UNIVERSIDADE DE BRASÍLIA

Instituto de Ciência Política e de Relações Internacionais

Pós-graduação *Lato Sensu*

Curso de Especialização em Relações Internacionais

CYBERWAR: NOVAS FRONTEIRAS DA GUERRA

Autor

Luis Henrique Almeida de Oliveira

Orientador

Prof. Dr. José Flávio Sombra Saraiva

Brasília - 2011

LUIS HENRIQUE ALMEIDA DE OLIVEIRA

CYBERWAR: NOVAS FRONTEIRAS DA GUERRA

Monografia apresentada como requisito parcial para a obtenção do título de Especialista em Relações Internacionais pela Universidade de Brasília.

Orientador: Prof. Dr. José Flávio Sombra Saraiva

Brasília

2011

AGRADECIMENTOS

Este trabalho é dedicado

Aos meus pais, Oswaldo e Juvelina, pela curiosidade que demonstram, de maneira inspiradora, pelas coisas do mundo; pelo incentivo permanente enquanto busco o meu lugar no mundo virtual.

Ao Prof. Dr. José Flávio Sombra Saraiva, que com intervenções precisas e uma abordagem objetiva, tornou a elaboração desta monografia um desafio pessoal que me proporcionou grande satisfação. Foi uma honra e uma oportunidade que jamais esquecerei.

A Gadi Evron, pela visão do que um ataque cibernético pode significar para um povo e um país - no caso, a Estônia. Sua palestra me levou a questionamentos que culminaram com o objeto dessa monografia.

A Kathleen, pelo apoio no ordenamento conceitual deste trabalho e no caminho que me levou a explorar o campo de batalha virtual.

A Ricardo, pela indicação de que os robôs já estão entre nós.

A Augusto, pelo mapa da guerra.

A Cyrus Farivar, pelo panorama da internet e da mídia cidadã no Irã.

A toda a equipe do IREL/UnB, pelo apoio, com um agradecimento especial a Odalva, Anderson e Celi.

A Rafaela, pela visão humanista e pelo entendimento de que há mais do que tecnologia na guerra cibernética: é preciso investigar o seu impacto nas pessoas.

EPÍGRAFE

A maquinaria do Estado-nação, inventada e cultivada para garantir a soberania territorial e separar claramente os de dentro dos de fora, foi apanhada despreparada pelo "cabeamento" do planeta. Dia após dia, uma atrocidade terrorista após outra, as instituições de lei e ordem dirigidas pelo Estado aprendem sobre sua própria inépcia em lidar com os novos perigos que gritantemente atacam as categorias e distinções ortodoxas consagradas, aparentemente testadas e confiáveis.

Zygmunt Bauman, "Medo Líquido", p. 163.

RESUMO

O presente trabalho explora como um ataque cibernético pode constituir um ataque à soberania de um país. Para tanto, considera as hipóteses de que o espaço cibernético e as múltiplas redes configuram-se como domínios nos quais também se exerce a soberania do Estado, partindo da premissa de que nesses espaços se coordenam sistemas econômicos, político-administrativos, sociais, entre outros, e que uma perturbação no ambiente virtual pode causar distúrbios no cotidiano dos cidadãos e na capacidade de reposta do Estado. Trabalha-se ainda a hipótese de uma relativa fragilidade do Estado na Era Digital, também em decorrência do avanço das Tecnologias da Informação e Comunicação, que passam a influir em temas como a segurança nacional, a dependência tecnológica, a racionalidade de mercado, a porosidade das fronteiras e a ascensão de atores não-estatais no sistema internacional. A pesquisa foi realizada a partir da consulta à bibliografia especializada abrangendo livros, artigos e blogs. Os resultados indicam que o Estado ainda exerce um papel importante, mas não detém mais as reservas clássicas de poder e legitimidade que o consagraram como ator central no sistema internacional. Territórios físicos ainda importam, mas o espaço cibernético vem se configurando como um domínio fundamental e estratégico para o desenvolvimento das sociedades, para a manutenção da estabilidade e da segurança. A soberania está desafiada e a capacidade de resposta estatal encontra-se limitada por sua perda relativa de poder, pela agilidade da cooperação em rede e pela natureza transnacional dos desafios presentes e futuros.

Palavras-chave: guerra cibernética, soberania, segurança, poder, atores não-estatais.

ABSTRACT

This paper explores how a cyber attack could be an attack on State sovereignty. For this, it considers the hypothesis that cyberspace and multiple virtual networks are domains in which sovereignty can be applied, based on the assumption that, in these spaces, economic, political, administrative, social and other systems coordinate themselves. As a result, disturbances in the virtual realm can disrupt the daily lives of citizens and the response capacity of the State. The study also examines the hypothesis of a relative weakness of the State in the Digital Age, also due to Information and Communication Technologies advancements, impacting on issues such as national security, technological dependence, the rationality of the market, the porosity of borders and the rise of non-state actors in the international system. The research focused on the specialized bibliography covering books, articles and blogs. The results indicate that the State still plays an important role, but has no more reserves of conventional power and legitimacy that have established him as the central actor in the international system. Physical territories still matter, but cyberspace has emerged as a vital and strategic domain for the development of societies, for the maintenance of stability and security. Sovereignty is defied and the State response capacity finds itself limited by relative loss of power, the agility of the cooperation network and the transnational nature of present and future challenges.

Keywords: cyberwar, sovereignty, security, power, non-state actors.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

INTRODUÇÃO

A guerra é uma regularidade no sistema internacional que causa fascínio e horror. Tal fascínio é evidenciado pela existência de leitores e pesquisadores que tornaram o tema objeto recorrente de estudo há séculos. A paz é uma exceção nas dinâmicas históricas, mas quais as razões para se estudar a guerra? Utópicos, realistas e estrategistas militares buscaram compreendê-la para disciplinar as tratativas entre Estados beligerantes. Outros buscaram uma solução definitiva para este flagelo. Houve quem procurasse aprimorar a estratégia e assegurar a derrota total do inimigo. Sun Tzu, Grotius, Clausewitz e Aron são alguns dos estudiosos clássicos que inspiraram antigos e modernos especialistas. Da guerra ritual à guerra pela pátria, da guerra total à Guerra Fria e então à guerra cibernética, a técnica sofreu tremendas evoluções ao tempo em que a estratégia e a fundamentação teórica parecem ainda refletir o que, em essência, pensavam Sun Tzu ou Clausewitz, cada um em sua época. Em um mundo sem fronteiras, marcado pela conexão em rede global e instantânea, ainda é possível identificar os princípios de Westphalia (1648) e a defesa de uma soberania cada vez mais fluidificada pela interdependência e pelo estabelecimento de redes mediadas por Tecnologias da Informação e Comunicação (TICs). Em um cenário no qual algumas pessoas se pretendem cidadãs do mundo, conectadas via blogs e redes sociais, mesmo assim a lealdade à pátria ainda se configura como um argumento para a defesa de interesses tidos como nacionais.

A técnica, o espírito de corporação, a estética da guerra, tudo isso mudou e reflete um pouco a sociedade de consumo e a economia política internacional nos conflitos contemporâneos. Se na indústria já se considera normal haver muitos *recalls* de automóveis porque a produção em série ganhou eficiência com o sacrifício da qualidade, a facilidade com que se mata alguém a distância, com recursos tecnológicos, também aumenta o risco do fogo amigo ou de ataques a alvos errados. Algum dano colateral é inerente à guerra.

Da guerra pela honra à guerra ao terror, do território ao mar, das trincheiras ao ar e então ao espaço, e hoje nos computadores interconectados, a batalha alternou ciclos entre conflitos diretos e indiretos, sangrentos e de dissuasão. Hoje, ser o maior

em poderio bélico já não é garantia de inviolabilidade. A estratégia de flanquear perdeu um pouco sua relevância porque primeiro é preciso encontrar o inimigo. Isso tem se tornado cada vez mais difícil também: disperso na população, muitas vezes o inimigo é o próprio civil. Há autores que trabalham com a ideia de que os civis hoje desempenham também o papel ativo nos conflitos armados, não são mais apenas vítimas.

A complexa combinação de velhos valores e novas tecnologias gera desconforto, desconfiança e desacordo entre atores estatais e não-estatais. Nas reuniões de cúpula da Sociedade da Informação, blogueiros juntam-se a representantes oficiais de governos. Não só a soberania está ameaçada pela fluidez do mundo conectado via internet: o monopólio do uso da força pelo Estado, sua última reserva de poder privativo, passou a ser questionado.

A Rede trafega em si as suas próprias contradições: com a privatização das telecomunicações estatais e a oferta privada de infraestrutura (cabos, fibra ótica, *backbones*, *backhauls*), retira-se do Estado sua capacidade de ter reservas de recursos estratégicos. A tecnologia do satélite, dos servidores de rede, os padrões de interconexão – todos derivam de patentes e são influenciados por interesses privados transnacionais e acordos multilaterais. Tais acordos acabam sendo pautados pelos interesses de países que detêm recursos de poder.

Do mesmo modo, críticas ao sistema internacional, mobilizações globais e os produtos da cultura hacker também trafegam pela Rede, corrompendo o sistema com recursos tecnológicos providos pelo próprio sistema. Esse ambiente contraditório é fruto também da interdependência de uma economia globalizada. Em um mesmo ambiente, pacifistas, revolucionários e vendedores de armas coexistem. As contradições não são novas, mas são dramaticamente amplificadas pela comunicação em rede, com alcance mundial. A crescente interdependência é o preço da conectividade global. Nesse contexto, a informação passa a ser um ativo crucial para os países administrarem sua segurança nacional e coletiva, objeto permanente da atenção das forças armadas, dos regimes e dos espaços de interação regional e global.

O presente trabalho analisa a afirmação do ciberespaço como nova fronteira da guerra. Analisa, sob a perspectiva da soberania, o mundo virtual como espaço

social, político e estratégico, dentro do qual uma perturbação da ordem leva a distúrbios na vida dos cidadãos e na capacidade de coordenação do Estado em resposta às ameaças. Destaca também a relativa fragilidade do Estado diante da multiplicidade de atores não-estatais que representam potenciais novas ameaças ao papel central do Estado na sociedade; vulnerabilidade que decorre também de sua crescente dependência de Tecnologias da Informação e Comunicação sobre as quais não tem como exercer grande influência por não deter sua plena propriedade (e, assim, não há controle total dos recursos tecnológicos que suportam os sistemas estatais). Por fim, o estudo que se segue busca identificar, a partir da bibliografia revisada, os impactos das dinâmicas da guerra cibernética também nas populações.

Esse estudo privilegia a perspectiva dos Estados na abordagem da guerra virtual, muito embora boa parte da literatura corrente a respeito de segurança cibernética esteja também relacionada ao terrorismo, aos *hackers*, à espionagem industrial e a outras ações perpetradas por atores não-estatais. Justifica-se o estudo do conflito a partir de uma perspectiva estatal por ser um tema ainda pouco abordado na academia, e que pode contribuir para o avanço das discussões sobre poder, conflito e segurança com uma abordagem bastante atual, também renovando o debate sobre soberania e os novos paradigmas da guerra.

Para tanto, o capítulo 1 faz uma breve revisão histórica do conceito clássico de guerra e o atualiza segundo conceitos e análises sobre a guerra cibernética e as características desse novo domínio de poder. O capítulo 2 aborda a revisão do papel clássico do Estado e os questionamentos que este papel ordenador, e a própria soberania, passam a sofrer no ambiente virtual. Para tal, o capítulo fala da soberania desafiada e das novas formas de cooperação, aborda também as vulnerabilidades do Estado face ao espaço virtual e a necessidade de novos *policy constructs* para o aprofundamento da análise do estado de guerra virtual. O capítulo 3 avança na revisão dos efeitos da guerra cibernética sobre as populações, buscando identificar quem são os novos soldados das batalhas à distância, a mudança no papel dos civis, agora também vistos como perpetradores de ataques por adesão voluntária, e as formas de engajamento online. Busca-se apurar, ainda, a relação entre o real e o

virtual e como vem se tornando cada vez mais importante a capacidade de distinguir um e outro.

Por fim, registra-se que o presente trabalho apresenta alguns termos originais em inglês, mantidos por serem jargão ou por não terem uma tradução equivalente ou amplamente aceita em português.

1. GUERRA E CIBERGUERRA

1.1 A GUERRA CLÁSSICA EM PERSPECTIVA

MAGNOLI (2006:8) fala da origem da Organização das Nações Unidas, idealizada por Franklin D. Roosevelt, e de um dos seus propósitos maiores, descritos na Carta da ONU - “libertar as gerações futuras do flagelo da guerra”. Citando Roosevelt, destaca que a justificativa do antigo presidente dos Estados Unidos (EUA) ao entrar na II Guerra Mundial era por querer “um fim para o início de todas as guerras”. Para este autor, a guerra, na visão dos EUA, seria uma “aberração monstruosa” (p.9), fruto da imperfeição das instituições políticas estrangeiras. Em contraponto, a visão europeia da guerra seria mais realista: a guerra integraria o “fluxo incessante das relações internacionais” (p.10). Magnoli vê no texto de Sun Tzu o “reconhecimento da guerra como componente intrínseco da política...”. O sistema de Sun Tzu, apud Magnoli, no qual o inimigo era minado politicamente e depois derrotado militarmente, de certa maneira apresenta um paralelo com a adoção de recursos cibernéticos para desestabilizar inimigos com ataques cirúrgicos ou massivos. A estratégia soa familiar.

CLAUSEWITZ (2006), oficial prussiano, escreveu a obra clássica, Da Guerra, publicada em 1832, na qual define a guerra como um ato de violência entre partes que visa compelir o oponente a atender a sua vontade. Este autor afirma que a motivação da guerra pode ter duas origens: a hostilidade instintiva ou as intenções hostis, prevalecendo em sua teoria as intenções hostis. Já em 1832 a informação era uma preocupação para Clausewitz, que caracterizou a dificuldade de se obter informações corretas durante a guerra, uma vez que a maioria seria contraditória, falsa ou de caráter duvidoso, exigindo dos oficiais a capacidade de filtrar isso tudo e buscar determinar uma interpretação que não seguisse a tendência generalizada a acreditar no pior em detrimento do melhor. O autor definiu a guerra como mais do que um ato político, na verdade como um instrumento efetivo de exercício da política e uma continuação da política só que por outros meios.

GROTIUS (2005:71-72) afirma que, para Cícero, a guerra é “um debate que se resolve pela força” e que a definição consagrada pelo uso da palavra foi o *estado de guerra*, no qual dois indivíduos “resolvem suas controvérsias pela força”. O autor discute em sua obra a questão da justiça do uso da força, indicando que se os homens fossem justos o emprego da força não seria necessário (p.47). Em sua obra *O direito da guerra e da paz*, Grotius lista alguns limites de uma guerra justa, conduzida para a obtenção de justiça, segundo princípios de boa-fé e respeitando o direito. Também distingue a guerra pública, realizada por uma autoridade, da guerra privada; e, na guerra pública, separa a guerra solene da não solene, sendo a guerra solene desempenhada por partes investidas “do soberano poder em sua nação” (p.168). Tudo isso diz muito sobre a burocracia do conceito da guerra à época de Grotius.

Nesse sentido, é interessante destacar três pontos abordados por Grotius em sua obra: um em que cita o rei Teodorico: “as leis romanas chamam *violência* o que acontece todas as vezes que seja concedido o que se crê que é devido, sem recorrer ao juiz”(p.160); outro em que cita Agostinho: “a ordem natural estabelecida para conservar a paz dos mortais exige que o poder e a vontade de fazer a guerra residam na pessoa dos príncipes”(p.169); e o terceiro, em que afirma que o poder soberano é aquele cujos atos independem “da disposição de outrem”(p.175).

A guerra, na visão de BULL (2002:211), “é a violência organizada promovida pelas unidades políticas entre si”. Bull destaca o caráter oficial da guerra quando exercida entre unidades políticas, distinguindo-a dos ataques de Estados a indivíduos ou mesmo dos ataques entre indivíduos. Assim, a guerra só se qualificaria como tal se empreendida entre Estados. Esse monopólio “legítimo” da violência é alvo do interesse do Estado na manutenção do *status quo*, e o autor reconhece que existe um rito na sua execução e que nem sempre os objetivos da guerra são racionais, uma vez que

> […] foi conduzida por tribos primitivas como uma forma de ritual, pelos cavaleiros cristãos e os sarracenos segundo o código da cavalaria, pelas nações modernas para testar sua coesão e senso de identidade e, ao longo da história, motivada pelo desejo sanguinário de conquista.(p.212)

A análise feita por BULL (2002:215) soa válida para o cenário corrente: a guerra reflete a "desordem na sociedade internacional", é um "instrumento de política" do Estado que pode ser utilizado para manter equilibrado o poder na sociedade internacional, ou manipular o cenário para a satisfação de objetivos de Estado.

O autor considera existir uma tensão básica entre a tendência dos Estados a promover a guerra para alcançar os seus objetivos e a ameaça à sociedade internacional. Ameaçada, a sociedade internacional passou a reagir buscando impor limites ao direito soberano de guerrear. Daí derivam restrições como o conceito de que a guerra só se faria entre Estados soberanos, o surgimento de regras de conduta nos casos de guerra, o disciplinamento da neutralidade (e, por conseguinte, da disseminação regional dos conflitos) e a limitação das razões que legitimavam o engajamento em um conflito (nos primórdios dos sistemas estatais, alegavam-se causas justas para a guerra e, atualmente, no direito internacional, vigoram limites dispostos primeiro pela Liga das Nações e posteriormente pela Carta das Nações Unidas).

Com a evolução da tecnologia de guerra, porém, e a introdução do armamento nuclear, o poder de persuasão da guerra sofreu uma guinada radical: o antigo instrumento de política exterior tornou-se instrumento de aniquilação em massa, gerando temor na sociedade internacional. Para Bull, ainda assim manteve alguma "utilidade política" (p.217) visto que ou as potências em conflito não dispõem de aparatos nucleares, ou apenas um dos lados detém tal poderio, e o seu uso geraria determinado ônus político e moral para o Estado ofensor. A análise de Hedley Bull conclui que tornou-se mais custoso optar pelo uso da força e as possibilidades de ganhos políticos por meio da guerra foram se reduzindo após a II Guerra Mundial.

