a reação.

Ante o exposto, a ofensiva cibernética de fato limitou uma resposta eficiente da Geórgia, incapaz de coordenar o funcionamento dos diversos órgãos civis e militares, em função da dificuldade de comunicação ampla do governo com a comunidade. Ademais, esta investida teria grande impacto psicológico sobre a população, ao gerar pânico e angústia diante do ‘silêncio’ oficial (HANDLER, 2012, p. 224).

Para Mshvidobadze (*apud* GILES 2011, p. 46), Moscou vislumbrou a cibernética como importante ferramenta da guerra de informação, ao articulá-la com outros instrumentos como o sistema de inteligência, de contrainteligência, de *maskirovka* (antigo sistema de camuflagem soviético – KEATING, 1981, p. 4), de desativação do sistema de comunicações, de degradação do auxílio de navegação e, por último, de destruição da capacidade computacional do inimigo.

As táticas empregadas no conflito de agosto de 2008 desencadearam uma variedade de “operações de informação” – em inglês, Information Operations (IO). A Rússia utilizou redes de computadores – em inglês, Computer Network Operations (CNO) – com a finalidade de desativar os sítios oficiais da Geórgia ou os de veículos de comunicação locais. (BARKER, FERMAINT, NEFF, 2013, p. 3).

O mesmo entendimento é apresentado por Giles (p. 51) que identificou como “tropas de informação” (Information Troops) nas forças armadas russas as operações de informação. Panarin (*apud* GILES) chamou de Forças Especiais de Informação (Information Special Forces) que deveriam “(...) preparar operações efetivas sob condições potenciais de crise”, na qual a orientação era a de cobrir todos os aspectos das atividades de informação, incluindo até o supracitado CNO. “O objetivo é certamente criar centros que envolveriam os chamados ataques de “*hackers*” em território inimigo” (p. 51).

O perfil das denominadas ‘Tropas de Informação’ abrange diplomatas, peritos, jornalistas, escritores, publicitários, tradutores, técnicos em comunicação, *web designers* e mesmo *hackers*. Ao mirar o propósito de edificação de uma rede de contramedidas de informação, far-se-ia necessário o desenvolvimento de um centro para determinar a importância dos dados sobre o adversário, inclusive sobre como anulá-lo psicologicamente, como manter um sistema de contrapropaganda e como efetuar com êxito operações de rede com treinamento de *hackers* (BBC MONITORING, *apud* GILES, p. 52).

O envolvimento de CNO na desinteligência contra a Geórgia havia sido refutado de maneira veemente pelo Kremlin, porém o titular da Segurança Nacional da Geórgia, Eka Tkeshelashvili, afirmou em 2009 que “(...) existem diversas evidências que esses ataques foram diretamente organizados pela Rússia” (SHACHTMAN, 2009, 1, *apud* BARKER, FERMAINT, NEFF, 2013, p. 4). Shachtman destaca também os acometimentos digitais à Geórgia três semanas antes do início oficial da disputa russo-georgiana.

De acordo com Hollis (*apud* HADDCIK, 2014, p. 2), unidades de inteligência russa haviam efetuado o reconhecimento de sítios importantes naquela nação e a partir de então infiltraram-se em suas redes civis e militares em busca de dados úteis para direcionar as futuras investidas digitais.

Outrossim, a Rússia teria coordenado grupamentos cibernéticos, com a participação oficiosa até de *hackers*.

Reconhecida sem hesitação a interrupção do funcionamento de vários sítios de escol da Geórgia, não se pode estimar com segurança o grau de envolvimento do governo russo na ofensiva cibernética de 2008, devido à dificuldade de se localizar com exatidão até hoje de quais redes de computadores teriam partido as arremetidas. Por conta de tal situação, Moscou pôde contestar seu envolvimento com o prévio “apagão” inédito da Geórgia antes do começo assinalado da confrontação (BARKER, FERMAINT, NEFF, 2013, p. 5).

