SEGURANÇA NA ERA DIGITAL: SMARTPOWER E NOOPOLITIK NA SOCIEDADE DE REDE

Caio Cesar da Silva Rebelo[1]
Gabriella Nunes da Silva[2]
Renato Borges Macedo[3]

Resumo

Este artigo terá como objetivo explorar a articulação das novas tecnologias de informação na nova realidade geopolítica mundial, observando como o Brasil pode se utilizar dessa dinâmica em sua política externa. Para tanto, tais análises serão feitas a partir das teorias das Relações Internacionais, entre as quais figuram autores da corrente realista moderna como Hans Morgenthau e da corrente neoliberalista como Joseph Nye, assim como outros autores das Ciências Sociais, tais como Castells, Arquilla e Rondfeldt. Para reunir informações acerca do tema discutido, optou-se por uma pesquisa bibliográfica, abarcando algumas das principais obras sobre o tema. Uma vez que o trabalho objetiva partir da formulação de paralelo entre os exemplos mais notórios do uso da cibernética como ferramenta estratégica para a política, para a elaboração do raciocínio presente neste artigo, optou-se pelo uso do método comparativo. Ao final, espera-se apreender melhor as principais tendências no que toca o emprego da cibernética pelos Estados em termos de política externa, especificando o papel do Brasil nessa dinâmica.

INTRODUÇÃO

Desde as últimas décadas, o progresso e desenvolvimento das tecnologias de informação e comunicação em massa desencadearam uma série de transformações tanto na dinâmica das relações interpessoais quanto na produção e difusão de conhecimento. Graças à Internet, às redes sociais e à moderna telefonia móvel, surgiu todo um conjunto de estruturas e redes que transcendem os limites do tradicional modelo de Estado-Nação. Por um lado, essas novas ferramentas aumentaram exponencialmente o dinamismo e o alcance de ideias e informações, bem como os espaços de participação popular junto à esfera governamental; por outro lado, também se provaram um conjunto de instrumentos extremamente útil para práticas ilícitas e criminosas.

Este artigo procura explorar essa nova dinâmica sob o viés da segurança cibernética nacional, apontando as principais perspectivas para a inserção do Brasil nesse novo contexto das Relações Internacionais. Para tanto, partimos inicialmente de uma breve retrospectiva acerca do desenvolvimento tecnológico por trás da atual Era da Informação. Em seguida, buscaremos analisar como diferentes teóricos, tanto das Relações Internacionais, quanto das Ciências Sociais, abordam a temática da utilização do poder político através da cibernética, explorando conceitos como o Poder Político em Morgenthau, Poder cibernético e *Smartpower* em Nye e *Noopolitik* em Rondfeldt, Arquilla e Castells.

Posteriormente, realizaremos uma análise comparativa entre a forma como o Brasil trabalha atualmente sua política cibernética e como os Estados Unidos desenvolvem a sua própria. Por fim, iremos apontar algumas das principais possibilidades para que o Brasil desenvolva uma política externa mais condizente com a atual conjuntura internacional e suas potencialidades, além de reforçar sua posição enquanto potência regional.

EVOLUÇÃO HISTÓRICA

Para traçar a origem da internet e do próprio ciberespaço é preciso retornar à lógica de segurança dentro da Guerra Fria. Ao final dos anos 1960, havia por parte dos norte-americanos uma série de iniciativas para desenvolverem sua superioridade tecnológica frente ao sucesso soviético com o lançamento do *Sputnik* em 1957 (CASTELLS, 2003). A rede de computadores criada pela *Advanced Research Projects Agency* (ARPA) foi um projeto pautado em aperfeiçoar a transferência de informação entre os diversos computadores dos sistemas de inteligência norte-americanos. Apesar de constituir uma rede fechada, a Arpanet -como a rede foi chamada- já abarcava muitos dos elementos presentes na internet atual, tais como os primeiros sistemas de e-mail e salas

de bate-papo. Essa rede inicial, território de um grupo restrito de acadêmicos e técnicos, constitui o que –para fins didáticos- convenciona chamar de *web* 1.0 (PARRY, 2012).

