Bruno M. Nathansohn:

Uma análise sobre a política de informação para a defesa militar do Brasil: algumas implicações éticas

Abstract:

An analysis about the information policy for the military defence of Brazil

Some ethical implications: It is presented the development of the information policy for the military defense of Brazil, taking into consideration information actions, which were implemented during the Brazilian history, and in the context of the regions where the country carries out geostrategic influence. The hypothesis is that there is a dilemma of the Brazilian state between cooperative international relations, based on a multilateral perspective, and the threats to its critical information infrastructure. Besides, technically there is a fragility of the cybernetics infrastructure because of the lack of an appropriate information policy, which could contribute to the position of Brazil in the international system of power, in accordance with its potentialities. Questions that imply ethics dilemmas about the threshold between the cooperative interchange, on the one hand, and the preservation of sovereignty, on the other, related with what should, or should not, be shared in the cyberspace.

Agenda:

Author(s):

MSc. Bruno Macedo Nathansohn:

- Pesquisador da Rede Latino-Americana de Geopolítica e Estratégia (RELAGE), Rua Xavier da Silveira, 22/Apto.601 – Copacabana – Rio de Janeiro/RJ CEP: 22061-010
- Tel.: +55 (21) 3204-1461; Cel.: +55 (21) 8228-7208; e-mail: bnathansohn@gmail.com; http://nathansohn.blogspot.com (Arquivo de Ideias)
- Relevant publications:
  - Estudo de usuários on line. Revista Digital de Biblioteconomia e Ciência da Informação. Unicamp. v.3, n.1 (2005). Bruno Macedo Nathansohn, Isa Maria Freire. p.39-59. Disponível em: http://www.sbu.unicamp.br/seer/ojs/index.php/rbci/article/view/324
  - Um estudo sobre o processo de tomada de decisão política para a ação de inteligência: a possibilidade de gestão da informação arquivística. Perspectivas em Gestão & Conhecimento, João Pessoa, v. 3, n. 2, jul./dez. 2013. Bruno Nathansohn. p. 280-299. Disponível em: http://periodicos.ufpb.br/ojs2/index.php/pgc. ISSN: 2236-417X.

© by IRIE – all rights reserved

ISSN 1614-1687

Introdução

O governo brasileiro vem intensificando o desenvolvimento de ações para seu programa de defesa militar cibernética, o que está registrado na Estratégia Nacional de Defesa (END). Entretanto, o próprio Ministro da Defesa reconheceu, recentemente, que o Brasil não está preparado para se defender militarmente de um ataque à sua infraestrutura crítica de informação. Apesar da iminência de uma ciberguerra ser remota para o Brasil, existem indícios históricos de que atores estatais e não-estatais visem as riquezas proporcionadas pelo território brasileiro, o que inclui o monitoramento político do País. Vide as recentes operações de espionagem estadunidense contra o Brasil, os crimes de biopirataria na Amazônia por agentes de diversos países, a reativação da 4ª Frota estadunidense no Oceano Atlântico e as atividades do crime organizado nas fronteiras terrestre e marítima, o País busca desenvolver sua infraestrutura cibernética para o fortalecimento de seus laços políticos em fóruns como os do Mercosul e o da União Sul-Americana (Unasul). Torna-se primordial, nesse sentido, que haja primeiramente a construção de marcos institucionais que orientem a produção e os usos das Tecnologias de Informação e da Comunicação (TIC) para a defesa dos países considerados periféricos no sistema internacional. Essa perspectiva tornar-se-ia viável se a estratégia de defesa fosse orientada por princípios cooperativos, regidos por uma eficiente política de informação.

"A TI é usada para gerenciar as forças militares – por exemplo, para o comando e o controle e para a logística. Além disso, as munições guiadas com precisão ilustram como o uso de TI, integrada aos sistemas de armas, aumenta sua letalidade e reduz o dano colateral associado com o uso de tais armas. Movimentos e ações de forças militares podem ser coordenados através de redes que permitem obter informação e imagens por quadro do campo de batalha para serem amplamente compartilhados"[1]. (**Tradução nossa**: LIN, 2012)