No mundo conectado em rede, a racionalidade econômica que considera custos e economias de escala aplicados ao campo de batalha é um assunto bastante atual. Por ora, no entanto, na revisão que faz Bull, ele identifica a economia, a segurança e a ideologia como fatores motivadores para as guerras movidas pelos Estados (p.222). O próprio autor identifica a flexibilidade do conceito de segurança,

que pode ser adaptado também à segurança econômica (ex.: guerra por petróleo) ou à segurança ideológica (ex.: guerra contra o comunismo). Citando Grotius, Bull resgata a motivação de uma guerra justa ("a autodefesa, a recuperação da propriedade e a punição") e atesta que "excetuados os casos de autodefesa", a sociedade internacional evoluiu no sentido de refutar a guerra a título de implementação do direito (p.226).

Por fim, com o estabelecimento de economias globalizadas e a exploração do mercado por companhias transnacionais, o autor acredita na manutenção da soberania do Estado mesmo quando este decide abrir o território para exploração estrangeira. A abertura de mercado, para Bull, decorreria de escolhas estatais que não seriam um sinal de submissão ao poderio transnacional. Para Bull, a operação das companhias ainda depende das decisões estatais. Huntington, apud BULL (2002:305), reforça essa tese afirmando que o aumento da atividade transnacional demanda maior acesso a territórios, e tal acesso é uma das reservas de poder do Estado nacional.

Embora a guerra seja parte integrante da história do sistema de estados, ela não necessariamente é uma decorrência desse sistema, pois, afirma BULL (2002:318-319), há e houve regiões com paz relativa e duradoura por longos períodos. Porém, a guerra é "estatisticamente provável" no longo prazo, pois, "dada a existência de estados que são soberanos, armados e politicamente divididos […] [é] pouco razoável esperar […] uma paz universal e permanente".

WALTZ (2001: 187-188), por sua vez, questiona se a guerra ocorreria porque haveria homens e Estados maus, e lembra que mesmo bons homens e bons Estados eventualmente são obrigados a recorrer ao uso da força. Citando Rousseau, corrobora a ideia de que a ausência de um poder superior aos Estados torna a guerra inevitável uma vez que os conflitos provavelmente serão resolvidos pela força. Na Sociedade da Informação, tal força assume diferentes variações, do *hard power* ao *soft power*, aos quais se agrega agora o *cyber power*.

1.2 CYBERWAR: GUERRA CIBERNÉTICA

1.2.1 O mundo cibernético

O mundo cibernético, na visão de PARKS e DUGGAN (2001:122), são as realidades virtuais que subsistem em uma série de redes e computadores. Os autores diferenciam a guerra virtual da guerra cinética (aquela praticada no mundo real). Dada a natureza diferenciada dos ambientes em que guerras reais e virtuais são travadas, princípios diferentes seriam aplicáveis a cada caso[1].

MANJIKIAN (2010:383-385) argumenta que tanto a teoria neorrealista quanto a teoria neoliberal reconhecem o espaço cibernético como "um novo tipo de território" (p. 383). Na crítica realista, a tecnologia da informação cria a necessidade de o Estado adaptar suas estratégias de emprego da força a essa nova ferramenta. A informação é um bem público a ser protegido, ela pode ser controlada e serve como "uma arma na luta por territórios, por credibilidade e na guerra de ideias"[2]. Essa visão não é a mesma dos liberais utópicos, grupo que não reconhece fronteiras na internet e, assim, não entende que existam territórios a serem defendidos – como afirmou BARLOW (1996:1): "Governos do Mundo Industrial (…) vocês não exercem soberania sobre nós. (…) Nós vamos nos declarar imunes à sua soberania, mesmo que sigamos consentindo que suas normas nos regulem"[3].

Comentando a evolução do espaço cibernético, MANJIKIAN (2010:385) identifica como duas de suas principais funções (1) ser o espaço para o comércio eletrônico e (2) o campo para a batalha virtual, funções que se desenvolveram a partir dos anos 1980. Conclui que, apesar da independência de nacionalidade e de gênero, o ciberespaço tem ideologia econômica, "é capitalista, não é socialista". A visão realista, para Manjikian, refere-se a diferentes estratégias virtuais para alcançar os

1 Ver PARKS e DUGGAN (2001:123) para uma breve comparação entre princípios da guerra real e virtual.

2 Para um quadro comparativo completo, ver MANJIKIAN (2010:387), disponível em: http://www3.interscience.wiley.com/cgi-bin/fulltext/123499963/PDFSTART (acesse restrito)

3 Para complementar essa ideia, ler a Declaração de Independência do Ciberespaço, por John P. Barlow, disponível em: http://editions-hache.com/essais/pdf/barlow1.pdf Acesso em: 28 janeiro 2011.

mesmos objetivos do mundo real: atores estatais e não-estatais estariam buscando, no fim, o poder, a defesa contra os inimigos, a expansão territorial o atendimento de interesses nacionais. Assim, trata-se de uma mesma batalha só que travada com armas diferentes.

Uma visão comum em relação à adoção de TICs é o seu poder multiplicador de forças. A ideia de desmobilizar o inimigo sem recorrer à destruição física em massa é atraente para muitos atores. MANJIKIAN (2010:386) corrobora essa análise:

> Na visão realista, o ciberespaço oferece vantagens sem igual para o ator estatal – incluindo a possibilidade de servir como um elemento multiplicador da força, por permitir que um oponente menor derrote um oponente maior, às vezes apenas por meio da intimidação.

No processo de securitização do ciberespaço, a visão realista passou a considerá-lo como um espaço perigoso em razão do baixo custo das transações online (considerando o baixo investimento em equipamentos e banda larga, por exemplo, para efetuar um ataque), da dinâmica das conexões em rede, da possibilidade de anonimato. O próprio espaço cibernético passou a ser referido como campo de batalha virtual, um "santuário para os inimigos" (p. 387), "um local para a globalização da ameaça" (p.391). Nesse sentido, MANJIKIAN (2010:394) cita a visão de Arquilla e Ronfeldt: o ciberespaço oferece vantagens para aquelas pessoas engajadas nos "meios irregulares de conflito", incluindo crimes e terrorismo.

Com a evolução do ambiente eletrônico, a visão liberal foi atualizada e passou a considerar duas perspectivas do ciberespaço: uma que trata a internet como espaço público, outra que o considera o espaço das trocas econômicas e comerciais. Isso levou a um impulso regulatório em resposta a novas premissas assumidas pelos liberais: de que a internet seria essencialmente composta por espaço privado, não público; de que a questão do veto ao acesso a determinados conteúdos, com base em regulamentos locais, indicaria que a internet tem, sim, fronteiras; de que o espaço cibernético não é um mundo que se constrói em separado, tendo em vista que os problemas do mundo virtual já geram efeitos no mundo real.

A questão do impacto no mundo real fez com que as cortes de justiça passassem a considerar o ambiente virtual como espaço para o exercício de controles

de comportamentos e também do discurso (citando Stein, p. 388). Por fim, Lachow e Richardson apud MANJIKIAN (2010:390), reconhecem que embora o mundo cibernético não tenha fronteiras, os agentes da lei têm e estão limitados por suas jurisdições.

1.2.2 *Cyber power*

NYE (2010:3) avalia que o espaço cibernético não suplantará o espaço geográfico ou a soberania estatal. Contudo, a difusão de poder sofrerá modificações, tornando mais complexo o exercício do poder. Na avaliação desse autor, o papel clássico do Estado como provedor de segurança pode ser reforçado em um cenário de crescente insegurança, porém, isso não deve ocorrer segundo o paradigma Westphaliano. Ele considera que a busca por mais segurança na rede levará à delegação de poder e autoridade a atores não-estatais (p. 15), e cita como exemplo os sistemas bancários, que desenvolveram recursos de segurança próprios prevendo, inclusive, sanções aos usuários que apresentam comportamento incompatível com as normas.

Qual a natureza do poder no espaço cibernético? O espaço cibernético constitui um novo e importante domínio do poder. Esse domínio é definido como o espaço em que se usam a computação e a eletrônica para "explorar informações por meio de sistemas interconectados e suas infraestruturas associadas" (p.3). O poderio cibernético (*cyber power)* seria a "habilidade de usar o espaço cibernético para gerar vantagens e influenciar eventos em outros ambientes operacionais" (p.4), perpassando os vários instrumentos de poder.

Para MANJIKIAN (2010:382), o termo *cyber power* ainda não dispõe de uma teoria ou definição amplamente aceita e capaz de explicar sua relação com formas tradicionais de poder e com o sistema internacional. Para ROTHKOPF (1998:326), o poder é "um dos principais vetores de instabilidade no mundo atual" pelo fato de estar em constante reformulação e redefinição.

NYE (2009:298) complementa o quadro com o "paradoxo da abundância", segundo o qual em meio a uma avalanche de informações, o recurso escasso é a

atenção, a capacidade de filtrar o excesso e compreender o que é importante. Para o autor, "[...] aqueles que conseguem distinguir as informações valiosas da confusão de fundo ganham poder". E a luta política passa a incluir também a busca do Estado pelo reconhecimento de sua credibilidade. Para o autor, a credibilidade "é o recurso decisivo e uma importante fonte de poder brando". Por fim, o autor adverte (p.301), vivemos apenas a fase inicial da revolução da informação, momento em que "quaisquer conclusões devem ser aproximadas". Essa advertência se aplica não só ao conceito de *cyber power* mas a todo o conhecimento implicado no presente trabalho. Nesse ponto da história, qualquer análise é limitada pelas possibilidades que conhecemos, e não dispomos de ferramental adequado para a plena compreensão das anomalias vigentes.

1.2.3 Princípios da guerra cibernética

Os princípios da guerra cibernética conforme PARKS e DUGGAN (2001:123-125) seriam os seguintes:

- A guerra cibernética tem efeitos no mundo real;
- Tudo o que é feito no mundo virtual é rastreável;
- Não há leis imutáveis de comportamento do mundo virtual exceto por aqueles casos que dependem de uma ação no mundo físico para sofrerem alterações;
- Alguém no mundo virtual tem a autoridade, acesso ou habilidade para executar ações de que um inimigo depende para atingir seus objetivos. Assim, os inimigos estariam sempre em busca de identidades para assumir para que possam executar essas ações[4];
- As ferramentas de guerra cibernética têm uso dual: podem servir tanto para o ataque quanto para a defesa;

4 Para DUTRA (2007:3), "a primeira regra na identificação de vulnerabilidades é que qualquer sistema computadorizado que possa aceitar a entrada de dados pode ser atacado".

- Cada oponente domina uma pequena parcela do espaço cibernético. Quem conseguir controlar a parte do espaço virtual que o inimigo ocupa poderá controlar o oponente;
- O espaço cibernético é inconsistente e não-confiável: nem sempre *hardware* e *software* responderão da maneira esperada pelo agente.
- Os limites físicos como distância e espaço não se aplicam ao mundo cibernético.

Mesmo sem a pretensão de criar uma lista exaustiva, os autores identificam sinergias possíveis entre princípios da guerra real e virtual e outros pontos que não são aplicáveis ao mundo cibernético. Essa discussão é importante na medida em que o mundo virtual apresenta uma natureza caótica e simples analogias nem sempre são suficientes para a apreensão mais adequada do significado das interações virtuais. Pelo contrário, as analogias às vezes confundem a análise ou limitam seus resultados. É possível avaliar que o crime virtual não perde sua característica fundamental que é a de ser um crime. Porém, o *enforcement* da legislação que coíbe o crime fica dificultado pela natureza virtual e transnacional da infração. Sendo assim, a simples discussão retórica da natureza do feito, se é ou não um crime, não é suficiente para oferecer respostas efetivas para o problema. O mesmo tende a ocorrer de maneira generalizada com as questões legais associadas ao mundo virtual e com o debate ainda inconcluso: leis convencionais são aplicáveis às guerras da informação?

1.2.4 Características do combate físico X virtual

Para NYE (2010:4), dominar o mar ou o espaço aéreo não é uma investida viável para atores não-estatais. Além disso, demanda vultosos investimentos em equipamentos e sistemas. No mundo virtual, por sua vez, tais barreiras seriam tão pequenas que atores não-estatais e pequenos Estados poderiam desempenhar papéis significativos com baixos custos. Para esse autor, há diferenças entre o conflito físico e virtual (ver Quadro I).

QUADRO I – Características do combate físico e virtual

Características do combate	
Mundo Físico	Mundo Virtual
Quase-monopólio do uso da força pelo Estado.	Diversidade de atores e possibilidade de anonimato.
A movimentação dos recursos para o combate (ex.: tropas) é cara.	O ataque é quase sem custos e tem vantagens em relação à defesa.
O defensor conhece intimamente o seu território.	A distância física não importa.
Conflitos terminam por desgaste ou exaustão.	O mais forte não pode desarmar ou destruir o inimigo.
Atores têm identidade conhecida e a dissuasão é uma opção estratégica.	A possibilidade de dissuasão é limitada pelo desconhecimento da real identidade do inimigo e da origem do ataque. Assim, a dissuasão entre Estados é mais complicada, mas não é impossível.
Prover segurança é uma função clássica do Estado.	A crescente insegurança pode levar os Estados a tentarem exercer sua soberania no ciberespaço. A soberania não necessariamente seguirá a tradição Westphaliana e alguma autoridade e responsabilidades poderão ser compartilhadas com atores não-estatais e privados.
O grupo de países que pode exercer o *hard power* e o *soft power* é restrito[5].	Atores de menor porte têm a capacidade de exercer *hard* e *soft power* com menores barreiras à entrada e possibilidade de anonimato.

Fonte: Elaboração do autor a partir de NYE (2010).

1.2.5 Guerras da informação

5 Para Joseph Nye, o hard power seria o poder da coerção (força militar, sanções econômicas) e o soft power seria o poder da atração (a disseminação e a valorização de uma cultura, por exemplo, atraindo aliados ou seguidores sem o uso da força de maneira coerciva). Uma definição concisa dos conceitos de hard power e soft power, conforme Nye, encontra-se aqui: http://www.spiegel.de/international/world/0,1518,643189,00.html Acesso em: 23 março 2011.

Na visão de Trevorrow et al. (em HALPIN et al., 2006:3), os termos *cyberwar, information warfare, netwar e revolution in military affairs* vêm sendo empregados por estrategistas militares há mais de uma década, em um debate que, inicialmente, era muito focado na ação de *hackers freelancers* e nas futuras possibilidades da adoção de TICs nas guerras. Porém, essa abordagem vem evoluindo por diversos fatores: a importância de comandar o espectro da informação, tão crucial hoje quanto foi o domínio de territórios e do espaço aéreo no passado (citação atribuída ao Comandante da Força Aérea dos EUA, em HALPIN et al. 2006:4); a ideologia do armamento não-letal, que também tem seu papel na evolução da guerra cibernética: "por que não tomar as cidades intactas ao invés de pulverizá-las", apenas para ter que financiar projetos de reconstrução caros? (p.4). Essa ideologia levou à ideia de *softkill*, e embora o uso de força letal ainda seja uma alternativa a considerar, trabalha-se de maneira persuasiva o argumento dos custos (não só humanos). A influência da economia política é bastante marcante no moderno discurso dos estrategistas, inclusive pela adoção do vocabulário típico dos analistas econômicos.

Chapman, Latella e Schaerf, no prefácio da obra de HALPIN et al. (2006:xi) reproduzem o conceito de *information warfare*, na definição do Departamento de Defesa norteamericano: ações desempenhadas por um ator para assumir a superioridade em termos de informações, interferindo nos processos, sistemas e redes de computadores dos adversários ao mesmo tempo em que protege suas próprias informações. Para estes autores, as ameaças da guerra cibernética ainda não podem ser adequadamente avaliadas e compreendidas. SIROLI (2006:33), por sua vez, define *information warfare* como as ações que visam corromper ou destruir as informações do adversário com estratégias ofensivas e defensivas. Para esse autor, os EUA são muito avançados em termos de tecnologia da informação e esse status confere ao país alto grau de dependência em relação a estruturas de comunicação. Por conseguinte, os EUA padeceriam de uma maior vulnerabilidade a ataques cibernéticos. Assim como os norteamericanos, vários países têm buscado alternativas para mitigar tais vulnerabilidades. A própria ONU já publicou uma resolução a

respeito[6]. Siroli também analisa as infraestruturas críticas, conceito que abrange o conjunto de sistemas interdependentes que integram cadeias provedoras de produtos e serviços em vários níveis, sendo que as cinco principais infraestruturas críticas (considerando a maior abrangência) seriam: informação e comunicação; energia; finanças; logística e serviços vitais – como serviços de emergência e serviços governamentais (SIROLI, 2006:35). Os dois primeiros, informação / comunicação e energia, sustentam os demais domínios críticos. Sendo assim, corromper essas infraestruturas pode causar impactos importantes na sociedade.

Na análise de riscos desses cinco domínios abrangentes, Siroli considera que megacentros de operações constituem alvos prováveis por concentrarem o fluxo de dados. No campo energético, os Sistemas de Supervisão e Aquisição de Dados são um ponto vulnerável. Comunicações e energia constituem, assim, vulnerabilidades para outros domínios: o sistema financeiro é considerado por Siroli relativamente seguro, porém, sofre os impactos de um ataque cibernético por depender de eletricidade e das comunicações. Na cadeia logística, a ameaça reside nos sistemas inteligentes (cada vez mais difundidos para aumento de performance dos transportes). No domínio dos sistemas vitais, as ameaças residiriam na sobrecarga de serviços de emergência e na invasão dos bancos de dados governamentais, com graves prejuízos para a privacidade do cidadão.

WU (2006:175) define as guerras da informação segundo conceitos presentes na visão dos EUA sobre o tema:

- A informação facilita o processo decisório em tempos de paz e de guerra;
- Guerras da informação visam a afetar o processo decisório do inimigo, levando a decisões erradas, atrasadas ou mesmo a nenhuma decisão;
- O objetivo final da guerra da informação seria alcançar a superioridade informacional frente ao oponente;

6 Resolução 53/70 de Dezembro 1998, que trata de segurança de informações, de sistemas de telecomunicações e de potenciais ameaças às estruturas de informação.

- A capacidade operacional em uma guerra da informação diz respeito à capacidade de reunir dados, processá-los, distribuí-los amplamente, enquanto se anulam essas mesmas capacidades do inimigo.