Desde seu surgimento, a *web* se ampliou consideravelmente nas décadas seguintes, como pode ser percebido pelo *boom* no número de *sites*, que passaram de 50 em 1993 para 5 milhões em 2000 (NYE, 2011), graças à proliferação de provedores de internet e do crescente barateamento e miniaturização dos componentes eletrônicos utilizados, como processadores e semicondutores. Atualmente, a *web* também permeia a esfera do cotidiano e das relações interpessoais, essa é a chamada *web* 2.0. O princípio por trás desse momento é erosão da barreira que existe dentro das mídias entre os produtores de conteúdo e os consumidores. Hoje as mídias tradicionais (imprensa, televisão, rádio, cinema etc.) se encontram, em maior ou menor nível, diluídas e englobadas pela *web*, como é o caso dos jornais e outros periódicos *online*, *blogs* e redes sociais - essas últimas ganharam notoriedade nos últimos anos devido a sua elevada capacidade de difundir ideias e mobilizar grupos, sinalizando uma possível tendência no futuro.

Se por um lado as novas tecnologias do campo cibernético oferecem a possibilidade de uma ampliação do leque de interações sociais e da produção e difusão de conhecimento e informação, por outro, também criou um conjunto de ferramentas que se provaram extremamente úteis para organizações criminosas e outros grupos ilegais. Ataques de *hackers* a servidores governamentais, roubo de dados de empresas e governos, e esquemas fraudulentos via internet e até mesmo ataques coordenados entre países, tem se tornado algumas das principais preocupações dos governos na atualidade. Sobre esta temática, tanto os postulados de autores mais clássicos, como Hans Morgenthau, quanto os mais atuais como Joseph Nye possuem contribuições pertinentes para o entendimento das Relações Internacionais nessa nova era.

APORTE TEÓRICO: PODER POLÍTICO, CIBERNÉTICA E NOOPOLITIK

Entre os autores que figuram no rol dos clássicos das Relações Internacionais, Hans Morgenthau figura não somente como um grande expoente do realismo moderno, como também da disciplina como um todo, contribuindo para desenvolver a discussão sobre a natureza do poder político nas Relações Internacionais, campo onde muitos de seus postulados permanecem atuais mesmo diante das teorias mais recentes.

Falecido em 1980, a tecnologia de informação e comunicação em massa conhecida pelo autor se encontrava em primeiro lugar limitada pelo desenvolvimento de sua época e em segundo monopolizada por um pequeno número de grupos particulares e órgãos governamentais. Morgenthau não pôde, portanto, ver a expansão e a difusão da internet (incipiente na época), especialmente seu uso pela população em geral, uma marca comum da contemporaneidade.

Entretanto, esse fato não o impede de formular algumas colocações pertinentes dentro dessa discussão, ainda que algumas ressalvas sejam necessárias. O aspecto "faca de dois gumes" das tecnologias de informação, que ao mesmo tempo em que possibilitam aos indivíduos se comunicarem entre si com rapidez e eficiência, também fornece aos governos e aos órgãos privados de comunicação uma miríade de recursos tecnológicos para monitorar e –se necessário, cortar- quaisquer transmissões (MORGENTHAU, 2003) é extremamente atual, ainda que o autor subestime, devido em grande parte seu enfoque estadocêntrico, a natureza dinâmica dos meios de comunicação, principalmente o ciberespaço.

Atualmente, com o nível de acessibilidade e recursos de mídia disponíveis para toda a nova geração de computadores e telefonia móvel conectados a uma rede cada vez mais globalizada, é virtualmente impossível para qualquer Estado controlar completamente o fluxo de informação que entra e sai do próprio território – a exemplo do ocorrido no Mundo Árabe a partir de 2011 ou ocasionalmente na China -, dessa forma, a construção de uma opinião pública tanto nacional como internacional por parte dos órgãos políticos de cada Estado se torna um processo cada vez mais complexo e imprevisível.

Se por um lado sua formulação a respeito das tecnologias de comunição em massa – e notadamente da cibernética – deixam a desejar se analisadas à luz da realidade atual, sua formulação de poder na política internacional se mantém coerente e extremamente atual. A política enquanto uma das dimensões das Relações Internacionais, segundo o autor, resume-se a

luta pelo poder como fim imediato, seja para adquiri-lo, seja para conservá-lo ou demonstrá-lo, sendo a política internacional, portanto, a disputa entre aqueles que exercem o poder no sistema internacional: os Estados nacionais (MESSARI & NOGUERA, 2005). O Poder a que Morgenthau (2003) se refere é uma relação comportamental: se trata da forma pela qual um Estado utiliza seus recursos de poder para então transformar e influenciar o comportamento de outro, de maneira a possuir certo grau de controle sobre o mesmo, seja por forma de coerção direta ou cooptação, para atingir algum objetivo específico em sua política externa. A ameaça de ocupação militar e o peso econômico são exemplos clássicos, porém não podermos deixar de lado a questão da formação do apoio da opinião pública tanto nacional como internacional, levando em conta a base comportamental do exercício do poder (CASTRO, 2010).