Nos últimos tempos, o Brasil vem se notabilizando pela busca de relações internacionais multilaterais que valorizem acordos político-institucionais, e não restritos à competitividade mercadológica. A valorização dessa perspectiva pode indicar uma tendência contra-hegemônica nas relações internacionais pela centralidade das relações Sul-Sul, em detrimento de relações marcadas pela desigual Norte-Sul. A política externa brasileira orienta-se, em certa medida, por trocas mais equânimes entre atores que compartilham experiências históricas e condições sociais, políticas e econômicas semelhantes. Nesse sentido, ao contemplar relações simétricas, sob a lógica cooperativa, tende-se a relativizar a compreensão dos usos da técnica em relação à política. Isso não significa que o Brasil e os Estados que questionam o sistema hegemônico não se utilizem da técnica para alcançar seus objetivos de poder, muito pelo contrário. Entretanto, ao apresentar canais para a cooperação, tende-se a diluir o discurso e as práticas assimétricas entre os atores políticos, propiciando outras possibilidades de relacionamento para a diminuição das desigualdades interestatais e a resolução de conflitos.

Isso não que dizer também que a cooperação só seja possível e realizável entre atores que apresentem posições simétricas no cenário internacional, muito pelo contrário. A cooperação também pode ocorrer entre atores estatais e não-estatais, situados em condições absolutamente díspares. Todavia, o que consolidará relações mais ou menos sólidas entre os atores será a natureza das necessidades que compartilham e o nível de estabilidade política entre eles. Assim, o desenvolvimento de uma política de informação para a concretização de ações de informação dependerá da capacidade tecnológica dos atores em desenvolver e utilizar recursos de informação. O posicionamento do Estado, e da lógica de sua política de informação, no contexto internacional, será definido por meio dos usos dos recursos de informação e da aplicação dos mesmos de acordo com suas necessidades de poder. O que, de uma forma, ou de outra, tende à construção de uma agenda multilateral para solucionar questões de ordem prática.

Como destacado pela United Nations Institute for Disarmament Research (UNIDIR), apesar de se tratar de cibersegurança e não de ciberguerra,"(...) os elementos de cibersegurança internacional – cooperação na construção da segurança doméstica, a expansão de capacidades militares, e aplicação da lei – apresenta uma

[1] "Military forces are no exception. IT is used to manage military forces – for example, for command and control and for logistics. In addition, modern precision- guided munitions illustrate how the use of IT embedded in weapons systems increases their lethality and reduces the collateral damage associated with the use of such weapons. Movements and actions of military forces can be coordinated through networks that allow information and common pictures of the battlefield to be shared widely". (LIN, 2012, p.516)

agenda robusta para o trabalho multilateral"[2]. Nesse sentido, a própria noção de defesa (e segurança) ganha novos contornos. O princípio da defesa reconquista uma projeção que foi, de certa forma, relegada a partir do período pós-Guerra Fria, orientando-se sob novos princípios, principalmente a partir dos atentados de 11 de setembro de 2001, nos Estados Unidos (EUA). Desses eventos resultou o Ato Patriótico, no governo de George W. Bush, como um conjunto de normas para o enfrentamento de qualquer ameaça sentida, ou percebida, contra a segurança nacional norteamericana. Os EUA, como única potência global, passaram a investir em novos armamentos e em ações de informação relacionados à vigilância, à espionagem, e para suprimir protestos internamente. Não existindo, por parte dos recentes governos, qualquer preocupação em discernir a defesa militar, portanto contra inimigos de fato, de atividades de monitoramento e controle que atingem direitos de privacidade de indivíduos, dentro e fora do território estadunidense. Tendência que foi acompanhada por vários países, potencializando o uso do ciberespaço como recurso de infraestrutura em todas as agências governamentais para a troca de correspondências, para o planejamento estatal, para a gestão de documentos e de sistemas operacionais. E por ser um recurso de infraestrutura, a informação é utilizada como um recurso de poder sistematizado, capaz de fornecer o comando e o controle sobre todas as etapas de processos decisórios num contexto complexo formado por diversos atores estatais e não estatais. Essa perspectiva, principalmente num país como o Brasil, que se caracterizaria como periférico emergente, apresenta algumas implicações éticas justamente pela necessidade imperial de se fazer valer uma política de informação que oriente o investimento técnico-científico para a defesa militar. Portanto, quando se trata de planejamento estratégico, devem-se valorizar os aspectos políticos que dão sentido a esse planejamento e trazem em seu bojo questões sociais e humanas.