A despeito da identificação precisa dos autores das algomgavarias digitais, o fato é que a capacidade de defesa cibernética da administração georgiana ficou severamente limitada e, destarte, a barreira de proteção das redes de computadores não pôde ser eficaz para resguardar sítios e arquivos virtuais do país.

Comprova-se a ineficácia da reação da Geórgia quando se observa que a primeira medida oficial ao grande volume de atividades em sua infraestrutura de Internet foi a de estabelecer de balde mecanismos de filtragem para firmar o bloqueio de todos os endereços IPs (*internet protocol*) russos que acedessem a suas redes.

Hagen (2012, p. 10) menciona que a análise da *U.S. Cyber Consequences Unit* enfatizou que a maioria das incursões veio de servidores de dados da Rússia. Os bloqueios iniciais realizados pela Geórgia foram contornados sem restrições porque *hackers* utilizariam logo a seguir servidores de outros países para continuar a desestabilizar os sítios georgianos.

Sem capacidade de se defender digitalmente na velocidade adequada, a Geórgia contatou logo em seguida a Estônia que havia sido alvo no ano anterior também de ofensivas cibernéticas, porém em vão. A única contramedida eficaz foi a de manter alguns canais de informação abertos ao público por meio da transferência de ativos de rede e de hospedagem de sítios em servidores de nações consideradas mais guarnecidas como os de norte-americanos, poloneses e estonianos.

Desta maneira, o país foi auxiliado por companhias privadas, algumas das quais bem conhecidas pelo público em todo o mundo. O sítio da própria Presidência da Geórgia seria situado em servidores da Google em Mountain View (Califórnia), ao passo que o do Ministério da Defesa em uma empresa de Atlanta (Geórgia). O das Relações Exteriores abrigar-se-ia na Estônia. Ademais, a Polônia autorizaria a hospedagem dos demais sítios oficiais em seus servidores (TIKK et al *apud* HAGEN, 2012, p. 11).

De acordo com Clarke e Knake (*apud* HAGEN, 2012, p. 11), a empresa estadunidense Tulip havia ofertado seus serviços à Geórgia com o propósito de possibilitar o acesso aos sítios de lá, mesmo de modo intervalado. Após a conclusão do conflito, a corporação relatou ter sofrido também ataques cibernéticos em seus próprios terminais.

Não obstante esses esforços todos, os servidores, ainda que guarnecidos no exterior, continuariam a permanecer suscetíveis à exploração pela ‘inundação’, em decorrência do volume de força bruta digital utilizado pelos ofensores (BUMGARNER E BORG *apud* SAKARIAN, 2011, p. 69).

Korns e Kastenber (*apud* HAGEN, 2012, p. 12) registram que se na época daquela guerra existisse legislação internacional relativa à soberania do espaço cibernético o simples fato de se usarem

servidores de dados de outros países poderia ter ampliado a escalada do conflito russo-georgiano porquanto ataques em grande escala aos bens – servidores – de um país concorreriam na prática para estimular um governo a defender suas companhias também.

Essa realocação de ativos cibernéticos poderia ter envolvido os Estados Unidos, a Polônia ou a Estônia na confrontação Moscou-Tbilisi. Derrubar sítios na Internet é muitas vezes considerado crimes de inegável gravidade; todavia, Kornis e Kastenberg salientam que a gradação de tais ilegalidades deveria ser reconsiderada e logo ampliadas, caso elas derivassem de finalidade bélica. Ante o exposto, o emprego desses ativos ocasiona novo precedente em operações militares em larga escala e, por isso, precisaria ser regulado por normas, após debates nas organizações internacionais.

Conclusão

A dissolução da União Soviética em 1991 desaguou em uma dezena e meia de novos países, sendo o herdeiro principal do espólio a Rússia. Os processos de secessão pareceram não incomodar o Kremlin do pós-Guerra Fria, sob a liderança de Boris Yeltsin.