Além de comportamental, a ideia de recursos de poder também é contextual. Morgenthau (2003) concebe os recursos de poder como variáveis, na medida em que ganham ou perdem relevância no cenário político internacional, conforme surgem novas tecnologias e formas de interação. Dessa forma, é possível afirmar que, muito embora o poder continue a ser produto de uma relação comportamental e o fim imediato de todos os Estados, os recursos a partir dos quais ele é exercido não apenas podem como tendem a mudar conforme as transformações do Sistema Internacional. Assim, a cibernética não era um recurso de poder tão importante na época de Morgenthau, mas isso não quer dizer necessariamente que a mesma não pudesse ganhar importância estratégica, conforme se vê na atualidade.

Se por um lado Morgenthau pouco analisou a dinâmica da cibernética, Nye (2012), por outro lado, dedicou especial atenção a esse novo domínio. O domínio cibernético, partindo de uma conceituação mais abrangente, não se limita apenas à Internet e às redes convencionais, se estendendo também às diversas intranets (redes de computadores fechadas, tanto públicas quanto privadas), à telefonia móvel e à comunicação via satélite.

Assim, em um sentido literal, o poder cibernético é definido como "um conjunto de recursos que se relacionam à criação, ao controle e à comunicação de informação baseadas em computador" (NYE, 2012). Apesar pertencer a uma tradição teórica fortemente contrária ao realismo de Morgenthau, Nye acaba por concordar com o mesmo ao conceituar o poder pelo viés comportamental e aponta o poder cibernético como sendo a capacidade de alcançar objetivos pretendidos, dentro ou fora do espaço cibernético, através do uso de recursos que a cibernética oferece (NYE, 2012).

Na esteira das transformações desencadeadas pela chamada Era da Informação, Nye (2012) observa que diversos novos atores no cenário internacional - como grandes corporações, grupos de indivíduos e ONGs – agora despontam dentro do cenário das relações internacionais justamente por causa das novas tecnologias de comunicação em massa e das novas teias de relações fora do controle efetivo do Estado-Nação tradicional que surgem com as mesmas (NYE, 2012). A esse fenômeno Nye chama de difusão de poder:

O que isso significa é que a política mundial não será a província isolada dos governos. [...] Tanto os indivíduos quanto as organizações privadas, variando desde corporações até ONGs e terroristas, estão capacitados para desempenhar papéis diretos na política mundial. A difusão da informação significa que o poder será amplamente distribuído e as redes informais enfraquecerão o monopólio da burocracia tradicional. [...] Os líderes políticos vão desfrutar de menos liberdade antes que possam reagir aos acontecimentos, e terão de compartilhar o palco com mais atores. (NYE, 2012. p. 154-155)

Isso não quer dizer, no entanto, que é possível considerar o Estado-Nação como uma relíquia ultrapassada, muito menos que a tecnologia de informação tenha nivelado em um mesmo nível de poder as grandes potências e os pequenos estados, e estes com as corporações e indivíduos. Como o próprio Nye afirma, embora os efeitos descentralizadores da tecnologia de informação sejam uma tendência, os Estados nacionais ainda figurarão como os protagonistas dentro da política internacional para os próximos anos (NYE, 2012).

Tanto como ferramenta quanto como um domínio à parte, os recursos cibernéticos podem ser usados tanto para o exercício de *Softpower* (a dimensão da cooptação) quanto de *Hardpower* (a dimensão da coerção) dentro do próprio domínio cibernético. Desde práticas de espionagem e ataques guiados a servidores governamentais até campanhas de diplomacia e

mobilização política, são inúmeras as possibilidades para a geração de impacto do poder cibernético, tanto dentro da própria rede quanto na infraestrutura na qual se apoia.

Neste contexto, o poder cibernético se apresenta sob três faces. A primeira delas, diz respeito à "capacidade de um ator para fazer outros realizarem algo contrário às suas preferências ou estratégias iniciais" (NYE, 2012). Neste primeiro aspecto, o *Hardpower* pode ser exercido, por exemplo, por meio de ataques a servidores, inserção de *malwares*, prisões de bloggers "oposicionistas", etc. O *Softpower*, por sua vez, pode ser exercido quando um ator tenta persuadir terceiros a mudar seu comportamento. Vídeos e páginas com o objetivo de divulgar uma mensagem específica e atrair indivíduos e grupos para uma determinada causa, como a revista eletrônica *Inspire* – no caso, dos grupos ligados a Al-Qaeda - ou da propaganda do governo russo durante os ataques à Geórgia em 2008, destinada aos hackers; são bons exemplos dessa prática.