A sistematização da informação como recurso de poder para a defesa

Apesar do monitoramento e do controle de cidadãos e grupos políticos, por parte do aparato estatal, não ser algo novo, o arcabouço legal estatuído no Ato Patriótico norteamericano consagra a perspectiva das ameaças difusas, mesmo que imaginárias, além de contemplar recursos de informação[3] para o enfrentamento das mesmas de forma preemptiva. Ou seja, ao menor sinal de perigo, segundo a avaliação da burocracia estatal, deve-se atuar para aniquilação, mais do que para a contenção de potenciais inimigos. Pode-se dizer que essa tendência implica no uso indiscriminado dos recursos de informação como instrumento de controle, e em um processo decisório baseado na supremacia da técnica, numa lógica que valoriza o comando e a obedência em detrimento da Política[4] que, segundo Arendt (2002, p.21), "se baseia na pluralidade dos homens".

O que não quer dizer que não haja propriamente uma definição política (no sentido do desenvolvimento de políticas públicas) de informação voltada para o alcance daqueles objetivos. Pois, mesmo a falta de planejamento é uma opção política. No entanto, o que existe é um estreitamento do espaço para a troca e o debate sobre a lógica, o sentido e os impactos que determinadas decisões impõem sobre a vida social, constituindo-se como uma das questões éticas fundamentais. Implica, portanto, em questões éticas fundamentais no que tange à forma de se fazer política, pois naturaliza as questões sociais e humanas, e os usos de técnicas para o controle do corpo e do espaço sem o consentimento da sociedade. Dentre as questões éticas que precisariam ser levadas em consideração, destacam-se: i) a defesa como recurso usado prioritariamente para a manutenção da paz entre Estados; ii) o uso dos recursos de informação para o monitoramento serem usados exclusivamente para conter comprovadas ameaças externas à sociedade e ao Estado brasileiro; e, iii) utilização de recursos de informação dentro de um modelo cooperativo, preferencialmente para a cobertura de necessidades de defesa de setores críticos entre Estados menos desenvolvidos econômica e tecnologicamente.

[2] "The elements of international cybersecurity—cooperation in building domestic security, the expansion of military capabilities, and law enforcement—present a robust agenda for multilateral work". (UNIDIR 2013, p.4).

[3] Segundo a definição do site do Ministério do Planejamento, Orçamento e Gestão, do governo brasileiro, "Recursos de informação: são tanto os acervos de informações quanto os conjuntos ordenados de procedimentos automatizados de coleta, tratamento e recuperação destas informações". Disponível em: http://www.governoeletronico.gov.br/sisp-conteudo. Acesso em: 02 de agosto de 2013.

[4] Política (com "P" maiúsculo), no sentido conferido por Hannah Arendt, que significa a troca de ideias e experiências entre diferentes, baseada na "pluralidade dos homens".

Muitas das iniciativas para a resolução de questões sociais e humanas, ou mesmo econômicas, vem sendo implementadas sob a égide de uma lógica calcada na precisão técnica. Como se constata, ao destacar que o objetivo fundamental da nação é a busca da segurança, efetiva-se uma série de ações pautadas pela burocracia militar. Nesse sentido, processos de tomada de decisão que deveriam passar por processos formais democráticos, contando com a participação popular, de acordo com o princípio da pluralidade, de Arendt (2002), são realizados através de decisões de cúpula, como na guerra ao terror, com as invasões do Afeganistão, em 2001 e do Iraque, em 2003, e as investidas estadunidenses na guerra contra o narcotráfico em território sul-americano, como no caso do Plano Colômbia e das construções de bases militares no Peru e no Paraguai.

No contexto brasileiro, essa tendência de uso de recursos de informação como recursos informáticos para o monitoramento e o controle também é uma realidade, tanto no âmbito nacional quanto no internacional. Todavia, sucessivos governos, principalmente em períodos ditatoriais utilizaram-se daqueles recursos para a segurança interna, mais do que para a dissuasão de potenciais inimigos externos. O que se justificou por dois motivos: o primeiro, pelo Brasil se enquadrar como um país periférico no sistema de poder internacional, não apurando a percepção para importantes ameaças externas, também por causa de governos subjugados aos poderes hegemônicos internacionais; e segundo, por causa da percepção que aqueles governos nutriam pelas ameaças de grupos internos que contestavam os regimes políticos vigentes.

O golpe militar de 1964 foi marcante nesse sentido, impulsionado pela criação do Serviço Nacional de Informação (SNI), que teve como objetivo supervisionar e coordenar as atividades de informações e contrainformações no Brasil e no exterior. O SNI foi substituído, em 1999, pela Agência Brasileira de Inteligência (Abin), com menos força e um papel aparentemente secundário no sistema de defesa nacional. Atualmente, mesmo com o Brasil ganhando maior vulto no cenário político internacional, inclusive como referência no uso das Tecnologias da Informação e da Comunicação (TIC) nas mais diferentes áreas, a tecnologia de monitoramento e controle na área de defesa ainda se apresenta em estágio embrionário e de forma descoordenada.