Em termos táticos, Wu considera que a guerra da informação pode envolver ataques eletromagnéticos, ataques a redes de computadores, manipulação de informações capazes de desorientar o inimigo, ações psicológicas que levam a erros de avaliação e a proteção ou quebra de códigos encriptados.

Um dos prováveis alvos de ataques cibernéticos é a infraestrutura de informações de um país, que na definição de SIROLI (2006:32), corresponde aos sistemas de informação e redes de telecomunicações e tecnologias associadas. Tais estruturas vêm recebendo mais atenção nas políticas nacionais de segurança. O caráter dual de recursos associados às TICs, como ferramentas ou armamentos, é abordado a seguir.

1.2.6 Ferramentas ou armamentos?

SIROLI (2006:41) exemplifica alguns tipos de ferramentas que podem ser empregados em ataques virtuais e ajudam a compreender a natureza de um ataque desse tipo. Há, por exemplo, programas chamados *scanners* para mapear a topologia de redes, ou *sniffers* para monitorar pacotes de dados. *Cracker programs* podem "quebrar" as senhas de acesso a sistemas. Existem também cavalos-de-tróia (ou *trojan horses*, códigos maliciosos que podem vir camuflados em aplicações inofensivas como uma foto ou um slide) e *worms* (código malicioso que se replica e inunda a rede causando sobrecarga). Há muito mais, tanto em variedade quanto em sofisticação, o que leva Siroli a requerer uma espécie de abordagem zoológica para a classificação das espécies de ferramentas.

O comportamento padrão dessas ferramentas empregadas em ataques envolve o mapeamento prévio, a disseminação e a ativação. Tal ativação não precisa ser imediatamente após a disseminação, pode ser posterior. A exemplo de células

terroristas, o software invasor pode permanecer em latência por muito tempo até que seja útil e necessária sua ativação.

ZUCKERMAN et al. (2010:3) avaliam que ataques do tipo DDoS (*Distributed Denial of Service*) podem impactar a liberdade de expressão na internet. A análise desses autores enfatiza a ocorrência de ataques DDoS contra a mídia independente e os ativistas de direitos humanos, tradicionalmente críticos do status quo. Os autores acreditam que esse tipo de ataque tende a aumentar. Um exemplo recente são os ataques ao site Wikileaks quando da revelação das comunicações diplomáticas no final de 2010. Sendo assim, um ataque DDoS pode ser eficaz para favorecer poderosos grupos de mídia e calar as vozes dissonantes.

Os sites, porém, não estão sujeitos apenas a ataques DDoS. PARSA (2010?) relata que no Irã a velocidade de acesso a um site pode ser reduzida, os sites que publicam notas contra o governo podem sofrer *filtering* (que impede o acesso ao seu conteúdo), e os autores podem estar sujeitos à perseguição ou prisão pelo governo. O autor ressalta, ainda, o importante papel das redes sociais no engajamento da sociedade civil e na mobilização da juventude. E comenta as suspeitas de que o governo estaria pagando caro para que blogueiros escrevam *posts* favoráveis ao sistema[7]**.** Esse movimento envolveria as forças Basij, milícia pró-governo ligada à Guarda Revolucionária, na definição do *The New York Times*[8]. ASHRAF (2011) complementa esse quadro refletindo sobre como a internet pode ser vista de maneiras tão diferentes no mundo:

> Será que existiria o conceito de "internet livre" se a única internet que conhecêssemos fosse a internet censurada? Para o usuário médio da internet censurada no Irã, [é comum] ouvir notícias sobre pessoas sendo presas por usarem o Facebook, e-mails sendo hackeados, milhões de websites bloqueados, ou sobre como o Facebook é um ninho de espiões, e agora os milhares de cyberpoliciais se espalhando pelo país. Tudo isso pode tornar uma internet assustadora ainda mais intimidante.

7 Como relatado no site Azadcyber, disponível em: https://www.azadcyber.info/articles/1342 Acesso em: 25 janeiro 2011.

8 Como consta do Times Topics, disponível em: http://topics.nytimes.com/topics/reference/timestopics/organizations/b/basij_militia/index.html Acesso em 25 janeiro 2011.

Fazendo uma analogia com os ataques DDoS, de natureza técnica, ASHRAF (2011) avalia que a "negação do serviço" pode ser também burocrática[9] ou psicológica. O atual cenário do acesso à informação online no Irã exemplifica os dois casos: um site com conteúdo sensível (contra o governo) precisaria ser hospedado em servidores estrangeiros, o que é dificultado pelas sanções aplicadas pelos EUA ao Irã em relação ao comércio (entrave burocrático). Do mesmo modo, ao anunciar os passos para o estabelecimento de uma polícia cibernética, o governo do Irã cria um clima de terrorismo psicológico capaz de influenciar as decisões de milhares de iranianos em relação ao uso dos recursos disponíveis na internet local.

As ferramentas citadas, os ataques DDoS entre elas, não são exclusividade do Estado. Há mais atores atuando nesse tabuleiro, muitos deles não-estatais. Eles são brevemente abordados na próxima seção.

1.2.7 Os atores

SIROLI (2006:42) reconhece que *hackers* podem envolver-se em ataques virtuais por um desafio pessoal. Grupos de *insiders* buscando recompensas financeiras ou vingança também podem ser agentes ativos de ataques cibernéticos. O autor ainda cita criminosos, agindo sozinhos ou como parte de uma organização, engajados em atividades que podem envolver, por exemplo a espionagem industrial. Por fim, Siroli cita atores estatais e não-estatais, engajados em atividades de coleta de dados, propaganda, vigilância, censura e sabotagem, grupos que podem abranger agentes de inteligência ou grupos terroristas. Apesar da variedade de atores, Siroli avalia que *players* relevantes no jogo virtual precisam, além da competência técnica e da capacidade de produzir inteligência, "de uma grande disponibilidade de recursos"[10]. Essa visão ajuda a analisar com mais profundidade um lugar comum nos comentários sobre o mundo cibernético e seu poder catalisador: apesar do baixo grau

9 Conforme a análise de Ethan Zuckerman no Yahoo!, Moniker: why is Mowjcamp.com still offline 6 weeks after hack attack? Disponível em: http://www.ethanzuckerman.com/blog/2010/02/01/yahoo-moniker-why-is-mowjcamp-com-still-offline-6-weeks-after-hack-attack/ Acesso em: 26 janeiro 2011.

10 Embora não fique claro no texto, o conceito de recursos deve abranger os financeiros, logísticos, patrimoniais.

de barreiras à entrada, danos significativos tendem a ser produzidos por ataques engendrados por aqueles atores que têm acesso a mais recursos (físicos e virtuais).

ROTHKOPF (1998:326), por sua vez, identifica um mundo povoado de novos atores que são capazes de exercer influência e causar danos aos interesses alheios. A revolução da informação fornece a esses atores as ferramentas analíticas que lhes permitem competir em pé de igualdade com os competidores maiores, mudar o ânimo dos mercados, transacionar em tempo real como os grandes *traders* fazem (p. 336).

BAUMAN (2008:128) avalia que todos estão em perigo e são também perigosos, contexto em que "há apenas três papéis a desempenhar – perpetradores, vítimas e 'baixas colaterais'". Citando "uma avaliação confidencial do governo britânico", relata a identificação de dois perfis de atores envolvidos em atos terroristas entre os jovens britânicos muçulmanos: entre planejadores e perpetradores haveria jovens graduados, com qualificações técnicas e jovens com pouca ou nenhuma qualificação e, muitas vezes, com ficha criminal. Para Bauman, essa é a deixa para afirmar que as raízes sociopolíticas do terrorismo não serão combatidas de maneira eficiente com os limites impostos às fronteiras, os controles biométricos e a violência dos soldados. As fronteiras já são fluidas porque o mercado necessita que assim o sejam. O terrorismo também derivaria, assim, de uma questão social que demanda a implementação de medidas práticas como o perdão das dívidas e o acesso à educação para o seu enfrentamento.

ALMEIDA (2011:4), analisando as revoltas no mundo árabe desencadeadas em 2011[11], afirma que "todos se esforçam para entender o novo modelo revolucionário que mobiliza uma massa heterogênea em cultura e classe – sem lideranças definidas – em busca de mudanças". O autor avalia que esse movimento representa um "poder anônimo, sem líderes carismáticos". Se uma das contradições modernas é a ascensão dos supraindivíduos como novos atores no tabuleiro internacional, muitas vezes com recursos de poder (econômico, cultural, carismático) para demandar fortemente os Estados nacionais, a figura desse poder anônimo é mais

11 A título de exemplo, ver a cobertura dos Protestos no Egito em 2011 do site Global Voices disponível em: http://pt.globalvoicesonline.org/cobertura-especial/protestos-no-egito-em-2011/

um elemento para aumentar a complexidade do quadro de atores envolvidos nas questões de guerra cibernética e da soberania. A introdução das TICs na equação no mínimo potencializa o efeito desse movimento. Almeida avalia que "[...] a força das redes sociais mostra uma enorme capacidade de mobilização, sem distinção de classe ou cultura [...]" na dinâmica em curso no mundo árabe (p.6). O poder das redes permite que vários atores com diferentes propósitos conjuguem suas forças em nome de objetivos momentaneamente comuns. A tecnologia torna possível que "a multidão anônima, apesar das diferenças individuais, encontre pontos em comum para lutar" (p.6).

Para NYE (2010:9), o salto de poder viabilizado pelas TICs não equivale a dizer que todos os atores, na Sociedade da Informação, agora estão em pé de igualdade em termos de níveis de poder[12]. Os grandes governos ainda podem lançar mão de mais recursos. Buscando uma aproximação bem geral, Nye identifica três macrocategorias de atores no mundo cibernético:

- governos;
- "organizações com redes altamente estruturadas";
- indivíduos e redes com baixo grau de organização.

O autor alerta que há inúmeras subcategorias para cada divisão. A categorização desses atores é extensa e não se justifica fazer um detalhamento de suas características, para não derivar muito dos objetivos deste trabalho. Contudo, considerando o estudo formulado por NYE (2010:10), é útil ter em mente um quadro geral dos atores no ambiente virtual (ver Quadro II):

12 Nye afirma que na internet, nem todos são iguais ("*on the internet, all dogs are not equal*").

QUADRO II – Visão geral dos atores no ambiente virtual

Atores	Poder relativo	Vulnerabilidades
Governos	Regulação, coerção legal e física, oferta de bens públicos, burocracia estruturada, capacidade e orçamento para ataques cibernéticos, agências de inteligência.	Ataques à reputação, instabilidade política, dependência de sistemas complexos que podem ser atacados facilmente.
Organizações com redes altamente estruturadas	Grandes orçamentos e economias de escala, flexibilidade transnacional, controle de códigos e do processo de desenvolvimento de produtos, marcas estabelecidas e reputação.	Perda de reputação, roubo de propriedade intelectual, ataques a sistemas, vulnerabilidades legais.
Indivíduos e redes com baixo grau de organização	Enfrentam poucas barreiras para entrada no mundo cibernético, facilidades para a saída do sistema dado o anonimato, vantagens pela assimetria se comparados aos governos e grandes organizações.	Coerção legal ou ilegal, executada por governos e outras organizações.

Fonte: Tabela 3: Recursos de poder relativo entre os atores no domínio cibernético, NYE (2010:10)

1.2.8 Como a tecnologia afeta os atores e o sistema internacional?

SIROLI (2006:41) reconhece que a conexão global e a interdependência trazem vulnerabilidades em termos de segurança. FRITSCH (2006:107) avalia a tecnologia como um elemento que influencia não apenas os atores no sistema internacional, mas também as próprias estruturas e processos desse sistema. Reconhece, ainda, uma escala de influência que transita do âmbito individual ao âmbito global. No primeiro, a tecnologia viabiliza uma série de interações – comerciais, culturais, etc. No último, a tecnologia é vista como parte de

megassistemas nos quais se definem os seus usos futuros, por exemplo. É nesse cenário que se constrói a ideia determinista da crescente dependência do ser humano em relação à tecnologia[13].

ARQUILLA (2010:2) argumenta que antes da internet e do www, seria inviável a articulação de uma rede terrorista "operando de forma coesa em mais de 60 países". Para o autor, esse tipo de contrassociedade civil[14] não precisa ser o único ator a beneficiar-se dos recursos digitais. Se bem empregados, tais recursos podem tornar o conflito "mais barato e menos destrutivo". Na era da "guerra em rede"[15] Arquilla elenca três regras (p. 3-5) para nortear o Estado em busca de um esforço de guerra que poupe "sangue e divisas":

- "*Many and smal beats few and large*" - Na análise de Arquilla, a mentalidade militar não concebe a vitória com menos, sempre se dará com quem tiver mais recursos. Assim, cria-se um problema de escala que torna as forças dos EUA incapazes de lutarem o que chama de *little wars*, em um mundo que já não comporta grandes contingentes. Fazendo referência às legiões romanas, Arquilla ressalta que não se trata apenas de forças divididas em grupos menores, mas sim da conexão em rede entre essas forças, variados equipamentos de ataque (como aviões de combate) e aliados locais.
- "*Finding matters more than flanking*"- o conceito fundamental dessa regra é que a grande guerra pelos flancos foi substituída por uma dinâmica de esconde-esconde, em que o inimigo surge apenas durante ataques surpresa e então desaparece. Nesse contexto, para enfrentar o inimigo é preciso primeiro encontrá-lo. A conversão de grandes unidades militares em pequenas unidades ganhas mais sentido na

13 A ideia de determinismo tecnológico é aprofundada por Fritsch em seu artigo. Ela permeia o discurso de organismos internacionais como a União Internacional das Telecomunicações (UIT), órgão do sistema ONU que reflete a composição combinada de atores estatais e não-estatais e que, em sua visão corporativa, já traduz o anseio de ser "proativo em relação ao que a humanidade possa necessitar no futuro". Essa visão consta do site da UIT, disponível em: http://www.itu.int/net/about/vision.aspx

14 No original em inglês*: uncivil society,* conforme Arquilla (2010:2).

15 *Netwar,*Arquilla (2010:2).

medida em que grupos menores passarão a rastrear o inimigo já que não é possível atacar em massa um único ponto.

- "*Swarming is the new surging*" - o *swarming* é caracterizado pelo ataque de pequenos grupos de maneira omnidirecional. Ataques por "*swarming*", ao invés de surtos em massa e localizados, são uma tendência identificada por Arquilla, autor que também evidencia a capacidade desenvolvida pelos inimigos de desencadear ataques simultâneos em múltiplos pontos. A incursão russa na Geórgia é citada como exemplo por demonstrar o emprego não só de militares, mas também de milícias étnicas locais somadas aos ataques simultâneos também no ciberespaço.

BAUMAN (2008:140) corrobora a ideia de desproporção da resposta estatal elencada por Arquilla. O autor considera os ataques estatais pesados e imprecisos, "[...]lançando-se sobre uma área muito maior do que a afetada pelo ataque terrorista [...]" geram mais terror do que seria previsto levando-se em conta apenas o ataque perpetrado inicialmente. Esse e outros fatores levam Bauman a considerar que quando um ato terrorista fracassar, "isso ocorrerá apesar da e não graças à crua e esmagadora violência dos soldados" (p.143).

ROSENAU (1997:18) suporta o conceito de que é difícil promover uma mudança de mentalidade quando afirma que os hábitos de análise são duros de matar[16]. Ele afirma isso em relação à dificuldade de muitos analistas de incorporarem aos seus estudos a noção de que "o mundo está passando por uma transformação fundamental". Alega Rosenau que embora tais analistas reconheçam algumas mudanças, não computam a elas caráter tão distinto que leve a adaptações no escopo da análise. Aprofundar essa tese foge ao escopo da monografia, mas suas considerações devem ser levadas em conta quando se analisa a guerra cibernética, o mundo virtual e o papel da tecnologia na sociedade internacional. Em vários

16 "*Analytic habits die hard*".

momentos esse tipo de questionamento virá à tona no estudo de um tema relativamente novo: a necessidade de novos *policy constructs*[17] é um exemplo.

A dificuldade de se analisar algo que foge ao *framework* analítico padrão ou ao costume pode ser uma das razões de a *cybercultura* ter operado por tanto tempo no *underground*. O mundo da mídia evidencia isso, dada a atenção (recente) dedicada aos *blogs* atualmente e o crescente descrédito da mídia tradicional, incapaz de adaptar formatos e linguagem ao mundo virtual com a agilidade que esse novo domínio exige.

1.2.9 Tecnologia – um tema subvalorizado nas teorias das RI

FRITSCH (2006:98) define tecnologia como "o conhecimento e os artefatos acumulados com o objetivo de realizar objetivos humanos de uma maneira específica e replicável". Para Fritsch, a densidade do sistema internacional foi consolidada na medida em que cresceram e se aceleraram as comunicações. Para esse autor, a tecnologia é capaz de minar, na prática, os conceitos de soberania e autoridade vinculados ao Estado e ao território desde Westphalia. Voltando seus olhos para as Relações Internacionais e a Economia Política Internacional, Fritsch acredita que a tecnologia é um tema subvalorado na análise produzida por esses campos. Para FRITSCH, a tecnologia precisa deixar de ser um valor exógeno nos modelos de análise das RI. Precisa ser integrada como um fator relevante, em resposta ao seu crescente papel e influência nas dinâmicas da sociedade internacional.

1.2.10 Aplicação de leis convencionais na futura guerra da informação

O direito internacional público e privado constituem campos em desenvolvimento nas RI, ainda marcados por dificuldades no *enforcement.* DARNTON (2006:140) avalia que a globalização e as dinâmicas transnacionais vêm

17 Seguindo a ideia de que meras analogias entre o mundo real e o virtual podem ser equivocadas.

criando novos desafios para o direito internacional nesses dois ramos. No caso do direito privado, a legislação internacional, baseada na soberania do Estado, já não estaria adequada a um ambiente de intercâmbios transnacionais. Para o autor, a obra de Hugo Grotius foi fundamental na constituição de leis da guerra com ênfase na aplicabilidade para os Estados e seria um ponto inicial igualmente importante na adaptação de novas leis aplicáveis também aos atores não-estatais.