A preocupação naquele momento era a aproximação sem reservas com o Ocidente, haja vista a necessidade de investimentos voltados para a modernização da economia e de legitimidade política depois do fracasso da administração de Mikhail Gorbachev perante seus próprios cidadãos – em vez da transição de um regime autoritário para um democrático, houve o ocaso de vez do comunismo.

A postura do primeiro governo no pós-Guerra Fria não trouxe as melhoras sociais aguardadas de maneira ansiosa pela população. Moscou tornar-se-ia pitoresca ao mundo pela adoção sem travas da democracia neoliberal do ponto de vista oficial: em pouco tempo, poder-se-ia vislumbrar que nem um, nem outro funcionariam a contento. Em cerca de setenta e cinco anos, a Rússia abraçou sem tergiversação dois regimes político-econômicos bastante antagônicos com resultados desfavoráveis em ambos a seu povo.

Na viragem do século vinte para o vinte e um, houve a revivescência nacionalista e autoritária, de sorte que a recuperação, ou melhor, a reconstituição do continental país se situasse em plano prioritário no horizonte da comunidade.

Assim, compreende-se a aspiração da elite russa de recompor territorialmente aos poucos sua nação, de maneira que ela retornasse ao molde similar do período monárquico; enfim, há para muitos o desejo quimérico de restaurar a grandeza da Rússia e, por conseguinte, de recuperar o respeito ou ao menos o temor por que o sistema internacional tinha por ela nos séculos predecessores.

A Guerra Russo-Georgiana em agosto de 2008 encaixa-se na visão de mundo acima descrita – além de ter sido ela mesma o maior sacolejo na Europa desde a desagregação da antiga Iugoslávia nos anos noventa da centúria passada. Comunidades russas, se maioria em determinadas áreas independentes, terão a atenção de Moscou com vistas a preservar sua identidade e caso desejem até a possibilidade de unirem-se à pátria mãe.

Diante disso, o conflito ocorrido há pouco mais de uma dezena de anos ocasionou uma forma distinta de enfrentamento no cenário internacional, ao conjugar batalhas digitais e convencionais de modo quase simultâneo.

O espaço virtual ofertou ao Kremlin a perspectiva de antes mesmo do início dos combates reais de isolar e logo silenciar, mesmo parcialmente, seu adversário, de maneira que semeasse pânico e angústia na população georgiana no dia a dia.

Assim, os habitantes da Geórgia sentiam-se amedrontados em decorrência da dificuldade de se conectarem com o restante do globo e, destarte, de obterem auxílio militar ou apoio diplomático à causa da integridade de sua soberania.

De uma perspectiva psicológica, com o moral descendente do inimigo, a Rússia teria maior facilidade para sobrepujá-los. Talvez isso tenha sido um dos motivos para a curta duração da confrontação.

Desde então, os embates digitais incorporaram-se à atuação rotineira das forças armadas contemporâneas. Seus efetivos já não podem prescindir do seu valor como instrumento tático de guerra, ao reduzir o grau de resistência de contingentes opositores e por que não da própria sociedade antagonica. Ademais, o número de baixas nas suas próprias fileiras reduz-se sobremodo, de forma que a opinião pública se mostra menos infensa a uma política exterior bélica.

A disputa de agosto de 2008 mostrou sem dúvidas isso, ao ocasionar o desnorteio da Geórgia pela Rússia no tocante à impossibilidade de se valer do sistema nacional de informação através da Internet e em decorrência disso de zelar pela segurança do povo durante o desenrolar do confronto.

Não obstante Moscou negar a utilização de ferramentas cibernéticas contra Tbilisi naquela época, analistas acreditam ser improvável tal posicionamento, em face da convergência temporal das investidas digitais e reais contra a nação caucasiana.

Portanto, este conflito no continente asiático representa estágio diferente nas relações internacionais quanto ao emprego da força física e digital ao mesmo tempo e, por extensão, com alcance bem mais amplo. Além disso, o novo instrumento da guerra, embora sem o estrépito das bombas ou tiros, é tão arrasador quanto o método tradicional.