Entretanto, pode-se dizer que ainda existe espaço para a realização de uma alternativa política que leve em consideração a troca cooperativa e, com isso, a possibilidade de mitigar o "rolo compressor" da lógica técnico-científica imposta pelos países centrais. Nesse sentido, em uma perspectiva que objetiva a proteção da infraestrutura crítica e das riquezas naturais brasileiras (minerais raros, pré-sal etc.), existentes nas plataformas terrestre e marítima atlântica, vislumbra-se fortalecer a defesa militar para tal fim. Considerando essa nova perspectiva, destaca-se, na Estratégia Nacional de Defesa (END)[5] brasileira, o setor cibernético[6] como área na qual devem ser empreendidos esforços para o enfrentamento de ameaças com características difusas, com origem indefinida[7]. Ou seja, dentre outras coisas, explora-se um novo cenário propiciado pelas TIC, considerando estratégias e táticas operadas no ciberespaço, sem se descuidar das relações políticas a serem desenvolvidas de forma multilateral. Nesse sentido, ao integrar sistemas de informação da administração pública, rearranjando a máquina estatal e promovendo a governança eletrônica, a ameaça ao monopólio do uso da força pelo Estado transmuta-se para o ciberespaço, impondo novos desafios à sua prerrogativa como garantidor da soberania nacional.

As TIC, por suas próprias características, contribuem decisivamente para o planejamento da política de informação, e potencializam as ameaças, colocando a ciberguerra como uma possibilidade. O ciberespaço reposiciona atores estatais e não estatais em torno de objetivos que transcendem o espaço nacional, afetando decisivamente a concepção de soberania e, consequentemente, as questões éticas subjacentes às possíveis

[5]Aprovada pelo Decreto no 6.703, de 18 de dezembro de 2008

[6] De acordo com o conceito estabelecido na END: "Cibernética – Termo que se refere ao uso de redes de computadores e de comunicações e sua interação dentro de sistemas utilizados por instituições públicas e privadas, de cunho estratégico, a exemplo do MD/FA. No campo da Defesa Nacional, inclui os recursos informatizados que compõem o Sistema Militar de Comando e Controle (SISMC), bem como os sistemas de armas e de vigilância". (CARVALHO, 2011, p. 17).

[7] De acordo com o conceito estabelecido na END: "Defesa Cibernética – Conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente. No contexto do preparo e emprego operacional, tais ações caracterizam a Guerra Cibernética". (CARVALHO, 2011, p.18).

relações estabelecidas em torno da política de informação. Assim, princípios éticos são colocados em questionamento pelo sobrepujamento da técnica sobre a Política, e pelas formas de uso abusivo dos recursos cibernéticos.

Se por um lado, torna-se necessária a cooperação para a resolução de problemas de ordem prática, referentes à ciberguerra, por outro lado, o País precisa manter-se precavido em relação aos atores hegemônicos que, por apresentarem superioridade tecnológica, tendem ao domínio das ações ofensivas de informação em relação aos atores tecnologicamente mais fracos. Portanto, o grande desafio do Brasil é colocar em prática uma estratégia de defesa sob um novo paradigma, que una ao mesmo tempo, o empoderamento dos recursos de informação já desenvolvidos, através do planejamento científico-tecnológico soberano, com a articulação de políticas de cooperação com outros países que tenham a mesma necessidade de defesa do Brasil, limitando ao máximo o acesso de informações estratégicas.

A emergência de sistemas de informação como elemento de comando e controle social teve lugar quando de sua percepção como algo sistematizável, manipulável e mensurável pelo Estado. Ciências de Estado, como a Estatística (Estadística em espanhol), desenvolvem-se sob os auspícios da administração pública, contribuindo para a consolidação de uma tecno-burocracia. Portanto, longe de ser efeito de processo técnico, como resultado de ações passivas e desinteressadas, o desenvolvimento técnico-científico é um processo ideológico, carregado de significado político e social. Estabelece-se, por assim dizer, por meio de regras e normas sob objetivos inerentes à razão de Estado. Um exemplo prático seria o investimento na fabricação de *drones*, seja para o monitoramento e o controle, seja para o ataque efetivo aos potenciais inimigos. Ao optar por ações de ataque e defesa por meio de *drones*, a burocracia responsável pela área de Defesa faz uma opção política pela utilização de uma tecnologia que substitua outros artefatos militares convencionais mais custosos. Isso ocorre levando-se em consideração percepções sociais dos diversos grupos que compõem o ambiente interno da administração pública, a percepção que esses grupos tem da dinâmica social externa à administração pública, assim como das necessidades estruturais e funcionais do aparato burocrático.