É de particular interesse para Darnton a tendência de convergência das atividades civis e militares, que afeta também a tecnologia: essa ideia de convergência é a chamada *civilianization*[18] da guerra e dos assuntos militares, e é impulsionado inicialmente por fatores (p. 142) como o custo (a adaptação da tecnologia militar ao cotidiano civil corresponde a ganhos de escala que interessam aos diversos atores) e a ideologia econômica (que envolve a ideia de competição e a melhor alocação de recursos, que demandam a extensão da tecnologia militar ao mercado civil). Para ambos os casos, o sistema GPS e a própria internet seriam bons exemplos.

Para Darnton, vem ocorrendo uma integração entre os diferentes atores: os não-estatais já estão engajados nos esforços de guerra, e o Estado vem se envolvendo em operações de escopo mais abrangente do que as meras operações militares. O envolvimento das Forças Armadas do Brasil na luta contra o tráfico, na construção de estradas, nas disputas comerciais envolvendo a compra de caças, evidencia a combinação de interesses militares e civis. A força do tráfico de drogas ilustra outra tendência comentada por DARNTON (2006:144): o crescente emprego da violência por atores não-estatais. Tudo isso, para o autor, cria "tensão" entre um *status quo* configurado pela tradicional soberania de Estados e essa nova situação em que as leis da guerra e o próprio direito internacional são surpreendidos por um dinâmicas globais que fogem ao comum.

O debate que surge nessa conjuntura discute a aplicabilidade das leis atuais, algumas já centenárias, sobre os novos conflitos e conceitos que não existiam na época em que foram redigidas, como as guerras da informação. O mesmo debate vem

18 Em livre tradução, algo como a civilianização dos assuntos militares ou, simplesmente, a crescente influência de atores civis nos assuntos militares.

se desenvolvendo nos diversos campos afetados pelas redes e pelas comunicações digitais (a efetividade de analogias entre o crime comum e o crime cibernético é um dos exemplos desse dilema).

Nesse sentido, DARNTON (2006:147) vê na chamada cláusula de Martens, como consta na Convenção da Haia de 1907, um fator que favorece a aplicabilidade das antigas leis, tendo em vista que seus principais pontos permaneceriam válidos: os usos acordados entre as pessoas civilizadas, as leis da humanidade e os ditames da consciência. Em sua análise, adiciona o protocolo de Genebra de 1977, que dita a obrigação dos Estados-partes de levar em consideração se a adoção de novas armas seria contrária aos termos acordados. Apesar disso, em suas recomendações, Darnton considera importante submeter os atores não-estatais aos princípios das leis da humanidade. No sentido de incorporar a guerra da informação aos dispositivos jurídicos, o autor recomenda o fortalecimento do direito internacional prevendo, no que for possível, as diversas categorias de guerras da informação. A abordagem de tais guerras pelo marco legal deveria incluir, ainda, a formação de organismos internacionais independentes da influência dos Estados para cuidar do *enforcement*.

Falando dos protocolos de negociação, RANTAPELKONEN (2006:56) considera que "quando o inimigo é tão demoníaco (…) é impossível iniciar negociações". Refletindo sobre a dificuldade de levar soldados ao combate contra inimigos indefinidos, o autor aborda pontos importantes para o futuro das preparações para a guerra: por ser virtual, a guerra cibernética superaria os protocolos de negociação? A reflexão do autor abre caminho para outra incógnita: há espaço para uma ciberdiplomacia?

1.2.11 Sobre a efetividade dos ciberataques e o recurso ao uso da força

SOMMER e BROWN (2011) consideram como armas cibernéticas o acesso não autorizado a sistemas, os vírus, os *worms, os* cavalos de tróia, os ataques DNS, o

uso de *botnets*[19], os *root-kits*[20] e o uso de engenharia social. Tais armas podem ser utilizadas individualmente ou de maneira combinada com armas (que os autores chamam de armas cinéticas), potencializando os impactos. Os impactos, por sua vez, podem incluir o comprometimento da confidencialidade, o roubo de segredos, de identidades, a extorsão, o sequestro ou o bloqueio de sistemas. Chama a atenção no trabalho desses autores a voz dissonante em relação ao *hype* que foi gerado em torno da guerra cibernética. Para eles, a verdadeira guerra cibernética apresentaria as características de um combate real mas seria travada no ambiente virtual. Assim, no cenário atual, o debate sobre a segurança cibernética estaria sendo afetado pela dificuldade na padronização da terminologia e também pelo exagero de algumas análises.

Para Sommer e Brown, não é possível considerar em um mesmo dado estatístico eventos tão diferentes como um ataque de vírus ou um massacre efetivado com recursos sofisticados e ataques vindos de múltiplas vertentes. Céticos, os autores veem baixa a probabilidade de uma verdadeira guerra cibernética ocorrer, pois: os sistemas críticos já estariam protegidos contra as ameaças conhecidas, obrigando os programadores a encontrarem novos pontos frágeis; além disso, os efeitos de ataques cibernéticos seriam difíceis de prever; por fim, não haveria razões para um agressor limitar-se a um único tipo de armamento - no caso, não seria lógico ficar restrito a um ataque virtual (p.7).

A análise de SOMMER e BROWN (2011) soa limitada quando contraposta à visão de NYE (2010), para quem o poderio cibernético pode ser empregado para obter ganhos tanto dentro quanto fora do espaço cibernético. Não há sentido em limitar a análise por ambiente – físico ou virtual. Para NYE, tampouco faria sentido falar em domínio da cibernética, pois a crescente dependência de sistemas complexos cria vulnerabilidades que podem ser exploradas por atores não-estatais. Essa

19 *Botnets* são redes formadas por computadores infectados que seguem instruções de quem instalou os bots, aumentando a potência de ataques virtuais, por exemplo. Para mais informações, consultar o Cert.br. Disponível em: http://cartilha.cert.br/malware/sec7.html#subsec7.3

20 *Rootkits* são conjuntos de programas utilizados por um invasor para camuflar e manter o seu acesso a um computador comprometido. Para mais informações, consultar o Cert.br. Disponível em: http://cartilha.cert.br/malware/sec8.html#sec8

afirmação opõe-se à visão de SOMMER e BROWN de que os sistemas já seriam seguros diante das ameaças atuais.

SIROLI (2006:32) recorre à Sun Tzu para ajudar a explicar o impacto da cibernética na guerra: a excelência não estaria em vencer todas as batalhas que empreende mas sim na dominação do inimigo sem lutar.

WU (2006:176) cita a guerra centrada em rede, Network-Centric Warfare (NCW) como um conceito desenvolvido a partir dos conflitos no Iraque e em Kosovo. Quando emprega essa tática, o Estado espera controlar unidades de combate a partir de uma rede central. Isso favorece a convergência de esforços no comando de forças que encontram-se dispersas e a gestão no campo de batalha é facilitada. Assim, toda a operação é sincronizada e realizada em rede (visando maior efetividade).

1.2.12 As novas regras da guerra

"*The new rules of war*" é o título de artigo de ARQUILLA (2010) no qual apresenta um panorama atual das demandas do esforço de guerra e os conflitos inerentes ao processo de modernização das técnicas face à teoria e à prática tradicionais do combate empreendido pelas forças militares. A análise do autor enfoca as Forças Armadas dos EUA. O primeiro problema por ele identificado diz respeito à relutância da classe militar de adaptar-se a mudanças – com os riscos a que estão expostos, não haveria espaço para experimentar. O autor considera que a introdução de novas tecnologias no campo militar foi sistematicamente mal compreendida no princípio em vários momentos históricos: teria sido assim com as metralhadoras e tanques, depois com as armas nucleares e, agora, a era digital apresenta o mesmo dilema. A avaliação de Arquilla é a de que os EUA ainda não têm a compreensão adequada do potencial do emprego da guerra eletrônica e há um

sentimento de incredulidade em relação à guerra massiva diante dos fracassos no Iraque, guerra que tem custos estimados em USD 3 trilhões[21].

FRIEDMAN (2011) considera que "quanto maior a distância, maior o custo logístico" e que a grande fraqueza dos EUA é a falta de inteligência tática, que prejudica o desempenho das forças que lutam em territórios estranhos, desconhecendo a geografia e a cultura locais. Para superar essa debilidade, Friedman afirma que os EUA investem em tecnologia. Para as pessoas que consideram que os EUA empreendem suas guerras atuais de maneira não tão implacável, o autor responde que mesmo a brutalidade dos nazistas não foi suficiente para assegurar suas vitórias. E alega, ainda, que a "guerrilha apresenta vantagens que a brutalidade não é capaz de compensar". Refletindo sobre diversos problemas estratégicos e questionando o contingente necessário para uma ação efetiva na Eurásia, por exemplo, o autor avalia que a alternativa diplomática deveria ser considerada como uma ferramenta prática, não apenas como um "princípio moral", na mediação de conflitos.

A dificuldade de adaptação a mudanças manifesta-se com maior intensidade em atores que detêm grande poder. KEOHANE (1984:179) reconhece esse traço ao afirmar que os Estados menores não tem alternativa senão adaptar-se; são os Estados poderosos que podem optar por "adiar ajustes". Quanto mais forte o Estado, e quanto maior sua autonomia em relação a outros Estados, maior pode ser o adiamento de eventuais decisões. BURTON (2003:4) complementa essa ideia citando B.H. Liddell Hart: "a única coisa mais difícil do que introduzir uma ideia nova na cabeça de um militar é tirar uma ideia antiga"[22]. A dificuldade de adaptação rápida dos militares a novas ideias é uma imagem recorrente na literatura da ciberguerra.

BAUMAN (2008:163) relata a desorientação dos exércitos em um cenário no qual já não há mais uma linha de frente, "somente campos de batalha distintos, altamente dispersos e eminentemente móveis". Descrevendo os exércitos terroristas,

---

21 Estimativa de Joseph Stiglitz e Linda Blimes, de 2008, citada por Arquilla. Artigo original disponível em:
http://www.timesonline.co.uk/tol/comment/columnists/guest_contributors/article3419840.ece

22 *"The only thing harder than getting a new idea into the military mind is to get an old one out"*.

refere-se a eles como “domésticos” por não demandarem as estruturas complexas de um exército formal (os quartéis, as “áreas de desfile”, etc.).

1.2.13 Armamentos não-letais: a destruição das redes não leva novamente ao sofrimento de civis?

PATHAK et al. (2001:93-94) define armamentos não-letais (NL) ou menos-letais (LL)[23] como ferramentas empregadas em combate que permitem destruir a capacidade do inimigo de atacar ou sustentar-se na batalha, sem causar, no entanto, “a perda direta e visível de vidas humanas”. Os autores reconhecem, no entanto, que sozinhas, tais ferramentas não são capazes de ganhar uma guerra. Exemplos de tecnologias NL seriam pulsos eletromagnéticos ou o laser. No caso dos pulsos, os autores relatam uma vantagem estratégica para nações com desenvolvimento tecnológico inferior ao das grandes potências: a capacidade de um pulso de desconectar redes poderia reduzir as assimetrias entre nações pouco conectadas e nações muito dependentes de redes (p.95).

RANTAPELKONEN (2006:60) identifica uma tentativa de conferir um ar virtuoso à guerra com uso intensivo de tecnologia e exemplifica citando a guerra do Afeganistão, iniciada em 2001. As imagens de bombas de precisão foram prontamente distribuídas para a mídia, que reproduziu os ataques cirúrgicos como um avanço da técnica da guerra. Porém, a contrainformação também foi distribuída online, apontando falhas que causaram a morte de inocentes e o bombardeamento de civis.

1.2.14 *Hard power, Soft power*

Já foi mencionado anteriormente que NYE (2010) identifica impactos do *cyber power* no espaço cibernético e fora dele. Tal influência pode ser gerada por

23 Non-lethal weapons (NL) e less-lethal weapons (LL), do original em inglês.

ferramentas do mundo físico ou do mundo da informação. No mundo da informação, o *hard power* pode ser exercido por meio de ataques DDoS[24] (intra rede) ou por ataques a Sistemas de Supervisão e Aquisição de Dados (extra rede), usualmente utilizados por grandes indústrias e *utilities* para gerenciar seus processos. Uma evidência do emprego de *hard power* com impactos extra rede é a suposta ação do vírus[25] Stuxnet, engenho norteamericano/israelense desenhado para retardar o avanço do programa nuclear iraniano. Consta de matéria do New York Times que o vírus teria sido programado para propagar-se e chegar aos computadores que controlam o funcionamento das centrífugas, equipamentos essenciais para o enriquecimento do urânio, buscando danificá-las ou destruí-las. A ação, bem-sucedida, teria levado o presidente do Irã a reconhecer que ataques cibernéticos causaram problemas a algumas centrífugas.

O exercício do *soft power* nos domínios cibernéticos pode envolver o estabelecimento de normas e padrões (intra rede) ou o recurso à diplomacia pública para estimular uma mudança da opinião pública. NYE (2010:5) exemplifica afirmando que a atração da comunidade de software livre para adotar um determinado padrão ou os vídeos online de recrutamento da Al Qaeda constituem formas de *soft power* intra e extra rede. SOMMER e BROWN (2011:12) avaliam que há problemas na definição do que é a guerra cibernética. Sommer e Brown relatam dúvidas em relação ao escopo do que Nye chama de efeitos intra e extra rede: como classificar um ataque no mundo físico que tenha como alvos redes de computadores e infraestruturas associadas?

---

24 DDoS é o acrônimo de Distributed Denial of Service, um tipo de ataque em que um computador-alvo recebe uma quantidade tal de requisições que o sobrecarregam, tornando indisponíveis os serviços por ele oferecidos. Leia mais a respeito no site da RNP – Rede Nacional de Ensino e Pesquisa. Disponível em: http://www.rnp.br/newsgen/0003/ddos.html

25 Vírus é um programa de computador que pode infectar outros programas e arquivos, propagando-se e gerando problemas variados como a perda de dados ou o mal funcionamento do sistema. Pode ser utilizado para fins maliciosos. Mais detalhes sobre vírus podem ser conferidos na Cartilha de Segurança na Internet do Cert.br, disponível em: http://cartilha.cert.br/malware/sec1.html#sec1 Para mais informações sobre o vírus Stuxnet, ver a matéria do New York Times disponível em: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1 e o quadro especial que descreve como se propaga o Stuxnet, disponível em: http://www.nytimes.com/imagepages/2011/01/16/world/16stuxnet_g.html?ref=middleeast

1.2.15 *Cyberwar*, *hype* e a necessidade de alvos militares

Para Gal Levy, entrevistado por CARTA (2011:67), "há interesses materiais para que as guerras prossigam", eles podem ser diretos (indústria de armas) e indiretos, tendo em vista que outras indústrias tiram proveito dos avanços tecnológicos produzidos pela ciência da guerra. Levy aponta, ainda, o apelo mercadológico da guerra: "generais viram políticos ou migram para o mundo dos negócios", e, de fato, já foi noticiado que militares com experiência em combate vêm sendo contratados por companhias privadas nos EUA.

O *hype* em torno da guerra cibernética pode ser fruto também do sentimento de insegurança generalizado de que fala BUZAN (1984:111), para quem a insegurança é um problema de "imensa escala e complexidade", cujos impactos são sentidos tanto na esfera do indivíduo quanto em âmbito global. Dada a natureza competitiva da relação entre Estados, o sistema estatal é, para Buzan, "dominado pelo problema da insegurança" (p.112). É provável que esse clima favoreça o papel ordenador do Estado, e, assim, seja uma justificativa para a sua afirmação. Ao mesmo tempo, o mundo globalizado e conectado apresenta novas ameaças à estabilidade que o Estado vem buscando assegurar. São dinâmicas que causam instabilidade e que não se resolvem com respostas locais e intrafronteiras. O próximo capítulo aborda os impactos do mundo virtual na soberania e as vulnerabilidades do Estado.

2. ESTADO, SOBERANIA E *CYBERWAR*

2.1 A SOBERANIA DESAFIADA

BODIN (1955) mencionava a dificuldade em estabelecer uma definição para a soberania, mas reconhecia que ela estava relacionada a um "poder absoluto e perpétuo investido na comunidade"[26]. O autor também entendia que o verdadeiro soberano deve manter-se atrelado ao seu poder, mesmo quando delega atribuições. Isso só é possível quando existe o reconhecimento de que o soberano é o verdadeiro detentor do poder.

Para GROTIUS (2005:169), citando Agostinho, "a ordem natural estabelecida para conservar a paz dos mortais exige que o poder e a vontade de fazer a guerra residam na pessoa dos príncipes". Os atos soberanos são aqueles que independem da "disposição de outrem" (p.175), não estando sujeitos, portanto, à anulação segundo a vontade de outros atores.

BAUMAN (1998:68) afirma que a ordem antes era representada pelo Estado, "que se gabava [de ser detentor] dos recursos suficientes para estabelecer e impor as regras e normas que ditavam o rumo dos negócios num certo território [...]". A ordem do mundo, assim, dependia do estabelecimento de Estados soberanos que organizavam seus respectivos setores na teia global. Para Carl Schmitt, apud BAUMAN (2008:164), a soberania era o "direito de excluir".A visão clássica da soberania de Estado é dramaticamente modificada na sociedade em rede. BAUMAN (1998:64) cita G.H. von Wright para mencionar a noção de que a nação-estado está se desgastando por "forças erosivas transnacionais". Tais forças não são coesas ou facilmente identificáveis, constituem "um aglomerado de sistemas manipulados por atores em grande parte 'invisíveis'"(p.65).

---

26 Do original em inglês: *SOVEREIGNTY is that absolute and perpetual power vested in a commonwealth which in Latin is termed majestas ... The term needs careful definition, because although it is the distinguishing mark of a commonwealth, and an understanding of its nature fundamental to any treatment of politics, no jurist or political philosopher has in fact attempted to define it. ...*

Em seu estudo sobre hegemonia e cooperação na economia política internacional, KEOHANE (1984:40;46) avalia que embora as relações hegemônicas do pós-II Guerra tenham tendido para uma espécie de "interdependência complexa", isso não confirmaria um declínio da importância do poderio militar. Talvez prevendo a crescente complexidade das relações internacionais (a edição data de 1984), o autor atestou a existência de relações complexas entre a hegemonia, a cooperação e os regimes internacionais. Nessa cadeia de relações, o poder do hegemon não seria garantia, por si só, de maior estabilidade ou de uma reconhecida liderança.