Referências Bibliográficas

- ARRAES, Virgílio. “Rússia: a aplicação incidental da doutrina Gerasimov”. Brasília: *Mundorama*. Ago. 2017. Disponível em: <<http://www.mundorama.net/?p=23880>>. Acesso em: 30 set. 2018.
- BAPTISTA NETTO, Irineo. Paradoxo russo. Curitiba, *Gazeta do Povo*. 17 dez. 2011. Disponível em: <<https://www.gazetadopovo.com.br/mundo/paradoxo-russo-aqzgon438enc8m1berttejo7i/>>. Acesso em: 20 nov. 2018.
- BEAUFRE, A. *Introdução à Estratégia*. Rio de Janeiro: Biblioteca do Exército, 1998.
- BRASIL. MINISTÉRIO DA DEFESA. *Doutrina Militar de Defesa*. MD51-M-04. 2ª ed., 2007. Disponível em: <<https://goo.gl/7tYGXh>>. Acesso em: 27 maio 2018.

- _____. MINISTÉRIO DA DEFESA. *Doutrina Militar de Defesa Cibernética*. MD31-M-07. 1ª ed., 2014. Disponível em: <<https://goo.gl/cHWJDg>>. Acesso em: 3 jun. 2018.
- _____. GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA. *Objetivo do Plano Nacional de Segurança da Informação*. Disponível em: <<http://dsic.planalto.gov.br/psni/objetivo>>. Acesso em: 3 jun. 2018.
- CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. *Estatística de Incidentes Janeiro a Dezembro de 2017*. Disponível em: <<https://www.cert.br/stats/incidentes/>>. Acesso em: 5 jun. 2018.
- CREVELD, Martin van. *Ascensão e declínio do Estado*. São Paulo: Martins Fontes, 2004.
- COPELAND, B. Jack. *The Modern History of Computing*. Stanford Encyclopedia of Philosophy. 2006. Disponível em <<https://plato.stanford.edu/entries/computing-history/>>. Acesso em: 30 maio de 2018.
- COSTA, Cristiano R. A. da. “Evolução da Arte da Guerra – Das Gerações da Guerra Moderna aos Conflitos Assimétricos. Parte 4 e 5 – A Quarta Geração da Guerra Moderna”. *Jornal de Relações Internacionais*, 2017. Disponível em <<https://goo.gl/62ovEB>>. Acesso em: 12 out. 2018.
- DUROSELLE, Jean-Baptiste. *Todo império perecerá*. Brasília: Universidade de Brasília; São Paulo: Imprensa Oficial do Estado, 2000.
- FREIRE, Maria Raquel, SIMÃO, Lúcia. *A Rússia e o Cáucaso do Sul: das relações neocoloniais à realpolitik no “estrangeiro próximo”*. Coimbra: Imprensa da Universidade de Coimbra, 2014.
- FRIEDMAN, George. *Os próximos 100 anos: uma previsão para o século XXI*. Rio de Janeiro: Best Business, 2009.
- GIELOW, Igor. Guerra que fez de Putin vilão também consolidou seu poder – Cinco dias de conflito em 2008 com a Geórgia mudaram equilíbrio geopolítico. *Folha de São Paulo – Mundo A18*, domingo, 12 ago. 2018.
- GILES, Keir. “Information Troops” – a Russian Cyber Command? *Conflict Studies Research Centre*, Oxford, UK. 3rd Internacional Conference on Cyber Conflict, 2011. Disponível em: <<https://goo.gl/fkWBSy>>. Acesso em: 18 maio 2018.
- HANDLER, Stephenie Gosnell. “The new cyber face of battle: developing a legal approach to accommodate emerging trends in warfare.” *Stanford Journal of International Law*, Winter 2012, p. 209. Disponível em: <<https://goo.gl/hYfpBT>>. Acesso em: 18 ago. 2018.
- HAGEN, Andreas. “The Russo-Georgian War (2008): The Role of the Cyber Attacks in the Conflict”. *The Armed Forces Communications and Electronics Association*, 2012. Disponível em: <<https://goo.gl/wnba2U>>. Acesso em: 30 set. 2018.
- HALLIDAY, Fred. *Repensando as relações internacionais*. Porto Alegre: Universidade Federal do Rio Grande do Sul, 1999.
- KARAGIANNIS, Emmanuel. “The 2008 Russian-Georgian war via the lens of offensive realism”. *European Security*. Abingdon, v. 22, 2013.
- KEATING, Kenneth C. *U.S Army Russian Institute – Student research report: Maskirovka – The Soviet System of Camouflage*. Garmisch: Germany, 1981. Disponível em: <<https://goo.gl/Xfc2rE>>. Acesso em: 18 ago. 2018.