A segunda face do poder é quando se faz uma reestruturação da agenda, onde um ator impossibilita as escolhas de outro(s), por meio da exclusão de suas estratégias (NYE, 2012). Se este ajuste da agenda for contra a sua vontade – por exemplo, através de firewalls, filtros ou pressão sobre companhias para que estas excluam algumas ideias -, caracteriza-se como exercício de *Hardpower*. Porém, se for aceito como legítimo, como o incentivo à criação de regras comumente aceitas, caracteriza-se como exercício de *Softpower*.

E, por fim, a terceira face do poder caracteriza-se pelo envolvimento de um ator ao moldar as preferências iniciais de outro para que determinadas estratégias não sejam sequer consideradas. Segundo Nye (2012), as ameaças de punição para bloggers que disseminam material censurado ou o desenvolvimento de normas de repulsa à determinada temática – como a questão da pornografia infantil – são exemplos de exercício de *Hardpower* e *Softpower*, respectivamente.

É importante ressaltar que o domínio cibernético é um campo que difere de qualquer outra esfera de domínio tradicional – terra, mar, ar e espaço - pois apresenta baixas barreiras de entrada, o que torna mais fácil a difusão do seu poder, permitindo com facilidade a atuação tanto de atores estatais como de atores não-estatais. Consequentemente, os conflitos no domínio cibernético também se dão de maneira muito diferente dos conflitos no mundo físico. Nye (2012) explica que, enquanto no mundo real o monopólio do uso da força em larga escala é praticamente exclusividade dos governos, os recursos quanto à mobilidade são dispendiosos e os ataques terminam devido ao desgaste ou à exaustão, no universo virtual, os atores são variados - muitas vezes anônimos -, a distância física é praticamente inexistente, e os custos de um ataque virtual, mínimos. Isso dificulta consideravelmente a elaboração de mecanismos de defesa, visto que no domínio cibernético é muito mais difícil identificar a fonte do ataque e qualquer atribuição equivocada poderá trazer graves consequências para as relações exteriores de um Estado.

A fórmula para uma política externa eficiente, seja no campo da cibernética, seja em qualquer outro domínio, não se encontra na adoção exclusiva de métodos de coerção ou cooptação, de uma escolha entre *hardpower* e *softpower*, mas sim de um manuseio estratégico de ambos, adaptado para a realidade e as necessidades particulares de cada Estado (NYE, 2012). A esse manuseio Nye (2012) chama de *Smartpower,* isto é, poder inteligente.

Ainda dentro da discussão sobre política internacional e cibernética, o sociólogo espanhol Manuel Castells (2003) retoma os conceitos de *noosfera* e *noopolitk* formulados por Arquilla e Rondfeldt ainda no início dos anos 2000 e os aponta como uma tendência crescente dentro do cenário das Relações Internacionais. Por *noosfera*, define-se o ambiente de informação global dada a sua configuração atual, ou seja, abrange tanto o ciberespaço quanto as demais mídias (estando ou não diluídos dentro das redes). *Noopolitik*, portanto, seria a todo tipo de medida que visa a promoção de interesses através da *noosfera*. (ARQUILLA & RONDFELDT, 1999)

Longe de se contrapor ao conceito clássico de *realpolitik* ou de negar a sua aplicabilidade no novo contexto internacional, Castells (2003) defende a *noopolitik* como um complemento à prática da política internacional tradicional. Nesse sentido, ele - juntamente com Arquilla e Rondfeldt - dialoga tanto com Morgenthau quanto com Nye. Castells (2003) por um lado trata a cibernética como um novo recurso de poder em moldes muito parecidos com o do realismo moderno, isto é, como um conceito que varia tanto de acordo como o período histórico como à capacidade dos atores

de utilizá-lo. Por outro lado, também trata o poder como um fenômeno comportamental, produto não somente da coerção por meios materiais, como também da cooptação, sendo esse último fortemente influenciado pelos fluxos de informação.

Num mundo caracterizado por interdependência global e moldado pela informação e a comunicação, a capacidade de atuar nos fluxos de informação, e sobre mensagens da mídia, torna-se uma ferramenta essencial para a promoção de um programa político. (CASTELLS, 2003. p132).