Para Keohane, o hegemon depende do escopo institucional para influenciar o estabelecimento de regras de seu interesse que venham a direcionar as ações das demais nações. Apesar de sua preponderância, o hegemon não consegue "criar e fazer cumprir as normas sem um certo nível de cooperação dos outros estados soberanos" (p.46). O esforço de combater o crime cibernético e a definição de normas de propriedade intelectual evidenciam esse quadro.

KEOHANE (1984:181) também considera em sua análise que uma redução do poder hegemônico pode aumentar a demanda, no sistema internacional, pela adoção de regimes, concluindo que, após a hegemonia, os regimes podem vir a tornar-se "meios importantes para a limitação da incerteza e a promoção de acordos com benefícios mútuos". Analisando o declínio de modelos hegemônicos, Keohane se pergunta se é possível a cooperação não-hegemônica face a evidências de que a ausência de um ator dominante a ditar as regras tornaria a cooperação mais difícil. Embora a resposta a essa pergunta fuja do escopo da presente monografia, tal discussão é vital, por exemplo, em termos do regime de governança da internet que vem tentando se estabelecer desde a última década. Esse debate repercute nas infraestruturas críticas e, portanto, no campo de batalha virtual.

MELANDER et al. (2009:510) afirma que o processo de construção de Estados no princípio da era moderna envolveu guerras, que levaram à consolidação de Estados em menor número e cada vez mais poderosos. O autor cita Holsti e Kaldor, para quem as novas guerras tenderiam a dificultar a delimitação entre "assuntos internos e externos, entre o público e o privado, entre o civil e o militar e mesmo entre a guerra e a paz".

A revisão apresentada por Melander depura, a partir de um conjunto de análises, a preponderância de "formas de organização social exclusivistas"[27], decorrentes do fracasso em se obter uma sociedade segura e na qual um cidadão possa se desenvolver. Essa insegurança e busca de desenvolvimento levariam ao reforço de grupos unidos em torno de algo em comum, como a religião, a língua, a cultura digital, ao invés de unirem-se em torno da bandeira de uma nação ou de um ideal como a democracia. A formação desses grupos exclusivos é importante para a compreensão do panorama quando o elemento virtual é adicionado: a porosidade das fronteiras é aumentada pelo poder das comunicações instantâneas e os grupos exclusivistas, antes restritos a âmbitos locais, passam a encontrar eco global na rede.

NYE (2010:9) avalia que o fato de a infraesturutra física da internet ainda estar sujeita à geografia[28] viabiliza um relativo controle pelos governos, que desempenham o papel de gestores dos espaços geográficos. Com isso, há um canal para o exercício de *soft power* pelo Estado, estimulando ou minando – por exemplo - o desenvolvimento de recursos diversos (pesquisa em ciência e tecnologia, patentes, ambiente legal e regulatório) que podem determinar a trilha de um país no mundo cibernético – o estímulo ao desenvolvimento ou a filtragem, a censura e a contenção.

ROSENAU (1997:8) entende que o papel da governança é "promover a ordem em meio a fronteiras em mutação, esquivas e frequentemente irreconhecíveis". Indicando um caminho possível para lidar com tanta incerteza, o autor diferencia "*governance in the world*" de "*governance of the world*". O jogo semântico em inglês carrega diferentes significados. Diante da impossibilidade da governança do mundo (*governance of*) por uma autoridade central, Rosenau fala de encontrar padrões de governança "onde quer que estejam se desenrolando (…) - nas comunidades, sociedades, ONGs, relações internacionais e ao longo da Fronteira[29]" (p.10). O autor resume o panorama de contradições vigentes, que geram dificuldades

27 *Exclusive forms of social organization*, citadas pelo autor, incluem religião, língua ou laços étnicos. *Inclusive forms*, por sua vez, são evidenciadas pela democracia, socialismo ou nacionalismo.

28 O núcleo central da internet, os principais roteadores que canalizam todo o tráfego do mundo, tem seu controle concentrado nas mãos de países desenvolvidos, principalmente dos EUA. Esse é um dos temas polêmicos no debate de questões sobre a governança da internet.

29 Essa Fronteira, com F maiúsculo, resume o conceito do autor para um novo e amplo espaço politico ("*a new and wide political space*") - ROSENAU (1997:4).

para autores e analistas avaliarem o estado das coisas no mundo: (ROSENAU, 1997: 4)

- "o sistema internacional tem menos poder de mando mas ainda é poderoso";
- "os Estados estão mudando mas não desaparecendo";
- "a soberania estatal vem sofrendo erosão mas ainda é defendida com vigor";
- "os governos estão mais fracos mas ainda têm peso";
- as paisagens variam, convertem-se em ambientes étnicos, midiáticos, mundos de ideias e tecnologia, mas a preocupação com o território continua sendo atual para muitos.

Skolnikoff, apud ROSENAU (1997:19) também contribui para o elenco dessas contradições ao comentar suas dúvidas sobre transformações tidas como marcos de grandes mudanças. Para ele, mudanças promovidas pela tecnologia podem "alterar a natureza das armas, mas não negam o papel do poder nas relações internacionais", modificam o balanco de poder mas não necessariamente o que esse poder significa nas mãos do Estado, estabelecem novos padrões de trocas econômicas entre as diferentes sociedades mas "deixam a gestão do sistema econômico basicamente nas mãos dos Estados", embora modifiquem a relação entre governos e atores não-estatais, não revogam a autoridade original dos governos. Em resumo, para Skolnikoff tudo isso leva a politica internacional a tornar-se "mais complexa, mas não fundamentalmente diferente". Na visão de Rosenau, a análise de Skolnikoff evidencia a dificuldade dos autores para abordar anomalias, mudanças e regularidades. Afirma ROSENAU (1997:20): "na ausência de critérios [que estabeleçam] o que Skolnikoff considera como mudança ou regularidade, ele não pode perder"[30]. Em contraponto, para Evans, apud ROSENAU (2003:65):

30 ROSENAU (1997:21) prossegue sua análise afirmando a necessidade de um refinamento do conceito de "mudança" para que a ambiguidade seja mitigada e para que o conceito permita o estabelecimento de futuras tendências. Mantidas as atuais condições, um analista enfrentará dificuldades para diferenciar entre as anomalias aquelas que correspondem a novos padrões e aquelas que representam apenas desvios em um "padrão recorrente".

> Na medida em que a riqueza e o poder vem sendo incrementalmente gerados por transações privadas que se dão através das fronteiras dos Estados, e não dentro delas, ficou mais difícil sustentar a imagem de que os Estados são os atores proeminentes na escala global.

ROSENAU (2003:61) cita Arquilla e Ronfeldt, que falam sobre a importância das redes e como progressivamente serão elas as promotoras do engajamento em conflitos, em lugar de estruturas hierárquicas estatais tradicionais (embora em sua linha de raciocínio o autor reconheça que "sempre haverá a necessidade de uma hierarquia"(p.266) e que o fato de as redes terem se convertido em um formato preponderante entre as formas de organização social "não implica que as hierarquias estão destinadas à extinção" (p.266)).

Rosenau aborda outra mudança quando afirma que a "erosão da soberania é também evidente na menor propensão do povo a enxergar o seu Estado como o alvo de sua maior lealdade" (p.70). Para algumas pessoas, a possibilidade de mover-se pelo mundo vem ganhando importância e, ao mesmo tempo, essa mobilidade vem contribuindo para o adensamento de "sociedades multiculturais". Diante desse quadro, e com as pessoas mais educadas, com a maior mobilidade entre os diferentes países, com o enfraquecimento dos governos e a proliferação de atores não-estatais, Rosenau identifica a formação de uma crise de autoridade que se alastra não apenas por governos, mas também por outros campos como a religião e os próprios domínios privados, nos quais os *shareholders* já questionam as ações dos *boards* de muitas companhias.

Por fim, BAUMAN (2008:26), citando Timothy Garton Ash, fala do processo de descivilização:

> Remova as bases elementares da vida civilizada, organizada – comida, abrigo, água potável, um mínimo de segurança pessoal – e em questão de horas voltaremos ao estado de natureza hobbesiano, à guerra de todos contra todos.

O papel ordenador do Estado, assim, poderia ser desestabilizado por abalos nas referidas "bases elementares da vida civilizada"? E se tais bases fossem cada vez mais dependentes de TICs na Sociedade da Informação? De fato, cadeias logísticas,

utilities e serviços vitais estão cada vez mais conectados em rede suprindo necessidades essenciais nos dias de hoje como água, transporte, comunicação. Quais os impactos das ferramentas e do ambiente virtual nessa ordem das coisas? A partir da definição das vulnerabilidades do Estado no domínio virtual, na seguinte seção, segue-se a discussão de tópicos que podem oferecer uma visão do que está em jogo

2.2 VULNERABILIDADES DO ESTADO NO DOMÍNIO VIRTUAL

Buscando uma visão multidimensional dos efeitos da tecnologia no campo das RI, FRITSCH (2006:104-107) reconhece a capacidade de articulação de interesses individuais que se combinam para formar coletivos de caráter global. Nesse sentido, o autor nota a crescente influência dos indivíduos e, citando Brown e Studemeister, replica a ideia de que os Estados não sabem como responder à demanda de "supraindivíduos" como Bill Gates, George Soros, Jimmy Carter ou Osama Bin Laden" (p. 104). Outra característica citada por Fritsch é que o controle do fluxo de informações é dificultado pela variedade de técnicas com as quais os atores podem criar alternativas de acesso a dados. Cita que para a hipótese de um controle ferrenho do tráfego de dados, há táticas terroristas que envolvem o uso de meios não digitais, como videotapes ou mensageiros. Assim, uma mensagem, apesar dos contratempos, invariavelmente consegue alcançar os destinatários.

FRITSCH (2006:106-107) também recorre a Rosenau para explicar as novas esferas de autoridade (SOAs, na sigla em inglês) vinculadas aos diversos atores que emergem do processo de globalização e registra, ainda, o aumento dos intercâmbios sócio-culturais, econômicos e políticos entre as diversas sociedades. Nesse mundo multicêntrico, atores não-estatais desenvolvem uma governança própria que, por vezes, tem que interagir com o tradicional mundo estado-cêntrico. O mundo tradicional, por sua vez, tenta assegurar algum controle por meio de mecanismos de governança global como regimes ou organismos internacionais, dentro dos quais podem influir no estabelecimento de regras, normas, padrões,etc. De todo modo, os Estados não estão mais sozinhos nesses arranjos internacionais e sofrem crescente pressão e influência de atores não-estatais.

A decisão de alguns governos de investir em poderio cibernético pode encontrar guarida na análise de KEOHANE (1984:24), para quem muitas das decisões tomadas pelos Estados decorrem de cálculos estratégicos de curto e longo prazos que podem levar em conta tanto o consumo de recursos quanto os ganhos de poder ou riqueza. Esse cálculo é feito face ao investimento necessário para alcançar tais ganhos. Se essa busca de poder e recursos se reproduzir no ciberespaço, os Estados estariam adaptando práticas do mundo físico ao mundo virtual. Uma dúvida presente é se o espaço virtual vai se limitar ao papel de uma arena adicional aos tradicionais espaços de disputas interestatais.

Para ROTHKOPF (1998:325), a Revolução da Informação provoca instabilidade nas relações de poder baseadas nos pilares econômico-político-militar. Autores como NYE (2010:3) já reconheceram que o mundo virtual é um novo domínio de poder que torna mais complexa a definição de soberania:

> o espaço cibernético não substituirá o espaço geográfico e não abolirá a soberania de Estado, mas a difusão de poder no ciberespaço coexistirá e e complicará o significado de ser um Estado soberano ou ou país poderoso.

NEUMANN (2006:73-74;77) avalia que todas as atividades humanas vêm ficando cada vez mais dependentes de computadores. Ele elenca algumas vulnerabilidades da tecnologia que, para os propósitos desse estudo, impactam nas dinâmicas do Estado. Os sistemas de informação, por exemplo, seriam cheios de vulnerabilidades e elos fracos, em parte por conta de um mercado de produção em massa que não vê vantagens no desenvolvimento de sistemas mais robustos. O autor ressalta que não se pode confiar em sistemas ditos infalíveis ou contar com a ausência de falhas humanas. Outra fraqueza deriva da Internet: por sua natureza aberta e anárquica, a rede torna-se vítima da “ganância corporativa, da falta de um comando central, dos anseios controladores dos governos”, dentre outros fatores. Outra variável listada por Neumann é a vulnerabilidade natural das infraestruturas críticas, que estariam sujeitas a ataques internos, externos ou mesmo ao colapso independentemente qualquer ataque. O autor afirma, ainda, que vários acidentes ferroviários foram associados à combinação de falhas humanas com problemas de hardware e de software.

FRITSCH (2006:101) analisa a perda de poder do Estado e põe em perspectiva o modelo proposto por Rosenau, que reconhece turbulências decorrentes de intercâmbios mais complexos e variáveis nas relações entre os atores da política global. Citando o aumento do número e da variedade de atores novos e antigos, bem como os processos de globalização que os integram nas áreas mais diversas como econômica, militar, social, cultural, Fritsch reconhece na tecnologia o poder de catalizar a turbulência de que fala Rosenau.

LARKIN (2006:113;118) fala da essencialidade das comunicações durante um momento de crise e relata que até a cadeia de comando dos EUA já foi abalada[31] no passado em momentos críticos que poderiam exigir uma resposta nuclear. Mesmo após o 11 de setembro de 2001, as fragilidades de comunicação ainda persistiam: naquela data, embora a estrutura de comunicações estivesse funcionando após os atentados, houve dificuldades em localizar o Secretário Rumsfeld, do Departamento de Defesa, fato que pode ter atrasado a tomada de decisão.

Indo além da comunicação, Larkin aponta falhas de configuração como outra vulnerabilidade do Estado e ressalta que, após os testes de instalação, não há políticas ou ferramentas empregadas para o contínuo monitoramento das configurações. O autor avalia que em termos de poderio militar, os EUA seriam capazes de vencer quaisquer batalhas contra inimigos desprovidos de artefatos nucleares. Porém, para Larkin, essa vantagem pode levar estrategistas neoconservadores a alimentar seus anseios de construir um poder imperial. “E os impérios caem” (p. 132). A visão do autor é a de que segurança e estabilidade são ganhos políticos que não podem ser assegurados apenas pelo poder militar ou pelas TICs. A construção de um ambiente estável e seguro demandaria um esforço visando a segurança coletiva e a formação de uma comunidade com interesses políticos comuns.

Para ROTHKOPF (1998:329), a facilidade da disseminação de informações por meio de TICs criou uma “Corte Internacional da Opinião Pública” com crescente influência sobre os Estados. Nem os EUA, com todo o seu poderio, estariam imunes

31 Para tanto, cita o incidente em 1981, quando o Presidente Reagan foi baleado e não havia clareza na cadeia de comando quanto a quem teria o comando dos códigos de ativação dos artefatos nucleares nem de quantos seriam.

ao burburinho gerado por essa "Corte"[32]. Além disso, Rothkopf identifica vulnerabilidades do Estado face à ascensão do setor privado em vários campos cujo acesso anteriormente era restrito: o valor das moedas, o lançamento de satélites espiões e a capacidade de influenciar as conversações entre as nações seriam evidência do papel mais ativo do setor privado na comunidade global - fruto das facilidades providas pelas TICs e do crescente poder dos mercados (p. 338).

2.3 A RESPOSTA ESTATAL E A NECESSÁRIA COORDENAÇÃO GLOBAL

Em 1997, um relatório chamado *Critical Foundations* foi publicado pelo governo norteamericano[33] reconhecendo a crescente dependência tecnológica do país e a possibilidade de ataques aos pontos vulneráveis de suas infraestruturas críticas. SIROLI (2006:43) acredita que a avaliação do que são essas infraestruturas críticas é um passo inicial e fundamental para a construção de uma estratégia visando protegê-las. A evolução desse plano veio com o *National Plan for Information Systems Protection* (no ano 2000). O plano também encorajava a proteção de liberdades civis e de dados proprietários, além de recomendar uma parceria-público privada para construir as bases da defesa cibernética. O autor reconhece, porém, que por mais que o compartilhamento de informações seja uma ação necessária, os diferentes interesses que movem atores públicos e privados podem constituir um problema e o grau de confidencialidade das informações compartilhadas também.

Ao mesmo tempo, o papel do governo na proteção das infraestruturas ficou mais incerto. A visão de que a segurança é reserva soberana do Estado já não se sustenta. Forças militares, por si sós, não garantem a segurança de cidadãos e de infraestruturas críticas. A mobilização durante emergências nacionais evidencia que o Estado, sozinho, em um cenário marcado pela privatização das *utilities*, não é capaz de oferecer as respostas adequadas que uma crise demanda. Ele pode assumir

32 Ver o caso de Guantánamo.
33 PCCIP – President´s Comission on Critical Infrastructure Protection.

um papel de coordenação e fomento, mas não proverá a manutenção de serviços de telecomunicações, das redes de energia ou das comunicações via satélite.

Mais do que isso, atualmente os dados de usuários transitam por bancos de dados de concessionárias privadas, prestadoras de serviços públicos, que têm natureza transnacional. Na hipótese de um conflito entre o país que privatizou os serviços para uma transnacional e o país que sedia a matriz dessa mesma transnacional, quais os riscos e interesses em jogo? Se a empresa for responsável por serviços essenciais, quais as implicações de um conflito de interesses entre os países e suas empresas? Alertando para o risco do estabelecimento de uma sociedade em estado de vigilância permanente[34], SIROLI (2006:45) considera que os limites entre a segurança nacional e internacional, assim como entre o militar e o civil, estão se afilando. Em sua análise, o autor identifica na coordenação global um caminho para o aumento da segurança das informações e dos sistemas de telecomunicações. Ressalta também que os interesses nacionais devem ser adequadamente balanceados com a preservação da privacidade dos cidadãos e a segurança das informações privadas (pessoais, comerciais, industriais) na esfera global.