Atualmente, as estratégias de defesa enfrentam novos desafios em relação à dinâmica das TIC. O que envolveria preocupações de cunho operacional, como: i) a instrução dos militares para a gestão eficaz e eficiente da informação, consubstanciando sua correta organização, em suas diversas formas; ii) o manuseio de componentes eletrônicos, para operar sistemas e redes de informação e comunicação, até a atuação no campo operacional; e iii) a observação do caráter humanitário, em relação às formas de uso dessas informações pelos Estados. Pois, quando uma informação é compartilhada, ela deixa de ser exclusiva de determinado Estado e passa a ser de uso comum do grupo cooperante. E o problema reside nas seguintes questões: quem a utilizará e como a utilizará, para atingir quais objetivos?

Nisso reside, de certa forma, uma mudança de paradigma que tem início na mudança de postura do Brasil frente aos desafios internacionais. A nova conjuntura política e econômica impõe ao País, dessa maneira, rever prioridades científicas e tecnológicas militares. Algumas delas não tinham importância alguma, como os recursos cibernéticos, e outras já tiveram importância, mas foram relegadas em passado recente, como o investimento em artefatos convencionais (i.e. navios de guerra, blindados, aviões etc.). O que está relacionado diretamente à complexidade que marca a estrutura burocrática estatal e sua necessidade de controlar recursos, planejar programas e projetar poder.

O esforço brasileiro em relação ao controle e ao domínio do ciberespaço confunde-se, de certa forma, com os objetivos traçados pelo Estado para a ocupação do território nacional. Expedições científicas realizadas desde o século XIX, com o objetivo de coletar dados sobre a natureza, a topografia etc., vem sendo parte de uma política de controle sobre tudo o que ocorre e quais seriam as potencialidades oferecidas pelo território brasileiro. Assim, expedições para a implantação das linhas telegráficas, lideradas pelo Marechal Cândido Rondon, por exemplo, demonstram a relevância concedida pelo Estado para a integração e o reconhecimento sobre onde se projeta essa soberania.

Nos anos 1960, concebeu-se o Sistema Brasileiro de Telecomunicações, como a primeira iniciativa no mundo para a construção de um sistema integrado de telecomunicações. Em 1998, o Brasil entra na era do georrefer-

enciamento por satélite para o monitoramento do espaço territorial amazônico, tendo como pilar o pacto cooperativo com os países amazônicos. Pode-se dizer que a concretização de várias ações de informação foram pautadas pela agenda do Tratado e Cooperação Amazônica (TCA), assinado em 1978. Posteriormente, nos anos 1990, implantou-se um sistema de informação para o controle e o monitoramento territorial, que ficou conhecido como Sistema de Vigilância da Amazônia (SIVAM), inserido na macroestrutura do Sistema de Proteção da Amazônia (SIPAM), e objetiva fornecer informação para a tomada de decisão política em várias áreas de atuação de atores públicos estatais e não estatais. Segue-se, no século XXI, a ampliação de uma agenda em política de informação baseada na expansão geoestratégica do Brasil, agora em direção às suas fronteiras marítimas. Surge a necessidade de proteger recursos naturais, antes inexplorados, mas devidamente mapeados pelo Estado brasileiro. Da necessidade política de afirmação de poder, cresce a necessidade de proteção dos recursos por meio de ações de informação em defesa. Agora, além do território amazônico, as preocupações do Brasil voltam-se também para o Oceano Atlântico, denominado "Amazônia Azul" pela Marinha de Guerra do Brasil.

Essa linha do tempo demonstra o quanto torna-se necessária à estratégia de defesa, a articulação de uma política de informação que leve em consideração o contexto geopolítico e os atores envolvidos, e a partir disso, o desenvolvimento de uma arquitetura dos recursos de informação que serão capazes de responder aos desafios impostos pelas relações internacionais. Atualmente, a descoberta do pré-sal e a liderança política exercida pelo Brasil de forma direta na América Latina (AL), por meio do Mercosul e da Unasul, e entre os países considerados emergentes, por meio do G-20 e dos BRICs, são eventos que contribuem para a projeção do País no cenário internacional. Essa realidade retroalimenta-se por meio do histórico papel que o Brasil exerce na AL e na África como ator cooperante na área técnico-científica em setores como: agropecuária, informação científica e tecnológica, energia, e segurança e defesa. Esse é um princípio de política externa que o Brasil carrega, e essa preocupação converge para o planejamento da END.