BRASIL E ESTADOS UNIDOS: ASSIMETRIAS VIRTUAIS

Dentro da atual conjuntura do Sistema Internacional, onde os fluxos de informação e a cibernética apresentam vital importância tanto no cotidiano das grandes cidades quanto em setores estratégicos da gestão política dos Estados, seria anacrônico pensar em um conceito de política externa ou de segurança nacional que não estivesse integrado a todo esse contexto.

Os fluxos de capital nas bolsas de valores, a possibilidade de ataques cibernéticos aos servidores governamentais, o roubo de propriedade intelectual através da rede, bem como a ameaça de espionagem internacional virtual, tornaram-se nos últimos anos algumas das principais preocupações dos governantes e *policy makers* das principais potências mundiais.

Nesse sentido, os Estados Unidos despontam como uma das principais autoridades no assunto, devido às exigências para a manutenção de sua condição de potência hegemônica dentro do novo contexto das Relações Internacionais, marcado pela emergência de redes e fluxos de informação paralelos ao controle do Estado e de novos atores internacionais (NYE, 2012).

Com um gasto de cerca de U$ 620,3 bilhões (ESTADOS UNIDOS DA AMÉRICA, 2012) em defesa em 2012, os Estados Unidos podem ser apontados como um dos principais exemplos de investimento nesse campo na atualidade. Juntamente com todo o complexo industrial-militar que o garante como sendo a maior potência militar do planeta, há também um grande sistema de agências de inteligência encarregado da logística e planejamento, responsável tanto pela defesa dos interesses norte-americanos no estrangeiro quanto pela segurança interna, em gastos que somam U$ 87,2 bilhões (ESTADOS UNIDOS DA AMÉRICA, 2012). Curiosamente, esses dados mais recentes figuram já como parte do quadro de corte de gastos levado a cabo pela administração Obama, em face do elevado endividamento estatal causado pelos gastos com as guerras do Iraque e Afeganistão – heranças da gestão anterior – e agravado pela crise econômica de 2008. Entretanto, se por um lado os gastos com o aparato militar tradicional entraram em uma relativa diminuição, os investimentos nos serviços de inteligência e defesa cibernética ganharam significativo destaque na agenda norte-americana.

Segundo o *International Strategy for Cyberspace – Prosperity, Security and Openness in a Networked World,* divulgado pela Casa Branca em 2011, os Estados Unidos pareceram assentar as bases para uma nova abordagem sobre o ciberespaço e poder cibernético. Conforme defenderam Nye (2012) e Castells (2003), a política norte-americana para esse domínio tomou contornos menos impositivos e mais próximos a um ideal cooperativo, buscando promover o que é descrito no relatório como uma infraestrutura de informação e comunicação aberta, segura e confiável para sustentar os fluxos do comércio internacional, fortalecer a segurança internacional e assegurar a liberdade de expressão e informação (ESTADOS UNIDOS DA AMÉRICA, 2011). Para tanto, a política cibernética norte-americana se pauta, em virtude da impossibilidade de controlar efetivamente todos os nós de informação da rede (CASTELLS, 2003), em ações de governança que buscam favorecer normas de condutas positivas entre os Estados e delegar responsabilidades entre os mesmos, juntamente com medidas de coerção a grupos criminosos e outros agentes não estatais.

Para tanto, foi formulada uma estratégia pautada em três eixos: Diplomacia, Defesa e Desenvolvimento. O primeiro eixo objetiva a cooptação de outros países à causa norte-americana de maneira a estreitar relações com os mesmos e criar uma coincidência de interesses que motive esses últimos a assumir parte do ônus da tarefa de monitorar a rede. O segundo ponto entra um pouco mais no âmbito da coerção, na medida em que investe em estratégias de dissuasão (fortalecendo a resiliência das redes domésticas norte-americanas e de outros países) e contenção (na medida em que encorajaria a ação de autoridades locais no combate aos cibercrimes e acordos

internacionais para investigação dos mesmos). O terceiro e último eixo, o de desenvolvimento, busca fortalecer a capacidade da própria rede em se defender de ataques, difundindo para tanto a tecnologia necessária por meio de acordos de comprometimento mútuos. A essa combinação de medidas coercitivas e cooptativas – *Hardpower* e *Softpower* – adaptada às condições e necessidades particulares de cada país Joseph Nye dá o nome de *Smartpower* (Poder Inteligente).