Apesar de novas dinâmicas entre o público e o privado, e do crescente poder dos mercados, para ROTHKOPF (1998:342), os Estados não devem deixar de existir no futuro e seriam os atores remanescentes que manteriam a capacidade de abordar as questões humanas e próprias do sistema internacional estranhas à lógica dos mercados: o suporte às populações atingidas por desastres naturais e pelas guerras são exemplos citados pelo autor (p. 342). Em vários trechos de sua argumentação, nota-se a crença de Rothkopf na redução das assimetrias, que viabilizariam a competição direta, e mesmo o conflito direto, entre nações com diferentes perfis de poder, uma visão que põe em perspectiva a ideia de predomínio do país militar ou economicamente mais forte. Tal ideia associa-se com o conceito de *novas regras da guerra* de Arquilla[35]. Rothkopf ainda associa a perda de poder das instituições políticas estatais ao declínio do poderio do Estado, e identifica crescente poder

34 *Surveillance society.*

35 Por exemplo, *small and many beat few and large.* Ver ARQUILLA (2010).

político de atores não-estatais, na medida em que ganham relevância nos diversos sistemas que integram (p.355).

2.3.1 O caso russo

PANTELOGIANIS (2006:157-158) relata que, apesar de não ter sido bem sucedida na modernização de seu arsenal, a Rússia soube prever as guerras da informação. O desenvolvimento de ferramentas para "desestabilizar a sociedade por dentro dela" seria uma evidência da vanguarda russa nesse assunto, reconhecendo a inviabilidade de grande formações e a importância de melhor gerir "recursos de defesa escassos". A compreensão do papel da tecnologia da informação no campo militar merece destaque: a capacidade das tecnologias de "incrementar a efetividade militar" (sem necessariamente multiplicar o contingente ou a quantidade de armamentos) ou o seu emprego no desenho de ambientes virtuais para treinamento militar. Para os russos, a adoção das TICs seria uma forma ágil de equiparar capacidades com o Ocidente.

2.3.2 O caso chinês

Para WU (2006:187), as forças armadas dos EUA avaliam a estratégia de guerra da informação chinesa nos seguintes termos: pelo emprego de táticas de dissimulação (ex.: vírus embarcados em e-mails de rotina ou serviços de rede); pela prática de não atacar o inimigo com força letal (nuclear) diretamente, evitando, assim, uma retaliação que levaria à provável aniquilação (um ataque indireto poderia ter como alvo, por exemplo, o tesouro do inimigo ou seu sistema financeiro); mesmo não sendo forte o suficiente para atacar um inimigo, o chinês empregaria meios alternativos, "usando a força dos outros" - lançando vírus ou disseminando informações falsas por intermédio de terceiros atores; há ainda a tática de desencadear vários ataques para exaurir a força do inimigo e guardar a força total

para o ataque decisivo; por fim, outra alternativa é adotar disfarces para infiltrar-se no ambiente do inimigo e roubar segredos ou destruir sistemas[36].

Apesar de considerar a guerra da informação "o sistema nervoso" das operações militares chinesas (p. 173), Wu prevê dificuldades para o Estado chinês no campo de combate cibernético, por não ter uma indústria criativa de software desenvolvida, pelo fato de tecnologias-chave tanto em hardware quanto em software não terem controle chinês, pela falta de mão-de-obra qualificada e pela supremacia dos EUA no setor de TI. Adicionalmente, Wu considera (p.188) que na China faltam sistemas de segurança da informação adequados, que a dependência de equipamentos estrangeiros constitui uma vulnerabilidade e que a ausência de uma estrutura formal e integrada de gestão prejudica a estratégia do país. Para Wu, a própria sociedade chinesa não reconhece a importância da segurança da informação, o que indica, por si só, uma vulnerabilidade a ataques.

36 Wu apresenta os conceitos originais dos chamados "36 estratagemas" chineses, em inglês: cross the sea under camouflage, besiege Wei to rescue Zhao / Surround one state to save another, kill with a borrowed knife, wait for the enemy, loot a burning house.

3. *CYBERWAR* E AS POPULAÇÕES

3.1 GUERRAS VIRTUAIS, COMBATES REAIS

BAYER (2006:28) fala do fascínio que a guerra exerce sobre os humanos e sobre seu efeito inspirador até mesmo para jogos eletrônicos. O mundo virtual é também o mundo do entretenimento, um espaço em que vem se consolidando a convergência entre a política e a diversão. BAYER (2006:17) identifica nos jogos eletrônicos a crescente influência de uma nova dimensão: a política, que inspira a adoção de jogos para o recrutamento de soldados para guerras reais (cita como exemplo *America´s Army*).

RANTAPELKONEN (2006:69) chama a atenção para o incremento da virtualidade no cotidiano do ser humano, que acaba perdendo de vista as guerras empreendidas no mundo real: "o Congo é o exemplo mais recente de uma das guerras mais perversas do mundo, mas nós não podemos vê-la nesses tempos paradoxais da tecnologia e da informação" (p.69). Seja pela concentração da mídia, pelas barreiras linguísticas, pela urgência da busca de informação, falta às sociedades em geral o conhecimento de realidades locais. Essa concentração pode ser perversa e, para o autor, o conhecimento de aspectos locais é uma competência importante para evitar que informações unilaterais nos tornem "prisioneiros de uma guerra permanente".

Outro questionamento apresentado por Rantapelkonen: será suficiente matar o inimigo na tela? Ele também avalia que a coerção se tornará mais difícil na medida em que existem barreiras culturais e o inimigo é invisível, ocultando-se na sociedade. Mesmo a tecnologia de ponta se mostra ineficaz nessas condições.

Para BAYER (2006:23), a experiência de guerra virtual é limitada e mais atraente do que o dia-a-dia do combate real, e a capacidade de distinguir o real do virtual será essencial no futuro. Algumas características próprias dos videogames tendem a influenciar a ação de um jogador convertido em soldado durante um conflito real. O jogo oferece ao jogador a oportunidade de parar e recomeçar a partir

de qualquer ponto, mesmo que perca uma partida ou seja morto. O jogo, via de regra, não oferece nenhuma oportunidade de negociação, funciona baseado no espírito do "matar ou morrer". Em alguns casos, quanto mais se mata, maior o mérito. Muitas vezes não se registra a presença de civis no jogo, de modo que torna-se mais fácil selecionar os alvos. Dadas as tendências da evolução do armamento militar, a experiência adquirida nos jogos poderá ser útil para o controle de veículos não-tripulados e outros equipamentos sofisticados que integram ou integrarão a força militar.

Bayer reconhece que jogos violentos podem ser adotados no treinamento de matadores mas alerta que o combate real é bastante diferente do virtual. Reforça suas ressalvas dizendo que as Forças Armadas vêm empregando os jogos também para outros tipos de treinamento, como cooperação e comunicação, e destaca que há vários estudos do comportamento humano apontando para a capacidade dos seres humanos de distinguirem o real do virtual, à exceção de pessoas com graves desordens de personalidade.

3.1.1 A guerra virtual é mais legítima (ou aceitável) porque reduz a perda de vidas?

Na visão de DARNTON (2006:151), apesar de considerar que muitos pontos da legislação existente se aplicam às guerras da informação, há vácuos legais importantes quanto à *civilianization* das ações militares e a problemas humanitários "potencialmente sérios e em larga escala" que poderiam ser causados por elas. Reconhece, assim, a existência de riscos para as populações. As prováveis violações, mencionadas pelo autor, iriam contra os princípios tradicionais do direito internacional descritos abaixo:

- discriminação entre alvos militares e não-militares;
- emprego de armas proporcional ao objetivo militar;
- legalidade, não violando tratados e outros instrumentos do direito internacional;
- o emprego da força deve ser realmente necessário;

- humanidade, não impondo sofrimento desnecessário às vítimas;
- respeito às populações dos Estados neutros.

O autor identifica potenciais violações em cada um desses princípios em meio a guerras da informação (ver Quadro III):

QUADRO III – Potencial de violação de princípios das RI nas guerras da informação

Princípio	**Potencial violação em guerras da informação**
Discriminação	Na guerra da informação, o ataque muitas vezes visa alvos civis.
Proporcionalidade	Nem sempre os ataques visam objetivos militares, ou seja, o princípio não se aplica.
Legalidade	Muitas formas de ataque não violam leis de guerra, mas vão contra determinados dispositivos (como os que proíbem a perturbação das comunicações, por exemplo).
Necessidade	Nem sempre os ataques visam objetivos militares, ou seja, o princípio não se aplica.
Humanidade	O alvo nem sempre se encontra no campo de batalha e os efeitos das perturbações causadas por um ataque cibernético podem impor sofrimento desnecessário às vítimas.
Neutralidade	Não há garantias de respeito à neutralidade tendo em vista a natureza da sociedade em rede.

Fonte: DARNTON (2006:150).

Daí decorre que os supostos benefícios de uma guerra virtual precisam de estudos mais aprofundados antes de ser possível estabelecer conclusões sobre a suposta baixa letalidade da guerra eletrônica.

3.2 CULTURA DIGITAL E COMPORTAMENTO HUMANO

Há quem veja na comunicação via internet uma forma de diminuir os conflitos, reunindo pessoas de diferentes formações e culturas e permitindo que se conectem. Redes como Facebook, Twitter e You Tube são hoje algumas das ferramentas online disponíveis para desempenhar esse papel. No entanto, estudos apontam que a segregação de pessoas no mundo físico se repete no mundo virtual. Nos EUA, a análise de tópicos do Twitter37 permitiu a segmentação e comparação entre o que discutem internautas brancos e negros. No Brasil, a rede de relacionamentos Orkut mantém um apelo popular enquanto segmentos mais elitizados preferem o Facebook[38].

Assim como nas mídias sociais, a vida das populações e a guerra são influenciadas por questões culturais. Mathieu Guidère, apud VIANA (2010:16-18), tradutor e professor, defende que "só as iniciativas de mediação cultural podem levar à paz". O professor alega que a guerra vem passando por alterações em sua natureza, o que implica novos desafios: a comunicação é um fator fundamental em todas as etapas do conflito ou da intervenção. Sem ela, uma vitória militar pode ser desestabilizada pois "não é possível democratizar um país pelas armas"[39]. Advogando a necessidade de se conhecer línguas e culturas como um passo para a difusão bem-sucedida de ideias, o que denomina como mediação intercultural, Guidère destaca a capacidade de comunicação dos grupos terroristas, que conseguem transmitir conceitos que as populações sabem captar e incorporar. O professor vê o

37 Sobre essa segregação entre brancos e negros no uso do twitter nos EUA, bem como uma análise de como a visão de mundo pode estar sendo restringida ao invés de ampliada pela internet, ver os comentários sobre a apresentação de Ethan Zuckerman, do Berkman Center for Internet and Society, disponível em: http://www.bbc.co.uk/news/technology-10642697 . Acesso em 15 janeiro 2011.

38 A cyber-house divided. THE ECONOMIST, E-communication and society. 2 setembro 2010.
Disponível em: http://www.economist.com/node/16943885?story_id=16943885 . Acesso em: 4 setembro 2010.

39 No contexto da entrevista, fala-se muito do Iraque e Afeganistão e as intervenções norte-americanas na região.

enfraquecimento dos grupos terroristas e sua substituição gradual por ações individuais perpetradas por gente que internalizou os ideais de determinado grupo/facção e luta por eles, às vezes de maneira violenta. A essência de tal fenômeno seria o fato de ser desencadeada por indivíduos.

A internet viabiliza a ação isolada do indivíduo, que passa a ter condições técnicas de realizar ataques pontuais independentemente de pertencer a um exército organizado. É uma batalha que o perpetrador sabe que não pode ser vencida pois não tem por trás o peso de uma divisão armada, nem o orçamento, nem o apoio logístico. Contudo, apesar disso, guerreiros solitários seguem se multiplicando. O que os motiva? A função consultiva da internet como espaço para o engajamento pessoal em batalhas, mesmo que virtuais, é um aspecto importante do futuro da guerra que merece aprofundamento em futuros estudos. De fato, já não é tão simples alistar jovens para o serviço militar. A ideia de morrer em combate perdeu o charme que a propaganda ideológica vendeu durante as Grandes Guerras. Até tempos recentes, muitos filmes tratavam de tocar nas feridas das guerras: revisões históricas, bastidores, temas como honra e defesa de ideais nacionais, temas que, atualmente, não passam incontestados pela opinião pública. Os interesses militares e econômicos enxertados no moderno combate, a privatização das forças que combatem em campo e as implicações da existência de novos mercenários são os temas em voga nos dias de hoje.

A dificuldade de atrair cidadãos comuns para a batalha não é um fenômeno recente. ARON (2002:235) cita que na 1ª Guerra, "civis uniformizados" já questionavam por quem ou por qual razão deveriam morrer em campo, fato encarado de maneira diferente por soldados profissionais, para quem o risco é parte da rotina.

A alternativa que vem se desenvolvendo nos EUA, por exemplo, envolve o uso de robôs. SINGER (2010:42-49) relata que a adoção de robôs fora anteriormente questionada por macular a "cultura guerreira", mas esse posicionamento teve que ser revisto em resposta a um "inimigo irregular, que detona explosões por controle remoto com telefones celulares e, em seguida, desaparece de novo no meio da multidão". O autor destaca que, apesar de tirar soldados humanos da linha de frente dos combates, a adoção da robótica gera também um debate de natureza política,

ética e legal sobre a facilidade de se iniciar uma guerra partindo desse distanciamento promovido pela tecnologia.

MANJIKIAN (2010:393), citando Demchak, identifica uma aproximação entre civis e causas nacionais ao analisar o engajamento cidadão em guerras da informação travadas entre israelenses e palestinos. Compara essa constatação, inclusive, aos altos níveis de engajamento popular na Guerra Civil Espanhola. Para Manjikian, na China os internautas representam forças de reserva que podem ser convocadas a participar de ataques virtuais ou deslanchar a guerra popular em rede. Para a autora, esse movimento retrata tentativas dos Estados de governarem "seus" internautas, ou direcionar o comportamento deles.

Voltando ao tema dos robôs, Singer também reconhece uma tentativa de distanciamento do modelo robótico consagrado pelos filmes de *Hollywood*. Outras denominações vem sendo utilizadas para afastar a visão do robô como humanóide. E suas funções vêm sendo aprimoradas com base em softwares, sensores, GPS (sistema de posicionamento global via satélite), de forma que atualmente já é possível manejar um equipamento desse tipo com controles similares aos de videogames. As funções de monitoramento, captação de dados, seleção de alvos e ataque em áreas inimigas "sem ter de expor o operador humano ao perigo", citadas por SINGER (2010:45), também derivam dos impactos dos ataques de 11 de setembro de 2001. As guerras no Afeganistão e Iraque levaram ao aumento da demanda por equipamentos de robótica militar, fazendo com que a guerra se constitua também uma oportunidade comercial para mais este campo da tecnologia.

Singer vê nesse processo uma mudança cultural, visto que a luta em campo de batalha era uma questão de honra para o guerreiro humano e para os seus comandantes. Com o uso de robôs, muda o perfil da batalha e mudam também os soldados, o que levou à necessidade de recrutamento e seleção baseada em novas competências: adolescentes vêm sendo o alvo de campanhas publicitárias pelas Forças Armadas dos EUA[40].

40 O uso de ferramentas como redes sociais e atrativos como jogos online fica evidente no site das Forças Armadas dos EUA, leia mais: em http://www.goarmy.com/content/goarmy/downloads.html . Um mundo virtual foi criado para simular uma base militar e, clicando nos diversos pontos disponíveis na tela, o aspirante a recruta pode

A evolução da tecnologia militar trouxe vantagens comparativas para quem adotou novas técnicas em primeiro lugar. Singer recorda que o arco de madeira foi um diferencial em favor de camponeses feudais contra cavaleiros, assim como foram o tanque de guerra, os aeroplanos e os submarinos a partir da 1ª Guerra Mundial[41]. Para este autor, no entanto, a vantagem é precária e o uso sempre pode ser aprimorado por outros combatentes[42].

Tudo isso cria um novo contexto para o exercício da guerra e para o significado de entrar em combate. Se antes ir à guerra demandava arranjos políticos e institucionais capazes de angariar apoio logístico, político e social, hoje países como os EUA se engajam em ataques controlados à distância em países como o Afeganistão sem que seja necessário o escrutínio público ou debates no Congresso Nacional. De fato, SINGER (2010:47) afirma que "até o primeiro semestre de 2010, os Estados Unidos realizaram mais de 130 ataques aéreos no Paquistão com aparelhos não tripulados *Predator* e *Reaper*". Os argumentos de precisão e baixo custo sustentam o avanço da tecnologia no campo militar. Mas, na realidade, tais avanços não têm significado vitória certa para os EUA e, como reflete o autor, apesar da ação cirúrgica, a figura do país é demonizada até mesmo em letras de rock "que acusam os Estados Unidos de não lutar com honra" (p.48).

Sobre esse assunto, é interessante resgatar o lamento do chefe mameluco Kurtbay, reproduzido em KEEGAN (2006:63): "Um único de nós pode derrotar seu exército inteiro. Se você não acredita, tente, mas por favor mande seu exército parar de atirar com armas de fogo"[43]. Para Keegan, a guerra não envolve apenas a política, tem uma dimensão cultural importante e muitas vezes pode ser "a própria cultura" para algumas sociedades. O autor também resgata a questão dos mercenários na

---

assistir ao cotidiano das diversas divisões militares, glamourizado pela linguagem cinematográfica e por um forte apelo bélico existente na sociedade dos EUA: http://www.goarmy.com/content/goarmy/home/virtual-world.html

41 Singer relembra que muitas inovações foram primeiramente citadas em narrativas de ficção de autores como H.G.Wells, Alan Milne e Conan Doyle.

42 Como ocorreu com o tanque de guerra, adotado primeiro por ingleses e que teve seu uso aprimorado pela Blitzkrieg alemã.

43 Keegan afirma que a cultura da guerra dos mamelucos, muçulmanos medievais, o manejo do arco e flecha predominava e houve resistência a atualizar as técnicas de batalha, o que levou à sua derrota para portugueses e turcos otomanos. Curiosamente, a necessidade de atualizar técnicas de guerra hoje pressiona mais os EUA, como discute Arquilla.

formação dos exércitos do período feudal. Numa época em que não havia nações e soberania, a ordem era mantida pela terceirização das forças de defesa, contratadas entre mercenários. Porém, a natureza dos mercenários era instável e, enquanto não guerreavam, saqueavam e causavam terror dentro dos próprios limites do reino. Atribui-se a Carlos VII o reconhecimento da primeira força mercenária oficialmente incumbida de proteger a monarquia (30-32). É interessante comparar a situação vigente à época, 1445-46, e o quadro atual em que o status de modernos mercenários pode ser atribuído aos *hackers*. Como é praxe, a história se repete, pois também no século XVIII, afirma Keegan, "todos os exércitos regulares, até mesmo os da Revolução Francesa, recrutavam soldados irregulares para patrulhar, reconhecer e travar escaramuças para eles" (p.21).

