# TERRITORIALIZANDO O "NOVO" E (RE)TERRITORIALIZANDO OS TRADICIONAIS: A CIBERNÉTICA COMO ESPAÇO E RECURSO DE PODER[1]

Walfredo Bento Ferreira Neto[2]

## RESUMO

Este artigo aborda a cibernética como recurso de poder e um espaço em si (o ciberespaço). Quanto a este, revisitando o processo de ocupação das dimensões tradicionais – terrestre, marítima, aeroespacial – e suas transformações pelo poder, deparou-se com o fenômeno da *territorialização*, abrangendo, agora, o domínio cibernético, que por ser originariamente rede e espaço, demanda um novo tipo e forma de fronteira: a "*fronteira-ponto*", resultante da capacidade tecnológica acumulada historicamente. Mais que isso, como originalidade, a "*fronteira-ponto*" traz para o sistema internacional a configuração de uma nova fase da Teoria das Fronteiras e a exigência de novas delimitações político-jurídicas. Vista como recurso, a cibernética acelera o fluxo informacional, altera o cálculo convencional de equilíbrio do poder e aumenta a capacidade de monitoramento e armazenamento de informações utilizada na *(re)territorialização* das dimensões expostas à globalização. Ainda como meio à disposição da política, a cibernética pode ser utilizada para a guerra. Além da observação e da construção hipotético-dedutiva, realizou-se uma investigação bibliográfica e documental, nacional e estrangeira, com ênfase em políticas públicas. Conclui-se que o "saber pensar" geopolítico, com sua respectiva aplicação no (e a partir do) ambiente cibernético, torna-se relevante para os formuladores de políticas na área de defesa e de estratégia, especificamente com relação às possibilidades advindas desse "novo" recurso.

**Palavras-chave**: Cibernética. Territorialização. Fronteira-ponto.

---

[1] Artigo vencedor do IV Prêmio Marechal-do-Ar Casimiro Montenegro Filho, tema cibernética, organizado pela Secretaria de Assuntos Estratégicos da Presidência da República, e elaborado a partir da dissertação de mestrado "*Por uma Geopolítica Cibernética: apontamentos da Grande Estratégia brasileira para a nova dimensão da guerra*" apresentada, defendida e aprovada pelo PPGEST/UFF, em 27 de junho de 2013.

[2] Mestre em Estudos Estratégicos da Defesa e Segurança, pelo PPGEST/UFF. Professor de Relações Internacionais e de Geografia da AMAN.
Lattes: http://buscatextual.cnpq.br/buscatextual/visualizacv.do?id=K4218339Y1.
Contato: wbfneto@bol.com.br

**Abstract**

his paper discusses cybernetics as power resource and space itself (cyberspace). On this, revisiting the process of occupation of traditional spatial dimensions – land, sea, aerospace – and their transformations for power, was faced with the phenomenon of *territorialization*, covering now the cyber domain, which, being originally space and network, demand a new type and form of boundary: the "boundary-point", resulting from historically accumulated technological capability. Furthermore, as originality, "boundary-point" brings the international system configuration of a new phase of the Theory of Borders and the requirement of new legal-political boundaries. Seen as a resource, cybernetics accelerates information flow, in space and time, changes the conventional calculation of the balance of power and increases the capacity for monitoring and storing information used in *(re)territorialization* of dimensions exposed to globalization. Also available as a means of politics, cybernetics can be used for war. Beyond observation and construction hypothetical-deductive, was realized documentary and bibliographical research, domestic and foreign, with emphasis on public policy. Concluded that the "know-think" geopolitical, to their respective application in (and from) the cyber environment, it becomes relevant to policy makers in the area of defense and strategy, specifically with regard to the possibilities resulting from this "new" feature.

**Keywords**: Cybernetics. Territorialization. Boundary-point.

## 1 Instigações iniciais e marcos teórico-metodológicos

Nos últimos anos tem-se verificado um aumento na quantidade de fatos, de documentos oficiais, de bibliografia e de pesquisas cuja temática é a cibernética empregada na relação entre Estados. Expressões como defesa e segurança, comando e centro militar cibernéticos e guerra cibernética ganham projeção e espaço nas agendas políticas.

Isso se justifica porque no interior dessa "nova" palavra se encontra um dos tradicionais recursos de (e do) poder: a informação. A novidade é que, dependendo da capacidade de cada ator, ciberneticamente falando, há a possibilidade de um ganho real de tempo e, a partir de então, de uma maior consciência situacional.[3] A partir do uso da cibernética, o tomador de decisão aumenta a probabilidade de influenciar outrem e, por conseguinte, aumenta sua chance de êxito na consecução do objetivo.