Um dos pontos mais importantes da END encontra-se no investimento em recursos de informação como fortalecimento da estrutura militar em relação à possibilidade da eclosão de uma ciberguerra. Nesse sentido, algumas iniciativas voltam-se para as discussões na área de Defesa, considerando dessa vez o investimento em recursos de informação para a guerra, envolvendo diversos órgãos, por meio de políticas cooperativas com atuação em rede.

Da cooperação política à infraestrutura das redes: a estratégia de informação para a Defesa

Pode-se dizer, de certa maneira, que no âmbito de atuação direta do Brasil sobre a América do Sul e o Atlântico Sul, as condições políticas seriam mais favoráveis para uma cooperação internacional irrestrita com aqueles países que possuem certa afinidade cultural e geográfica. Um exemplo seria o dos mecanismos de cooperação técnica internacional (CTI), na qual o Brasil usufrui de uma posição de fornecedor de *expertise* tecnológica nas áreas de infraestrutura, saúde, agricultura, prospecção geológica etc., por meio de empresas e órgãos estatais. De certa forma, estruturar um sistema de informação, que seja compartilhado, demandaria alguns cuidados estratégicos em se tratando de atores estatais com disparidade em nível tecnológico, mas que seria essencialmente cooperativo. Por outro lado, com relação aos *players* globais, com interesses no Atlântico Sul, como é o caso dos países membros da Organização do Tratado do Atlântico Norte (OTAN), o Brasil pode e deve cooperar, mas tendo a noção exata de que poderá ser uma relação desigual para o País, na qual entraria como potencial consumidor tecnológico. Ou seja, duas perspectivas, e duas formas de estar no mundo por meio dos possíveis usos cooperativos dos recursos operacionais de informação; como considera Amorim (2013): "[...] do ponto de vista regional, na América do Sul, cooperação; do ponto de vista global, dissuasão. Sem perder de vista que também tem que ter cooperação, nada é preto e branco."

Apesar de estar previsto na END a possibilidade de um conflito cibernético, e a adoção de medidas para a defesa militar da infraestrutura crítica, o atual Ministro da Defesa brasileiro, Celso Amorim, reconheceu que o

Brasil não está preparado para enfrentar os desafios impostos pelas ameaças cibernéticas[8]. Tendo em vista a projeção estratégica do País nas regiões amazônica e do Atlântico Sul, torna-se crucial questionar como deverá ser estabelecida a relação política entre os diversos atores com os quais o Brasil se relaciona militarmente para o compartilhamento e o uso das informações. Porque ações de informação preparativas para a ciberguerra, resultam de planejamentos diferentes, para atingir objetivos diferentes. No caso dos fóruns nos quais o Brasil é membro, como o da Unasul, as discussões giram em torno de uma perspectiva cooperativa, em que se valoriza, primordialmente, uma relação horizontalizada. Por outro lado, o Brasil insere-se no sistema político internacional como um ator de peso, transformando-se em alvo de ameaças potenciais.

A mesma necessidade que impulsiona o Brasil para a cooperação irrestrita com seus vizinhos de fronteira, impõe ao País a troca com outros atores hegemônicos, que alimentam outros interesses que não uma relação alicerçada na dialética política mas, estritamente, no mercado competitivo. Portanto, a mesma dinâmica que proporciona a cooperação, produz a ameaça à soberania nacional, acarretando questões éticas fundamentais, como a possibilidade de acesso, sem o consentimento dos órgãos de defesa às informações estratégicas nacionais, como no caso da coleta de dados do Pré-Sal feita pela Agência de Segurança Nacional (NSA, na sigla em inglês), dos Estados Unidos. Segundo González de Gómez (2008, p.4), o que se estabelece na política internacional repercute na política de informação e vice-versa, moldando o que se pode denominar, de "infopolítica". Ou seja, existem questões políticas referentes a um contexto geográfico que, ao se relacionar com o fluxo de informação, com a comunicação e com a cultura, geram determinada situação política. Dependendo da intensidade de utilização de recursos técnicos e dos objetivos traçados politicamente para a execução de ações práticas, tem-se o ambiente propício para o advento de uma ciberguerra.