Outro aspecto relevante abordado por Keegan é a discussão sobre os custos da guerra, também presente nos comentários de Singer. Keegan identifica uma inversão na percepção de tais custos: anteriormente, seriam compensados pelos benefícios e hoje,ao contrário, os custos seriam maiores que os benefícios. Sua linha de argumentação considera que há custos materiais e que mesmo países ricos enfrentam problemas orçamentários devido aos altos investimentos no orçamento militar. Ele aponta inclusive para a perda da autonomia de países pobres que investem demasiado em armamento, deixando de lado outras frentes de seu desenvolvimento. Com o alto preço em vidas humanas, Keegan entende que a guerra hoje seria insustentável para países ricos e uma derrota certa, com perda de bem-estar e dificuldades de recuperação, para países pobres. Percebe-se na linha de argumentação a influência do vocabulário e dos conceitos da economia política internacional, com seus custos de oportunidade e vantagens comparativas[44], vocabulário também adotado por Singer.

A nova característica da guerra, a capacidade de ser executada à distância, é um dos fatores mais surpreendentes para a atual geração, provavelmente assim como foram o avião para quem lutava em terra ou o espaço sideral para quem combatia no ar. SINGER (2010:48-49) relata que nos EUA já há casos de soldados que

44 Outro aspecto moderno da análise de Keegan é a questão de gênero: para o autor, a guerra tem sido uma "atividade inteiramente masculina" (p. 111).

despertam, se arrumam e seguem para o trabalho normalmente, com a peculiaridade de que seu trabalho é comandar equipamentos eletrônicos que executam ataques a milhares de quilômetros dali. Considerando que os maiores riscos a que está sujeito esse soldado são os riscos do próprio ambiente de sua cidade, a guerra remota traz importantes implicações para o significado de estar em guerra.

De pronto, mudam as características do soldado, que passa a ter um perfil mais técnico do que força para o combate homem a homem. Jovens recrutas muito rapidamente passam a ter acesso a atribuições e comandos anteriormente restritos ao oficialato mais graduado. Há também uma pressão natural e estresse pois, apesar de parte do trabalho ser executado remotamente, os soldados nas zonas de guerra dependem da ação precisa de quem comanda robôs à distância. Erros ainda custam vidas. Para Singer, existe um "fardo psicológico"(p.49) para o soldado que não se resume ao de um jogo de videogame[45].

Na linha de argumentos apontados por esse autor, identificam-se traços de uma vertente tecnicista que aprova o uso de robôs e atribui a eles a provável redução de erros em campo de batalha e o respeito às leis de guerra. Singer contrapõe a essa visão o fato de que certas decisões no campo de batalha são tão ou mais complicadas para um robô. O porte de armas é tecnicamente possível de se identificar mas o papel de quem carrega a arma naquele momento pode induzir ao erro tanto um humano quanto uma máquina[46]. As questões legais que surgem com esses novos problemas levam SINGER (2010:49) a concluir que "a tecnologia com frequência avança mais

45 Para a sociedade existe também uma pressão com a morte de soldados, o que leva a crer que a intensa terceirização de serviços mercenários em teatros de guerra como o Iraque também visam reduzir o impacto social e pressões da opinião pública sobre o governo. Sobre esse assunto, Singer alega que o Departamento de Defesa dos EUA nunca definiu apropriadamente serviços que seriam restritos ao governo e quais serviços seriam passíveis de terceirização. O autor chega a identificar uma certa dependência do Pentágono em relação às firmas terceirizadas em uma escala tal que, sem elas, ficariam comprometidas tarefas básicas das mais fundamentais como a movimentação de comboios e a distribuição de suprimentos. Ver mais em: http://www.brookings.edu/opinions/2010/0227_defense_regulations_singer.aspx A importância da distribuição de suprimentos também é citada por Keegan, que afirma que a alimentação, o abrigo e o transporte dos soldados em combate segue sendo umas das grandes preocupações do comando de uma operação (Keegan,, 2006:94).

46 É o inimigo ou apenas um inocente buscando se defender? O fogo amigo também é outro fator importante e há casos de ataques a aeronaves dos próprios EUA fruto de erros de programação nos softwares que comandam determinados equipamentos.

depressa que as instituições sociais" e a perguntar como se adequam leis de guerra que vigoravam no século XX a esse novo contexto de guerra virtual.

3.2.1 Comportamento humano

WALTZ (2001:16) analisa o comportamento humano face às relações internacionais e identifica, em seu primeiro plano de análise (*first image*), de viés pessimista, o egoísmo, a raiva mal direcionada e a estupidez como causadores da guerra. Ao revisar diversos autores que se enquadram no seu primeiro nível de análise, Waltz cita Rousseau, para quem o comportamento humano é fruto da sociedade em que se vive, atribuindo um caráter indissociável ao estudo da sociedade, do ser humano e do governo. Há um componente irracional no comportamento humano, que Waltz identifica em Spinoza - "cada homem busca o seu próprio interesse, mas, infelizmente, não o faz segundo os ditames da razão"(p.23). Mas, para Waltz, incorre no erro quem tenta extrapolar de maneira acrítica o comportamento psicológico individual para a análise de fenômenos sociais de grupo (p.28)[47].

Para BAUMAN (2008:167), vivemos tempos incertos marcados pelo medo e pela "[...] insegurança e a incerteza […] [que] nascem de um sentimento de impotência: não parecemos mais estar no controle [...]", seja como indivíduos, seja como sociedades. O mesmo sentimento vale para "os assuntos do planeta". Essa perda de controle é um marco da desorganização, do desequilíbrio que afeta as Relações Internacionais e os vários campos da vida neste planeta, abrangendo desastres naturais, convulsões sociais e novos arranjos de poder, de cooperação, de produção, etc. Se tudo isso afeta o comportamento humano, talvez seja um indício que corrobora a avaliação de Rousseau anteriormente citada por Waltz.

47 *"To attempt to explain social forms on the basis of psychological data is to commit the error of pshychologism: the analysis of individual behavior used uncritically to explain group phenomena".*

Para ROSENAU (2003:xii), não é o alinhamento com um perfil conservador, liberal ou radical que diferencia as pessoas hoje, mas o“seu posicionamento quanto aos mundos próximos e distantes sobre os quais suas vidas estão assentadas”. Nessa oposição entre “próximo” e “distante”, será que o mundo cibernético e a própria guerra, em meio a tantas contradições e rearranjos, podem ainda ser vistos como algo distante? Nas palavras de Rosenau, na presente era o que parece distante está também ao alcance das mãos.

3.2.2 Estratificação e nacionalização dos internautas

MANJIKIAN (2010:393) reflete sobre a existência de fronteiras e de um caráter nacional que converte os internautas de simples civis em agentes militarizados sujeitos ao direcionamento estatal. Para a autora, além de adquirirem nacionalidade, os internautas também foram submetidos a segmentação e estratificação típicas do mundo real. Com isso, haveria dois tipos de cidadania digital – uma, de primeiro mundo, permite que os internautas tenham níveis de interação real com seus governos (padrão europeu); outra cidadania, de terceiro mundo, com acesso à informação e oportunidades de participação restritas ou proibidas (padrão chinês ou médio-oriental).

Na visão de WEGNER E MASON (2008:843), os civis não são mais apenas as vítimas de um conflito. Desempenham também o papel de perpetradores, ou seja, não seriam só as elites armadas, consideradas as elites governamentais ou rebeldes, as únicas responsáveis pelos padrões de violência estabelecidos em um determinado conflito. A resposta da população civil também teria influência sobre esses padrões, dificultando a diferenciação entre crimes comuns e ataques que integram o conflito, ou mesmo a separação entre civis e combatentes, também citada por RANTAPELKONEN (2006:68), que avalia que uma guerra nunca poderá ser vencida, mesmo com os mais avançados recursos tecnológicos, se o inimigo estiver oculto nas estruturas sociais, disperso na sociedade. A força da coerção, nessas condições, não é capaz de superar as barreiras culturais, que tendem a se tornar cada vez mais difíceis de serem transpostas.

DARTON (2006:143) identifica uma linha de pensamento com clara tendência ao predomínio da cultura militar na convergência dos mundos civil e militar (*civilianization*). Citando Virilio e Lotringer, reconhece um "cenário aterrador" no qual o indivíduo seria reduzido à função primordial de ser uma peça em um sistema que busca poder e ganhos econômicos.

MANJIKIAN (2010:392) avalia que a cultura norteamericana prevalece na análise do comportamento em relação à internet. Nessa análise, relata que os "EUA parecem ser os árbitros que decidem quais partes da internet merecem existir e quais representam *failed space"*. Sendo assim, o país age como o guardião de normas gerais.

A mesma autora identifica uma visão de comando do Estado em relação aos internautas: na China, internautas seriam vistos como uma força auxiliar, de caráter militarizado, com nacionalidade e sujeitos ao governo (p. 393). Do mesmo modo, a análise de Manjikian aponta para diferentes graus de cidadania *online:* a visão europeia teria uma vertente cidadã mais ativa enquanto a abordagem chinesa ou do Oriente Médio seria muito mais controladora – estes governos, por temerem o avanço democrático, promoveriam uma internet com oportunidades limitadas.

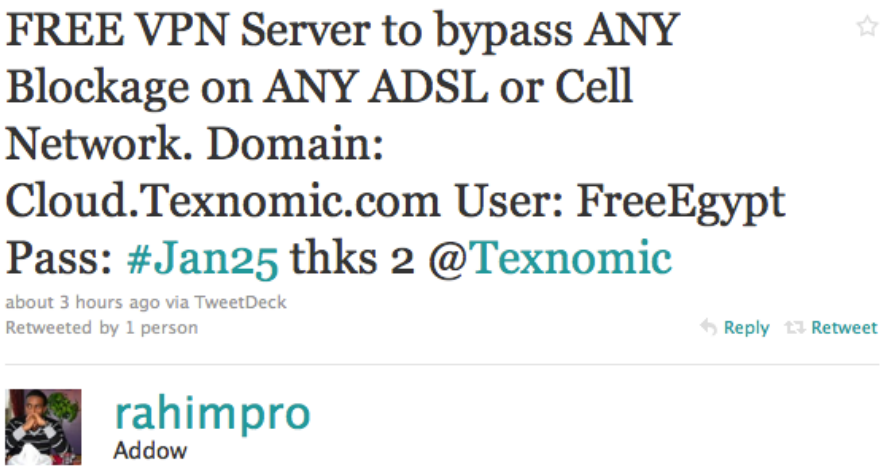
3.2.3 Mídias sociais e engajamento online

A capacidade de coordenação em rede de *hackers*, *trolls*, ativistas e atores similares pode indicar um poder multiplicador da internet maior do que o que ocorreria entre *rogue states*, por exemplo. No cenário corrente, um Estado não é mais capaz de desligar a internet e isolar-se do mundo pois o mundo pode prover aos cidadãos deste Estado as ferramentas que permitirão a eles ter voz e comunicar qual a sua visão e por que protestam. São vários os sistemas que permitem ao internauta evitar os filtros governamentais de uma internet fechada[48]. É possível usar uma VPN

48 *Circumvention tools* são softwares, que permitem ao internauta driblar filtros como o Grande Firewall da China, que barram o acesso a termos "sensíveis" ao governo, dentre outras restrições de conteúdo. Há relatos, contudo, de que apesar dos nobres propósitos, essas ferramentas também apresentam problemas na gestão de dados privados, que supostamente podem ser vendidos no mercado, como informa Hal Roberts, do Berkman Center for Internet & Society, em: Popular Chinese Filtering Circumvention Tools DynaWeb FreeGate, GPass, and FirePhoenix Sell User Data,

(Virtual Private Network)[49], de fato, foi um recurso disseminado via twitter para driblar os censores do governo egípcio.

FIGURA 1: Tweet revela os dados de acesso para uma VPN gratuita para os manifestantes Egípcios[50].



Fonte: Blog MASHABLE51

Outra forma de cooperação entre ativistas é demonstrada por sites como 10 tactics52 e Tactical Technology Collective53 , organizações que compartilham informações para empoderar ativistas no mundo inteiro ensinando estratégias de campanha e acesso à informação (algumas das publicações do 10 tactics) ou técnicas e ferramentas para garantir a segurança do ativista (Security in a Box, do Tactical Technology Collective). Grande parte dessa informação está disponível em inglês

---

disponível em: http://blogs.law.harvard.edu/hroberts/2009/01/09/popular-chinese-filtering-circumvention-tools-dynaweb-freegate-gpass-and-firephoenix-sell-user-data/

49 Conforme o glossário da Cartilha de Segurança para Internet 3.1 do Cert.br, disponível em http://cartilha.cert.br/glossario/, uma VPN, ou Virtual Private Network, é uma rede privada construída a partir da infraestrutura pública, como a internet, mas com acesso restrito a usuários e com informações criptografadas (associadas a outras técnicas de segurança da informação), de modo que nenhum dado que trafega pela rede é interceptado.

50 Dada a limitação temporal dos eventos mencionados, e no sentido de resgatar o contexto dos protestos da população contra o governo egípcio no início de 2011,ver a cobertura dos Protestos no Egito em 2011 do site Global Voices disponível em: http://pt.globalvoicesonline.org/cobertura-especial/protestos-no-egito-em-2011/

51 Disponível em: http://mashable.com/2011/01/27/bypass-twitter-facebook-block-egypt/ Acesso em: 3 fevereiro 2011.

52 Disponível em: http://www.informationactivism.org/

53 http://www.tacticaltech.org/

mas a necessidade de atender a diferentes públicos faz com que o conteúdo seja traduzido para outras línguas (espanhol, russo, árabe, chinês e vários outros idiomas). Esse trabalho muitas vezes pode ser executado por voluntários, o que indica a adesão do internauta a ideias, não necessariamente a bandeiras.

GHANNAM (2011:23) avalia que o impacto das mídias sociais no mundo Árabe ainda não pode ser efetivamente medido. Para o autor, blogues e redes sociais não podem ser vistos como ferramentas para uma mudança política imediata. Contudo, no longo prazo, os analistas devem ficar atentos ao desenvolvimento de novas formas de engajamento na política e na sociedade civil, a partir de competências adquiridas tanto por empresas quanto por indivíduos. Para Ghannam (p.25), as redes sociais "mudaram a natureza da liberdade de expressão conferindo aos árabes a possibilidade de fazer ouvir suas vozes de uma maneira sem precedentes". O autor imagina, por fim, se uma escalada da interação via redes sociais não seria capaz de criar uma unidade pan-Árabe.

Na análise de ARQUILLA (2010:2), a sociedade civil empregou as redes de uma maneira muito mais eficaz na promoção da causa da liberdade do que o arsenal militar norteamericano e "seus esforços problemáticos para levar a democracia ao Iraque e ao Afeganistão pela força das armas".

ROTHKOPF (1998:355), por fim, considera que o efeito democratizante das novas mídias pode ser um problema se a população for incitada por demagogos, cujos "abusos" as "democracias eletrônicas" teriam menos meios para controlar.

Para Eric McLuhan, entrevistado por BERTOL (2011:6), "quando uma identidade precisa ser reafirmada, forjada ou restaurada, a violência é um meio infalível para fazer isso rapidamente". Se a identidade também é impactada pelo mundo interdependente e conectado, e se McLuhan está correto, e a violência, como vista nas revoltas no Oriente Médio, "é sempre uma resposta à perda de identidade", será cada vez mais importante no futuro observar como se combinam as identidades no mundo cibernético e como se relacionam a violência e o engajamento online.

CONCLUSÃO

O presente trabalho é fruto de uma inquietação que surgiu em 2007, durante a apresentação de um estrategista de segurança informática israelense, Gadi Evron, no Fórum de Governança da Internet, na qual abordou o significado do ataque virtual à Estônia, atribuído à Rússia. Naquela oportunidade, o palestrante ilustrou o que significava a internet para o povo da Estônia, o fato de o cidadão não frequentar bancos, por exemplo, porque as operações já eram todas feitas via internet. Dito isso, ficou claro que um ataque à internet daquele país pode gerar graves perturbações. Ali plantou-se a ideia: um ataque virtual constitui um ataque à soberania?

Após a revisão da literatura, conclui-se que a definição de Rosenau, "turbulência", é uma característica dos nossos tempos. É certo que a história é marcada por anomalias que não são compreendidas, que têm seus impactos subavaliados, que são simplesmente desconsideradas para depois gerarem viradas surpreendentes nos rumos de uma sociedade. Mas uma característica marcante da turbulência na Era Digital é que sabemos demais e temos acesso a informações demais: talvez seja difícil aceitar que, apesar de tão educados e conectados, não dispomos do ferramental adequado para apreender a realidade em sua plenitude.

A análise dos vários autores nos leva a concluir que hoje não faz mais sentido observar as dinâmicas do ciberespaço apenas sob a ótica da soberania do Estado ou da disputa entre Estados. Mesmo uma organização como a Wikileaks foi capaz de compartilhar, via rede, segredos de Estado dos EUA que em outros tempos dificilmente viriam a público em estado bruto.

O caso Wikileaks x EUA aponta não só a fragilidade do controle de informações sensíveis mas também indica um novo tipo de atrito, não entre Estados, mas entre Estados e atores não-estatais. Se a luta não é por território ou soberania, como defender-se? Que ferramentas os EUA podem adotar para minar a Wikileaks? E o que os inimigos dos EUA podem fazer com as informações que foram vazadas? Não há respostas prontas e muito provavelmente nem os agentes inimigos sabem como atuar com tamanho fluxo de informações. O excesso de informações é um problema, pois demanda maior capacidade de processamento.