Desse modo, de timoneiro ou de governo, pelo sentido empregado na Grécia Antiga (MOREIRA, 1980), passando pelo estudo que visava à substituição das funções humanas de controle por sistemas mecânicos e eletrônicos (WIENER, 1973), a cibernética alcança, hoje, uma conotação que compreende as ideias mestras de informação e de comunicação, daí o termo infovias, utilizado para representar os meios pelos quais as informações digitalizadas circulam.

Como uma consequência, hipoteticamente falando, em face das possibilidades a partir do uso da cibernética, a segurança das infovias – estas constituídas por ferramentas de Tecnologia da Informação e das Comunicações – passou a ser mais uma meta perseguida pelo Estado, a fim de garantir o fluxo de suas mensagens e impedir ou negar acesso não autorizado ao conteúdo que por essas vias transitam.

---

[3] Segundo Silveira (2011, p. 33): "Uma robusta rede integrando forças geograficamente esparsas e de natureza difusa, todas providas por um mesmo nível de informações (táticas e estratégicas) de modo a tirar partido de um mais amplo conhecimento da situação (*situation awareness*) nos diversos níveis de comando, a permitir melhor sincronização de ações e acelerar decisões, aumentando a eficácia das missões dessas forças integradas por redes digitais de alta velocidade".

Ainda como hipótese, esses mesmos noticiários, agendas e discursos acerca da cibernética tratam-na: 1) ora como um recurso à disposição da política, materializado na informação, portanto um recurso clássico, que, de "novo", possui apenas seu processamento por um computador; 2) ora como mais uma dimensão espacial, o ciberespaço, um domínio espacial autônomo, da mesma forma que o terrestre, o marítimo, o aéreo e o extra-atmosférico.

Quanto a esta última ótica, apesar de formalmente considerado um espaço de uso comum, ou um *global common* na visão de Posen (2003), de Rodrigues (2012) e de Ferreira (2012), esse espaço tem seu controle, logo seu empoderamento, realizado por apenas alguns atores: os mais aptos.

Assim, a cibernética passa a ser tratada como um território, *locus* em que o poder é exercido e confrontado de forma constante, eis que é objeto inerente a uma relação. O que acontece é que, diferentemente dos espaços tradicionais, o ciberespaço é bastante artificial, fruto do atual estágio de desenvolvimento da sociedade e de suas ferramentas tecnológicas. Esse espaço, logo, possui características que desafiam a apreensão e, por conseguinte, a compreensão imediata acerca de sua realidade. Todavia, ao que tudo indica, ele existe.

Por conseguinte, tratando a cibernética como um espaço, verifica-se um processo que os estudos geográficos e geopolíticos denominam *territorialização*, definido por Robert Sack (1986 apud HASBAERT, 2002, p. 119) como uma "tentativa de um indivíduo ou um grupo de atingir, influenciar ou controlar pessoas, fenômenos e relacionamentos, através de delimitação e afirmação do controle sobre uma área geográfica". Esse processo enfatiza, portanto, "o controle de acessibilidade, o território definido, sobretudo através de um de seus componentes, a fronteira, forma por excelência de controlar acesso" (HASBAERT, 2002, p. 119).

Dessa forma, para dar o primeiro passo na direção de uma apreensão desse fenômeno aplicado a essa dimensão, é necessário entender que a delimitação da fronteira do "território cibernético", um território originalmente na forma de rede ("*território-rede*"), não pode ser pensada no formato de *zona* ou de *faixa*, como ocorreu

com o espaço terrestre até a Idade Média, nem no de *linha*, como passou a ser tratada a epiderme do Estado moderno (MEIRA MATTOS, 1990; RAFFESTIN, 1993; GIDDENS, 2001; BUZAN; HANSEN, 2012), aproveitando-se de uma maior capacidade de centralizar informações e de produzir tecnologia, como foi o caso da representação por meio de mapas cartográficos.

A fronteira do "*ciberterritório*", coexistindo com as formas pretéritas de delimitação de poder no espaço, deve ser vista na forma de *ponto*, que pode ser ao mesmo tempo uma informação em seu "pacote", ou um "nó" de uma infovia, ou, ainda, uma estrutura estratégica ou infraestrutura crítica selecionada graças, mais uma vez, ao aprimoramento dos recursos disponíveis ao principal ator do sistema internacional: o Estado.