Essa possibilidade encontra a existência de uma lacuna tecnológica entre os países, causada por profundas desigualdades políticas e econômicas. Essa tendência repercute no arranjo do sistema de poder internacional, em que os Estados mais desenvolvidos apresentam vantagens comparativas inigualáveis em termos técnicos e operacionais em relação aos Estados menos desenvolvidos. Os Estados que dominam a técnica info-comunicacional, e a posicionam de maneira ofensiva, por meio de sofisticados recursos de informação, como satélites, bases de dados, cabos de fibra ótica e até AWACS, podem provocar instabilidades políticas, e gerar confrontos no ciberespaço. Por outro lado, os Estados menos desenvolvidos tecnologicamente apresentam limitações quanto à potência e sofisticação de recursos técnicos, o que compromete as ações de informação a serem implementadas. Por isso, tornar-se-ia ambivalente uma tentativa de cooperação entre países desiguais em termos de poder absoluto, pois os mais fracos, de um modo geral, apresentam elementos motivadores para que fossem, eles mesmos, monitorados e, com isso, um alvo mais fácil para ser atacado.

No caso do Brasil, que é um país considerado emergente, os alvos, apesar de não serem claros, girariam em torno tanto das fontes de riquezas naturais, quanto da projeção de poder do País, com o cenário atual de crescimento econômico sustentável e proatividade no cenário político internacional. Esse parece ser o quadro do Brasil tanto em relação aos Estados Unidos da América (EUA), quanto em relação à China, por exemplo. Essa preocupação torna-se notória quando se torna evidente a atividade de espionagem dos EUA sobre o Brasil, assim como a preocupação da sociedade brasileira em relação às próprias ações de monitoramento do Estado brasileiro contra a própria população. O que já ocorreu em tempo histórico recente e impõe questões relevantes a serem respondidas em outra ocasião.

Algumas delas, como se seguem: a) Como viabilizar um programa de cooperação para a defesa, o que pressupõe compartilhamento de informações, sabendo que um dos países cooperantes pratica ações de espionagem contra o outro?; b) Pode-se considerar que a infraestrutura crítica do Brasil esteja minimamente imune em relação a essas ameaças?; c) Qual seria o amparo legal para a proteção das informações que devem ou não ser compartilhadas?; d) Quais seriam os desdobramentos éticos desse novo modelo de defesa?; Como o Brasil se posiciona nesse novo cenário de ameaças difusas, considerando sua complexidade social, política e geoestratégica? Defende-se, a partir dessas questões, que apesar da hegemonia da perspectiva da técnica sobre a política, o Brasil apresenta novas possibilidades de inserção via cooperação multilateral na área de defesa

[8] No Senado, Celso Amorim admite vulnerabilidades na defesa cibernética. Disponível em: http://g1.globo.com/politica/noticia/2013/07/ministro-da-defesa-admite-vulnerabilidades-na-defesa-cibernetica.html. Acesso em: 12 de julho de 2013.

militar. Tenta-se, com isso, inverter a lógica dominante do Mercado e da competição tecnológica, cedendo espaço ao compartilhamento de informações para a cobertura de necessidades comuns, baseado na valorização da negociação e do diálogo.

Considerações finais

A transversalidade é a marca de ameaças difusas, de origem imprecisa, que operam a partir de estruturas em rede, impactando severamente a segurança do Estado. Ações de grupos terroristas, ou do crime organizado transnacional, utilizam-se das TIC para expandir seus negócios. Inerente a esse processo, encontra-se a reprodução de um modelo de C&T que vem sendo implantado nos laboratórios e aplicados ao redor da aldeia global. Paralelo ao discurso da "liberdade de expressão", encontram-se outros valores que limitam essa liberdade a um grupo fechado de corporações privadas e governos centrais. Recentemente, os resultados de novas invenções tecnológicas, que foram publicadas em jornais de grande circulação, dão conta do desenvolvimento de tecnologias que já fazem parte do rol das tecnologias militares. Diversos projetos vem sendo colocados em prática em universidades pelo mundo, como o de controle de helicóptero com a força do pensamento, da Universidade de Minnesota, ou a tecnologia da invisibilidade, na Universidade de Rochester (Nova York). Baseado nessa tendência, as duas questões éticas subjacentes ao quadro geral apresentado são: i) Quem se beneficiará desses recursos tecnológicos?; e, ii) Como essas tecnologias serão utilizadas? A técnica domina a política e automatiza as relações sociais, colocando o cidadão comum como objeto da ação e não como ator, que demanda necessidades. As invenções tecnológicas que são elaboradas nas universidades e adotadas em projetos militares, impulsionam os mecanismos de controle ideológico sobre os cidadãos, pautados pelas necessidades de grupos ligados à agenda de defesa nacional.