Como afirma Rothkopf, é preciso ter em mente que vivemos em um período de transição, momento em que haverá tensões entre o novo e o velho, afetando pilares das sociedades locais e da sociedade internacional na medida em que emergem tensões entre o público e o privado, o dominante e o assimétrico, as instituições políticas e a democracia eletrônica. O território ainda importa, a soberania ainda importa, mas o Estado não é mais o principal ordenador ou a reserva exclusiva de poder nesse ambiente anárquico. Pelo contrário, o Estado é mais um ator relevante entre muitos atores não-estatais com naturezas tão diversas quanto organizações terroristas, companhias transnacionais, supraindivíduos e mesmo não-indivíduos (a multidão do Twitter, dos blogs, das revoltas no mundo árabe e de outros mundos que ainda desconhecemos). A soberania permanece relevante, mas, como Rosenau indica, torna-se mais porosa para se adaptar ao novo cenário. Assim, análises viáveis devem levar em consideração os atores não-estatais.

Nye propôs uma classificação geral para as diferentes categorias de atores: governos; organizações com redes altamente estruturadas; indivíduos; e redes com baixo grau de organização. Dadas as diferentes motivações que podem ser associadas a cada categoria – caráter de sedição, fundamentalismos, religião, ilícitos transnacionais, cerceamento por parte do Estado, uma combinação de várias tipologias, etc. –, o trabalho de detalhamento por categoria é um esforço útil para estrategistas e um objeto relevante para futuros estudos visando a melhor compreensão dos desafios impostos pelas dinâmicas entre atores Estatais e não-estatais no mundo cibernético.

Outro traço marcante condensado a partir da bibliografia é o impacto das TICs na vida das comunidades. A questão da identidade nacional e do interesse nacional vem se convertendo em outros tipos de arranjos cooperativos. Para Melander, um exemplo são as *exclusive forms of social organization*. A leitura das fontes nos permite inferir que a capacidade de coordenação em rede de *hackers*, *trolls*, ativistas e outras formas de associação sinaliza o poder multiplicador da internet. Um poder colaborativo que se concretiza na internet e que não seria possível na mesma escala se *rogue states*, por exemplo, resolvessem trabalhar de maneira coordenada no mundo físico. Os benefícios da virtualidade afetam a sociedade para o

bem e para o mal. No campo das boas intenções, a adesão de voluntários globais a projetos de tradução de conteúdo para línguas tão diferentes quanto o chinês, o urdu, e mesmo o português, pode demonstrar que a identidade forjada entre os internautas e o mundo das ideias não está necessariamente associada a um limite territorial, a um idioma em comum ou a uma bandeira.

Os novos atores não apresentam uma identidade intrínseca porque a sua constituição e os seus objetivos são diferenciados: as motivações podem visar a insurreição, o terrorismo, o crime transnacional, dentre outras. Essas redes são altamente flexíveis e transitam, como afirma Rosenau, entre as esferas individual, regional e global com relativa facilidade. Outro ponto relevante, destacado por Rosenau, é a revolução de competências (*skill revolution*) que, combinada com a comunicação em rede, permite que as pessoas aprendam e compartilhem conhecimento e soluções de maneira quase instantânea.

Toda essa multiplicidade de atores e ações leva a complicações analíticas também para o mundo acadêmico. A Teoria Política, a Economia Política Internacional, o estudo das RI tradicionalmente repercutem conclusões exaradas em artigos científicos, análises baseadas em metodologias de análise clássicas e *standards* econômicos. No entanto, a investigação dos impactos do mundo cibernético nos Estados, no mercado e na sociedade internacional demanda um universo de captura de fontes mais complexo: muitas fontes primárias efetivamente encontram-se nos blogs, na Wikipedia, nos sites para a transmissão de vídeos e nas diversas redes sociais e de relacionamento. Anteriormente consideradas fontes sem credibilidade, ou mesmo irrelevantes, as novas mídias refletem hoje com mais propriedade as dinâmicas da Sociedade da Informação: a multiplicidade de atores, a quebra de hierarquia, a cooperação em rede e a repercussão instantânea são algumas das características do meio digital e da mídia cidadã. A reflexão de Manjikian completa esse quadro, quando afirma que o ciberespaço é livre em muitos sentidos, mas tem ideologia econômica: “é capitalista, não é socialista”.

A guerra cibernética é o novo front de batalha em um mundo marcado pela interdependência e por crescente complexidade. A insegurança e a incerteza deste momento histórico estimulam a cultura do medo e uma postura defensiva. Nas

palavras de Bauman, somos marcados por um sentimento de impotência, fruto da incapacidade de exercer o controle dos assuntos do mundo, individual ou coletivamente.

REFERÊNCIAS BIBLIOGRÁFICAS

10 TACTITICS FOR TURNING INFORMATION INTO ACTION. Disponível em: http://www.informationactivism.org Acesso em: 3 fevereiro 2011.

ARON, Raymond. **Paz e Guerra entre as Nações**. 1.ed. Brasília: Editora Universidade de Brasília / Instituto de Pesquisa de Relações Internacionais; São Paulo: Imprensa Oficial do Estado de São Paulo, 2002. p. 235.

ALMEIDA, Edson Pinto de. O poder anônimo. **Valor Econômico**, São Paulo, 11, 12 e 13 de março de 2011. Eu & Fim de Semana, ano 11, no. 541, p. 4-7.

ARQUILLA, John. **The new rules of war.** Foreign Policy. March/April 2010. Disponível em: http://www.foreignpolicy.com/articles/2010/02/22/the_new_rules_of_war?page=0,0 Acesso em: 4 fevereiro 2011.

ASHRAF, Cameran. **Iran´s Cyber Police, Geography, and the Psychological Denial of Service**. Global Voices Advocacy. 20 janeiro 2011. Disponível em: http://advocacy.globalvoicesonline.org/2011/01/20/irans-cyber-police-geography-and-the-psychological-denial-of-service/ Acesso em: 25 janeiro 2011.

BARLOW, John P. A declaration of Independence of Cyberspace. 1996. Hache. Disponível em: http://editions-hache.com/essais/pdf/barlow1.pdf Acesso em: 28 janeiro 2011.

BAUMAN, Zygmunt. **Globalização – as consequências humanas**. Rio de Janeiro: Jorge Zahar, 1998. 145p.

BAUMAN, Zygmunt. **Medo líquido**. Rio de Janeiro: Jorge Zahar, 2008. 239p.

BAYER, Martin. **Virtual Violence and Real War: Playing War in Computer Games: The Battle with Reality**. In: HALPIN, Edward et al. Cyberwar, Netwar and the Revolution in Military Affairs. New York: Palgrave Macmillan, 2006, p. 12 - 31.

BERTOL, Rachel. O filho é a mensagem. **Valor Econômico**, São Paulo, 25 de março de 2011. Eu & Fim de Semana, ano 11, no. 543, p. 6-7.

BODIN, Jean. **Six Books of the Commonwealth**. Oxford: Basil Blackwell Oxford, 1955. Disponível em: http://www.constitution.org/bodin/bodin_.htm Acesso em: 5 março 2011.

BROAD, William J; MARKOFF, John; SANGER, David E. **Israeli Test on Worm Called Crucial in Iran Nuclear Delay**. The New York Times. Online. 15 janeiro 2011. Disponível em: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=1&_r=1 Acesso em: 17 janeiro 2011.

BULL, Hedley. **A sociedade anárquica: um estudo da ordem na política mundial.** Brasília: Editora Universidade de Brasília,Instituto de Pesquisa de Relações Internacionais; São Paulo: Imprensa Oficial do Estado de São Paulo, 2002. p. 211 – 358.

BURTON Jr, Gerald V. **Principles of Information Operations: a recommended addition to U.S. Army Doctrine**. School of Advanced Military Studies. United States Army Command and General Staff College, 2003, 62 p. Disponível em: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA415801 Acesso em: 15 junho 2010.

CARR, Jeffrey. **Inside Cyber Warfare.** Sebastopol: O'Reilly Media, 2009. 214 p.

CARTA, Gianni. As vantagens da democratização (Entrevista com Gal Levy). **Revista Carta Capital**. São Paulo, Ano XVI, nº 634, p. 67, 23 fevereiro 2011.

CLAUSEWITZ, Carl Von. **On War.** Gutemberg Project. 25 fevereiro 2006 [1832]. Disponível em: http://www.gutenberg.org/files/1946/1946-h/1946-h.htm Acesso em: 7 março 2011 .

DARNTON, Geoffrey. **Information Warfare and the Laws of War.** In: HALPIN, Edward et al. Cyberwar, Netwar and the Revolution in Military Affairs. New York: Palgrave Macmillan, 2006, p. 139 – 153.

DUTRA, André Melo Carvalhais.**Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto.** IX Simpósio de Guerra Eletrônico, 2007. Disponível em: http://www.sige.ita.br/IX_SIGE/Artigos/GE_39.pdf . Acesso em: 12 outubro 2010.

FRIEDMAN, George. Never Fight a Land War in Asia. **Stratfor Global Intelligence**.1 março 2011. Disponível em: http://www.stratfor.com/weekly/20110228-never-fight-land-war-asia Acesso em: 1 março 2011.

FRITSCH, Stefan. **Technology as a source of global turbulence?** In: HALPIN, Edward et al. Cyberwar, Netwar and the Revolution in Military Affairs. New York: Palgrave Macmillan, 2006, p. 98 - 112.

GHANNAM, Jeffrey. **Social Media in the Arab World: Leading up to the Uprising of 2011.** 3 fevereiro 2011. CIMA – Center for International Media Assistance. National Endowment for Democracy. Disponível em: http://cima.ned.org/sites/default/files/CIMA-Arab_Social_Media-Report_1.pdf Acesso em: 4 fevereiro 2011.

GROTIUS, Hugo. **O direito da guerra e da paz.** 2. ed. Ijuí: Ed. Unijuí, 2005 [1625]. 767p.

HALPIN, Edward et al. **Cyberwar, Netwar and the Revolution in Military Affairs**. New York: Palgrave Macmillan, 2006, 253p.

KEEGAN, John. Uma história da guerra. São Paulo: Companhia das Letras, 2006, p. 12 – 111.

KEOHANE, Robert. O. **After Hegemony – Cooperation and Discord in the World Political Economy.** New Jersey: Princeton University Press, 1984. 290p.

LARKIN, Bruce D. **Nuclear Weapons and the Vision of Command and Control.** In: HALPIN, Edward et al. Cyberwar, Netwar and the Revolution in Military Affairs. New York: Palgrave Macmillan, 2006, p. 113 – 138.

LAVRUSIK, Vadim. **How users in Egypt Are Bypassing Twitter & Facebook Blocks.** 27 janeiro 2011. Mashable [blog]. Disponível em: http://mashable.com/2011/01/27/bypass-twitter-facebook-block-egypt/ Acesso em: 3 fevereiro 2011.

MAGNOLI, Demétrio (org.). **História das Guerras.** 3. ed. São Paulo : Contexto, 2006. p. 8.

MANJIKIAN, Mary McEvoy. **From Global Village to Virtual Battlespace:** the colonizing of the internet and the extension of realpolitik. International Studies Quarterly, 2010. ed. 54. p. 381-401. Disponível em: http://www3.interscience.wiley.com/cgi-bin/fulltext/123499963/PDFSTART. Acesso em: 21 julho 2010.

MELANDER, Robert et al. **Are new wars more atrocius? Battle severity, civilians killed and forced migrations before and after the end of the Cold War.** European Journal of International Relations. 2009. SAGE Publications and ECPR – European Consortium for Political Research. Vol 15(3). p. 505-536. Disponível em: http://ejt.sagepub.com/content/15/3/505 Acesso em: 9 fevereiro 2011.

NEUMANN, Peter G. **Risks of computer-related technology.** In: HALPIN, Edward et al. Cyberwar, Netwar and the
Revolution in Military Affairs. New York: Palgrave Macmillan, 2006, p. 72 - 81.

NYE, Joseph S. **Cooperação e Conflito nas relações internacionais**. São Paulo: Editora Gente, 2009. 369p.

NYE, Joseph S. **Cyber Power**. Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010. Disponível em: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf Acesso em: 17 janeiro 2011.

PANTELOGIANIS, Fanourios. **RMA: The Russian Way.** In: HALPIN, Edward et al. Cyberwar, Netwar and the Revolution in Military Affairs. New York: Palgrave Macmillan, 2006, p. 157 – 172.

PARKS, Raymond C.; DUGGAN, David P. **Principle of Cyber-warfare**. Proceedings of the IEEE Workshop on Information Assurance, 2001, p. 122 – 125. Disponível em: http://www.periwork.com/peri_db/wr_db/2004_May_11_11_30_41/DOCS%20WEB REVIEW/PrinciplesCYBER%20WARFARE.pdf . Acesso em: 12 outubro 2010.

PARSA, Ashkan. **Basij to Occupy Cyberspace.** Azadcyber. 2010? Disponível em: https://www.azadcyber.info/articles/1342 Acesso em: 25 janeiro 2011.

PATHAK, A. K. et al. **Concepts and Doctrines of IW: Impact of emerging non-lethal and less lethal technology weapons on limiting/preventing conflicts.** Global Business Review, 2001, p. 83-99. Disponível em: http://gbr.sagepub.com/content/2/1/83 Acesso em: 9 fevereiro 2011.

RANTAPELKONEN, Jari. **Virtuous Virtual War**. In: HALPIN, Edward et al. Cyberwar, Netwar and the Revolution in Military Affairs. New York: Palgrave Macmillan, 2006, p. 51 – 71.

ROBERTS, Hal. Popular Chinese Filtering Circumvention Tools DynaWeb, FreeGate, GPass and FirePhoenix Sell User Data. 9 janeiro 2009. Berkman Center for Internet & Society. Disponível em: http://blogs.law.harvard.edu/hroberts/2009/01/09/popular-chinese-filtering-circumvention-tools-dynaweb-freegate-gpass-and-firephoenix-sell-user-data/ Acesso em: 3 fevereiro 2011.

ROSENAU, James N. **Along the Domestic-Foreign Frontier: Exploring Governance in a Turbulent World**. Cambridge: Cambridge University Press, 1997. p. 3-21.

ROSENAU, James N. **Distant Proximities – Dynamics beyond Globalization**. New Jersey: Princeton University Press, 2003. 439p.

ROTHKOPF, David J. **Cyberpolitik: the changing nature of power in the information age.** Journal of International Affairs, volume 51, nº2, 1998. p. 325 – 359. Disponível em: http://link.periodicos.capes.gov.br/sfxlcl3?sid=metalib:EBSCO_APH&id=doi:&genre=&isbn=&issn=0022197X&date=1998&volume=51&issue=2&spage=325&epage=&aulast=Rothkopf&aufirst=%20David%20J&auinit=&title=Journal%20of%20International%20Affairs&atitle=Cyberpolitik%3A%20The%20changing%20nature%20of%20power%20in%20the%20information%20age.&sici=&__service_type=&pid=%20metalib_doc_number%3E012890360%20%2Fmetalib_doc_number%3E%20metalib_base_url%3Ehttp%3A%2F%2Fbuscador.periodicos.capes.gov.br%3A80%20%2Fmetalib_base_url%3E%20opid%3E%20%2Fopid%3E#3907928999695802606 Acesso em: 16 agosto 2010.

SECURITY IN A BOX. **Tactical Technology Collective.** Disponível em: http://www.tacticaltech.org/securityinabox Acesso em: 3 fevereiro 2011.

SINGER, P.W. Guerra das máquinas. **Scientific American Brasil**, São Paulo, Ano 8, nº 99, p. 42-49, agosto 2010a.

SINGER, P.W. The regulation of new warfare. **Brookings.** Fevereiro 2010. Disponível em: http://www.brookings.edu/opinions/2010/0227_defense_regulations_singer.aspx Acesso em: 5 setembro 2010b.

SIROLI, Gian Piero. **Strategic Information Warfare: An Introduction.** In: HALPIN, Edward et al. Cyberwar, Netwar and the Revolution in Military Affairs. New York: Palgrave Macmillan, 2006, p. 32 - 48.

SOMMER, Peter; BROWN, Ian. **Reducing Systemic Cybersecurity Risk**. OECD International Futures Programme: OECD / IFP Project on Future Global Shocks. Disponível em: http://www.oecd.org/dataoecd/57/44/46889922.pdf Acesso em: 18 janeiro 2011.

SZAFRANSKI, Richard. **A theory of information warfare**. Airpower Journal. 1995. Disponível em: http://www.airpower.au.af.mil/airchronicles/apj/apj95/spr95_files/szfran.htm Acesso em: 21 setembro 2010.

THE ECONOMIST. **A cyber-house divided.** E-communication and society. 2 setembro 2010. Disponível em: http://www.economist.com/node/16943885?story_id=16943885 . Acesso em: 4 setembro 2010.

VIANA, Diego. Estratégia idiomática. **Valor Econômico**, São Paulo, 3, 4 e 5 de setembro de 2010. Eu & Fim de Semana, ano 11, no. 515, p. 16-18.

WALTZ, Kenneth N. **Man, the state and war: a theoretical analysis.** New York: Columbia University Press, 2001. 263 p.

WEGNER, Andreas; MASON, Simon J. A. **The civilianization of armed conflict: trends and implications**. International Review of the Red Cross. Vol. 90, nº872, p. 835 - 852, December 2008. Disponível em: http://www.icrc.org/Web/eng/siteeng0.nsf/htmlall/review-872-p835/$File/irrc-872-Wenger-Mason.pdf Acesso em: 21 setembro 2010.

WU, Chris. **An Overview of the Research and Development of Information Warfare in China.** In: HALPIN, Edward et al. Cyberwar, Netwar and the Revolution in Military Affairs. New York: Palgrave Macmillan, 2006, p. 173 – 195.

ZUCKERMAN, Ethan et al. **Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites**. The Berkman Center for Internet & Society at Harvard University. Dezembro 2010. Disponível em: http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_DDoS_Attacks_Human_Rights_and_Media.pdf Acesso em: 25 janeiro 2011.

ZUCKERMAN, Ethan. Yahoo!Moniker: why is Mowjcamp.com still offline 6 weeks after hack attack? My Heart´s in Accra. 2 janeiro 2010. Disponível em: http://www.ethanzuckerman.com/blog/2010/02/01/yahoo-moniker-why-is-mowjcamp-com-still-offline-6-weeks-after-hack-attack/
Acesso em: 26 janeiro 2011.