- KORNS, Stephen W.; KASTENBERG, Joshua E. *Georgia's cyber left hook*. Strategic Studies Institute, 2009. Disponível em: <<https://goo.gl/SKKpVB>>. Acesso em: 22 ago. 2018.
- LIND, William S. “Compreendendo a guerra de quarta geração”. *Military Review*, v. 85, n. 3, 2005. Disponível em <<https://goo.gl/y16ra9>>. Acesso em: 26 abr. 2018.
- MILHAZES, José. *Dirigentes russos reconhecem crise tecnológica no país*. 2009. Disponível em: <<https://goo.gl/4JqHdm>>. Acesso em: 30 set. 2018.
- MORIMOTO, Carlos E. *O ENIAC – A História da Informática* (Parte 6: Sistemas embarcados e supercomputadores). Hardware.com.br, 2011. Disponível em: <<https://goo.gl/trbamV>>. Acesso em: 30 maio 2018.
- NOETZEL, Timo, SCHREER, Benjamin. Alliance divided. *World Today*. London, v. 64, n. 10, oct. 2008.
- NOGUEIRA, Michel Gomes. *O uso do processo de e-Discovery como forma de aprimoramento da segurança da informação*. Dissertação de Mestrado. Publicação PPGENE.DM – 624/2016. ENE/FT/UnB, 2016. Disponível em: <<https://goo.gl/2Dwrbs>>. Acesso em: 30 abr. 2018.
- RAMINA, Larissa Liz Odreski. “O Princípio da Autodeterminação dos Povos e seus Paradoxos: A Aplicação na Guerra do Cáucaso de 2008”. *Anais do XIX encontro Nacional do CONPEDI*, 2010. Disponível em: <<https://goo.gl/b6mg97>>. Acesso em: 27 jul. 2018.
- RANDIG, Rodrigo Wiese. “Guerra na Ossétia do Sul: a Geórgia como foco de conflito entre a Rússia e o Ocidente”. *Meridiano 47*, v. 9, n. 97, 2008. Disponível em: <<https://goo.gl/8MQc9H>>. Acesso em: 30 jul. 2018.
- RODRIGUES, Robério Paulino. *O colapso da URSS: um estudo das causas*. Tese de Doutorado. Universidade de São Paulo, 2006. Disponível em: <<https://goo.gl/9avGEc>>. Acesso: 30 set. 2018.
- SHAKARIAN, Paulo. “Análise da Campanha Cibernética da Rússia Contra a Geórgia, em 2008”. Kansas: *Military Review*, 2011. Disponível em: <shorturl.at/cGMY2>. Acesso em: 12 out. 2018.
- TEIXEIRA, Ana Paula T. *Breve panorama de uma nova “guerra”: os conflitos cibernéticos*. Café História, 2017. Disponível em: <<https://bit.ly/2LZo0iT>>. Acesso em: 14 out. 2018.
- VISACRO, Alessandro. *Guerra Irregular: terrorismo, guerrilha e movimentos de resistência ao longo da história*. São Paulo: Contexto, 2009.
- WALLERSTEIN, Immanuel, org. *Para abrir as ciências sociais*. São Paulo: Cortez, 1996.