Voltando aos anos 1950, o ex-presidente estadunidense Dwight Eisenhower pronunciou um famoso discurso, no qual enfatizava os perigos impostos à liberdade democrática, pela falta de controle do crescimento de um complexo industrial-militar. Atualmente, o complexo militar proporciona a cooptação da Política (com P maiúsculo), promovendo a desestabilização e a condenação do sistema democrático estabelecido. Os recursos de informação e comunicação há muito vem sendo utilizados não só como ferramentas para a troca, mas também como instrumentos de controle e monitoramento. E com isso nem sempre a privacidade dos cidadãos é respeitada. Nesse sentido, o que mais interessa em relação à utilização dos recursos de comunicação, são as formas de uso da informação.

A defesa nacional é um dever do Estado em relação à proteção de suas infraestruturas e da sociedade contra ameaças externas e internas. No entanto, o modelo de defesa que vem sendo implantado, obedece à uma dinâmica sistêmica baseada nas diretrizes técnicas orientadas em acordos de cúpula, com suporte do complexo industrial-militar. Nesse sentido, a produção técnica se impõe sobre a lógica da Política, reconfigurando o espaço das trocas e complexificando as relações de poder. Ao Brasil, com suas limitações técnicas, cabe reforçar laços políticos multilaterais, primeiramente com seus vizinhos de fronteira (terrestre e marítima), e depois em fóruns globais cooperativos, como, por exemplo, com os outros membros dos BRICs (Rússia, Índia, China e África do Sul), com o objetivo de fortalecer os recursos de informação para mitigar possíveis danos causados por potenciais inimigos à sua infraestrutura crítica.

Essa parece ser uma lógica diferenciada daquela imposta pelos atores hegemônicos, pois se propõe a estabelecer relações políticas entre atores que possuem interesses e necessidades sociais semelhantes. A técnica não é subssumida mas, de certo modo, deve ser relativizada, e colocada sob o guarda-chuva das relações políticas, possibilitando, dessa maneira, contemplar questões éticas fundamentais em relação à ciberguerra. Mesmo que sejam encontradas dificuldades para o controle técnico-operacional dessas ameaças cibernéticas, a política tecida entre os Estados, por meio da cooperação, possibilita identificar essas ameaças, e neutralizá-las pelo uso político da informação em uma estrutura em rede.

References:

Arendt, Hannah. O que é política?(trad.) Reinaldo Guarany. Rio de Janeiro: Bertrand Brasil, 2002, p.240.

Backstrom, A. and Henderson, I. New capabilities in warfare: an overview of contemporary technological developments and the associated legal and engineering issues. In: International Review of the Red Cross, Article 36 weapons reviews, v. 94, n. 886, Summer 2012, pp. 483-514.

Carvalho Paulo Sérgio M. de. Desafios Estratégicos para a Segurança e Defesa Cibernética. SAE, Brasília, 2011, p.18. Disponível em: http://www.sae.gov.br/site/wp-content/uploads/Seguranca_Cibernetica_web.pdf*. Acesso em: 07 de agosto de 2013.*

Felipe Néri. No Senado, Celso Amorim admite vulnerabilidades na defesa cibernética. Disponível em: http://g1.globo.com/politica/noticia/2013/07/ministro-da-defesa-admite-vulnerabilidades-na-defesa-cibernetica.html*. Acesso em: 12 de julho de 2013.*

González de Gómez, Nélida e CHICANEL, Marize. A mudança de regimes de informação e as variações tecnológicas. IX ENANCIB, USP: São Paulo, 2008.

Lin, Herbert. Cyber conflict and international humanitarian law. International Review of the Red Cross. Volume 94 Number 886 Summer 2012. p. 515-531.

MINISTÉRIO DO PLANEJAMENTO, ORCAMENTO E GESTÃO. BRASIL. Disponível em: http://www.governoeletronico.gov.br/sisp-conteudo*. Acesso em: 02 de agosto de 2013.*

UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH (UNIDIR). The Cyber Index - International Security Trends and Realities. New York/Geneva, 2013.