No caso brasileiro, a cibernética só passou a ser uma das prioridades nos planos de ação estratégica de defesa a partir de 2008 com o decreto n° 6.703:

O mencionado dispositivo legal também estabelece que as capacitações cibernéticas incluirão, como parte prioritária, as tecnologias de comunicações entre todos os contingentes das forças armadas, de modo a assegurar sua capacidade de atuar em rede. [...] Todas as instâncias do Estado deverão contribuir para o incremento da segurança nacional, com particular ênfase nos seguintes aspectos do setor cibernético: as medidas para a segurança das áreas de infraestruturas críticas*; e o aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à defesa nacional contra ataques cibernéticos e, se for o caso, que permitam seu pronto reestabelecimento. (CARVALHO, 2011. p).

Para cumprir o que foi colocado na Estratégia Nacional de Defesa quanto ao desenvolvimento da defesa cibernética nacional, o Plano Plurianual de 2012 a 2015 estipula que haverá financiamento da implementação de 40% do projeto para este período. Em 2012 anunciou-se a dotação de R$ 111 milhões para o orçamento anual do projeto, dos quais apenas R$ 34 milhões foram efetivamente pagos.

Mesmo considerando que este é um tema recente para a agenda governamental nacional e as diferentes perspectivas que cada país faz para a projeção de seu próprio poder no Sistema Internacional, é patente a diferença entre os programas brasileiro e norte-americano, tanto em termos de objetivos quanto de orçamentos. Essa relativa pouca atenção que os novos setores-chave dentro da atual lógica do poder no Sistema Internacional recebem, nas últimas gestões se devem não somente à possíveis esquemas ilícitos, mas também pela necessidade por parte do governo de priorizar determinadas áreas-chave da infraestrutura nacional interna em relação a projetos do âmbito da política externa.

Sendo um país que essencialmente inaugurou a ideia de empregar redes fechadas de computadores juntamente com o aparato militar tradicional, os Estados Unidos se provaram um campo extremamente prolífico para o surgimento de inovações na aplicação da cibernética como ferramenta de política externa. Juntamente com programas de monitoramente do fluxo de dados e outras inovações no campo da espionagem, bem como *firewalls* e sistemas de criptografia de dados, os cientistas norte-americanos têm trabalhado continuamente em tecnologias baseadas na utilização da cibernética como ferramenta para gerar resultados fora do domínio cibernético. Aeronaves não tripuladas, sistemas de localização por satélite e a recente tática do *swarming* (enxameamento) figuram entre as mais recentes aplicações encontradas.

Essa última, aliás, pode potencialmente revolucionar a forma como a guerra convencional é estruturada, visto que adiciona tecnologia de comunicação em tempo real entre tropas independentes e altamente equipadas à antiga lógica das guerras de guerrilha. Ao invés de haver um grande contingente militar dividido em especialidades como infantaria, comunicações, engenharia, etc, haveria pequenas divisões de soldados altamente treinados e capazes de operar cooperativamente em qualquer função necessária (CASTELLS, 2003).

Conforme afirma Castells (2003) é efetivamente impossível para qualquer Estado, mesmo uma potência mundial, oferecer total proteção à sua rede doméstica contra ataques, pois na mesma medida em que um país necessita da cibernética para funcionar plenamente, mais vulnerável também estará a ataques que fazem uso da mesma. Entretanto, os nós-chave das redes de cada país, que regulam os sistemas de defesa e a infraestrutura básica (água, luz e comunicação) contam claramente com defesas mais robustas No âmbito da segurança virtual interna, o governo norte-americano tem conseguido com sucesso garantir a proteção de setores prioritários de sua rede doméstica, e mesmo quando alguns destes se veem sob ataque, se mostra capaz de lhe garantir uma resposta imediata e inteligente e uma recuperação já em curto prazo.

Já no caso do Brasil, percebe-se, ao analisar em retrospecto os últimos episódios de invasão de sistemas governamentais, a herança negativa que a falta de investimentos no campo cibernético deixou. O episódio de espionagem da Petrobrás e de conversas particulares da presidente Dilma Rouseff neste ano, juntamente com casos mais esparsos de ataques de negação de serviços em 2011 ilustram de maneira bastante clara a deficiência tecnológica brasileira na questão da segurança virtual interna.

PERSPECTIVAS PARA O BRASIL

Como já foi discutido anteriormente, os impactos que as tecnologias de informação e comunicação tem no cotidiano e na dinâmica de relações entre os Estados e demais agentes, simplesmente não podem minimizados. A inclusão da defesa cibernética na agenda de projetos de interesse nacional é um passo inicial promissor – ainda que tímido – rumo a uma política virtual condizente com o atual momento histórico.

Para alcançar as metas de política externa pretendidas pelo governo (notadamente a reforma do Conselho de Segurança das Nações Unidas) e reforçar sua posição enquanto potência regional, um arranjo de *Smartpower* que combine uma política diplomática forte, juntamente com medidas e demonstrações de poder coercitivo, é fundamental. Um sistema de defesa cibernética capaz de proteger os pontos-chave da infraestrutura crítica nacional e assegurar a resiliência da mesma diante de ataques é um ponto crucial, conforme estabelece o documento de Estratégia Nacional de Defesa. Muito embora a entrada no domínio cibernética possua custos muito inferiores se comparada em relação a outros setores como o aeroespecial e o nuclear, ainda assim necessita de uma infraestrutura física considerável, levando em conta servidores, satélites, cabos de fibra ótica e demais recursos físicos imprescindíveis à construção de uma rede doméstica abrangente e eficiente.

A segurança virtual interna passa necessariamente pelo desenvolvimento de s*oftwares* e códigos nacionais de criptografia, o que implica em um investimento maior em projetos de pesquisa e capacitação de recursos humanos. O domínio e controle de um código-fonte totalmente nacional iriam contribuir consideravelmente para o aumento da dificuldade de tentativas de apreensão de informações de interesse nacional por parte de agentes externos, tanto governos como grupos de indivíduos.

Se por um lado no campo da defesa virtual as perspectivas para o Brasil se encontram mais fortemente aliadas ao aspecto da coerção, por outro, o campo da política externa apresenta uma maior diversidade de aplicações para o poder cibernético. Graças ao poder descentralizador das tecnologias de comunicação, a voz de qualquer país pode ser ouvida internacionalmente (ainda que em intensidades diferentes). Dito isso, as possibilidades para o uso da cibernética como um prolongamento da política externa brasileira são bastante promissoras.

Uma *Noopolitk* efetivamente nacional poderia utilizar a rede como forma de impulsionar o *Softpower* nacional ao ampliar o raio de divulgação e a qualidade da imagem vinculada ao Brasil no exterior. Programas de divulgação cultural, propostas de intercâmbio universitário e profissional, e divulgação de realizações técnico-científicas nacionais são apenas alguns exemplos de aspectos que poderiam ter sua divulgação ampliada exponencialmente por um uso mais estratégico das redes de informação. A ideia aqui, conforme afirmavam Castells (2003), Arquilla e Rondfeldt (1999), é transcender o limite da propaganda nacional pura e simples, uma vez que não objetiva apenas a interação entre governos, mas principalmente com as diferentes sociedades, influenciando na formação da opinião pública internacional. Somadas à diplomacia tradicional, as estratégias da *Noopolitik* contribuiriam para construir à longo prazo uma imagem que seja capaz de facilitar a cooptação de outros países dentro do Sistema Internacional.

Nesse sentido, as campanhas culturais destinadas a outros países como o "Ano do Brasil na França", realizado em 2012, são um excelente começo, visto que a aproximação cultural pode, a longo prazo, resultar na ampliação das oportunidades de aliança com outros países tanto no campo comercial como o diplomático, algo particularmente interessante para o potencial nacional de conseguir um lugar junto ao Conselho de Segurança das Nações Unidas.

CONSIDERAÇÕES FINAIS

O domínio da cibernética se desenvolveu exponencialmente e ampliou seu alcance e influência em uma escala considerável no últimos anos, indo de um conjunto de redes fechadas para uma intrincada trama onde circulam informações e dados a uma velocidade nunca antes vista.

Dentro da nova dinâmica de relações sociais, produtivas e políticas gerada pela nova Era da Informação, diversos atores não-estatais despontam dentro do Sistema Internacional: grandes corporações, grupos terroristas e mesmo indivíduos podem, ao explorar as possibilidades e vantagens oferecidas pela cibernética (e também suas vulnerabilidades), provocar resultados tanto dentro como fora das redes.

Dentro desse novo contexto, onde a internet e a cibernética surgem como um novo recurso de poder no Sistema Internacional do qual os Estados – tanto as grandes potências como os menores – devem se valer a fim de proteger e alcançar as metas de seus respectivos interesses nacionais. Desde medidas enérgicas como ataques de negação de serviço, envio de *malwares* com fins de sabotar sistemas-chave ou o roubo de dados vitais até estratégias mais coercitivas como programas de diplomacia virtual, divulgação de ideias pela rede, a cibernética fornece um amplo leque de opções estratégicas para o exercício tanto do *Soft Power* quanto do *Hard Power*.

Se por um lado os avanços do Brasil no setor cibernético parecem relativamente poucos em relação à política norte-americana para o ciberespaço, é importante ter em mente não somente a diferença de recursos de que cada país dispõem – não somente infraestrutura de comunicação e logística, mas também na questão da capacitação dos recursos humanos empregados -, como também os objetivos traçados por cada um e as abordagens pelos quais estes são buscados. Mesmo sendo a principal economia do planeta e destinando orçamentos bilionários para os setores de segurança e inteligência, mesmo os Estados Unidos se provam incapazes de controlar efetivamente todo o domínio cibernético, optando por uma estratégia mais realista de compartilhamento de responsabilidades na rede como forma de manter sua hegemonia.

Quanto ao projeto cibernético brasileiro, recomenda-se uma estratégia de *Smart Power* condizente tanto com as aspirações da política externa nacional, quanto com a cojuntura interna. Além de reforçar as defesas de pontos críticos das redes domésticas com investimentos em pesquisas de desenvolvimento de tecnologias – especialmente *softwares* e sistemas de criptografia – e ampliar o alcance e o poder de cooptação gerados pela atração do *Soft Power* nacional, por meio de uma *noopolitik* bem formulada, é crucial para o país superar os gargalos em sua infraestrutura de comunicação, bem como buscar diversificar e fortalecer quaisquer parcerias internacionais úteis para seus objetivos, tendo sempre em mente a consolidação de sua posição como potência-chave na dinâmica regional e internacional.

REFERÊNCIAS BIBLIOGRÁFICAS

ARQUILLA, John. RONDFELDT, David. **The Emergence of Noopolitik toward an American Information Strategy**. Santa Monica: 1999

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional**. Disponível em: <http://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf>. Acesso em 20. Ago. 2013

_____. Ministério da Defesa. **Estratégia Nacional de Defesa**. Disponível em: <http://www.defesa.gov.br/projetosweb/estrategia/arquivos/estrategia_defesa_nacional_portugues.pdf>. Acesso em 21. Set. 2013.

CARVALHO, Paulo. O Setor Cibernético nas Forças Armadas Brasileiras. In: BRASIL. Secretaria de Assuntos Estratégicos da Presidência da República. **Desafios Estratégicos para a Segurança e Defesa Cibernética**. Brasília: 2011. Disponível em: < http://www.sae.gov.br/site/wp-content/uploads/Seguranca_Cibernetica_web.pdf> Acesso em: 16. Set. 2013

CASTELLS, Manuel. **A Galáxia da Internet**: Reflexões sobre a Internet os negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

CASTRO, Thales. **Teorias das Relações Internacionais**. Brasília: Fundação Alexandre de Gusmão (FUNAG), 2012.

ESTADOS UNIDOS DA AMÉRICA. Office of Management and Budget. **Department of Defense - The Budget for Fiscal Year 2014**. Disponível em: <http://www.whitehouse.gov/sites/default/files/omb/budget/fy2014/assets/defense.pdf>. Acesso em: 21. Ago. 2013.

_____. White House. **International Strategy for Cyberspace** – Prosperity, Security and Openness in a

Networked World. Disponível em: < http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>. Acesso em 7. Set. 2013.

MENEZES, Dyelle. Ação para defesa cibernética recebeu apenas 31% do previsto ano passado. 15. Jul. 2013. **Contas abertas**. Disponível em: < http://www.contasabertas.com.br/website/arquivos/530 >. Acesso em: 07. Set. 2013.

MESSARI, Nizar; NOGUEIRA, João Pontes**. Teoria das Relações Internacionais** – Correntes e Debates. Rio de Janeiro: Elsevier, 2005.

MORGENTHAU, Hans J. **A Política entre as nações**: A luta pelo poder e pela paz. Editora Universidade de Brasília – IPRI, 2003.

NYE JR, Joseph S. **O Futuro do Poder**. São Paulo: Benvirá, 2012.

PARRY, Roger. **A Ascensão da Mídia:** A história dos meios de comunicação de Gilgamesh ao Google. Rio de Janeiro: Elsevier, 2012. p. 330-346.