Além disso, ao se abordar a cibernética como mais um recurso de (e do) poder, percebe-se que esse instrumento vem servindo também para uma *(re)territorialização* dos espaços tradicionais, que se encontram expostos ao que se convencionou chamar de globalização, e que, por consequência, estariam submetidos a um processo de *(des)territorialização*.

Esse é o fenômeno apontado por Raffestin (1984 apud SAQUET, 2007) pela sigla T–D–R, correspondendo à territorialização, à (des)territorialização e à (re)territorialização, respectivamente. Essa, portanto, é uma das linhas mestras e premissas deste trabalho, em que os conceitos (des)territorialização, por um lado, e territorialização e (re)territorialização, por outro, de forma ampliada, pela qual alcançam o espaço cibernético, estarão, pelo menos aparentemente, confrontando-se de forma constante, como na lei da ação e reação, mas nem sempre, historicamente, atingindo uma síntese, como nos mostram os imponderáveis *clausewtzianos*. É na permanência desse confronto que surgem os conflitos e a demanda por uma normatização a fim de se evitar a guerra.

Essa relação de causalidade pode ser assim evidenciada: quanto maior a territorialização do ciberespaço, maior é a capacidade de (re)territorializar, isto é, controlar as demais dimensões espaciais.

Ainda, em virtude da atualidade e da complexidade do tema – que, por si, envolve várias áreas do pensamento científico, tanto exatas quanto naturais, sociais e humanas –, faz-se mister o registro do que não se pretende realizar.

Primeiramente, ressalta-se que, como se está tratando de relações entre Estados, o trabalho não aborda a perspectiva entre Estado-indivíduo em seu ordenamento jurídico, como, por exemplo, as regras de uso e controle da internet e de redes sociais;[4] de crimes comuns via meios eletrônicos ou informatizados, de prostituição ou pedofilia "virtual".[5] Apesar disso, tem-se ciência dessa possibilidade, que, na visão do geógrafo suíço Claude Raffestin (1993), caracterizaria a utilização do aparelho estatal para o controle de sua população ou, para Kaplan (1974), serviria como mais um recurso que o Estado passa a possuir para garantir algumas de suas principais funções, como a institucionalização; a legitimidade e o consenso; a legalidade; a coação social; a educação e a propaganda; e a organização coletiva.

Também não se abordam profundamente as operações e os termos técnicos a respeito da cibernética ou do uso da segurança das informações, como no caso de modelos matemáticos ou chaves logarítmicas, sistemas criptográficos e *malwares* (vírus, antivírus, *trojan horses* e *worms*) no interior de um *software*.

O estudo e a aplicação da cibernética no campo da neurociência também não são levados em consideração, embora se tenha plena certeza que é de grande valia para o desenvolvimento científico por envolver o "comando e o controle" do próprio organismo, tal qual um sistema aberto idealizado por Wiener (1973[1954]) em sua teoria.

## 2 O ciberespaço e seu uso pelo e para o poder

Para Lévy (1999), o ciberespaço corresponde a um espaço de comunicação aberto pela interconexão de computadores e das memórias dos computadores, incluindo os sistemas de comunicação tanto por meio de ondas *hertz* quanto pela telefonia clássica, a partir do momento em que essas participarem do processo de transmissão de informações digitalizadas.

---

[4] Como vem ocorrendo com o debate sobre o *Stop Online Piracy Act* (SOPA) e o *Protect IP Act* (PIPA), ambos em tramitação no Congresso Norte-Americano.

[5] Como foi o caso, no Brasil, da aprovação, em 03/12/2012, da lei que prevê prisão para quem cometer crime na internet: "Invadir computadores alheios ou outro dispositivo de informática com a finalidade de adulterar, destruir ou obter informações sem autorização do titular", ficando conhecida como lei Carolina Dieckmann.

Mandarino Júnior (2011), do Gabinete de Segurança Institucional da Presidência da República do Brasil (GSI/PR), acredita que o espaço cibernético compreende também as pessoas, as empresas e os equipamentos que porventura estejam interconectados, participando, de alguma maneira, do tráfego de informações digitalizadas.

Richard Clarke e Robert Knake debruçaram-se sobre esse tema em um dos capítulos do *Cyber war: The Next Threat to National Security and What to Do About It*. Os autores iniciaram investigando o que seria o ciberespaço e indicando que o termo mais parecia, em um exercício de imaginação, outra dimensão, com iluminação verde e coluna de números e símbolos piscando no ar como no filme *Matrix* (CLARKE; KNAKE, 2010).[6] Mas, logo em seguida, atestam que esse novo espaço é realmente bem mundano, no qual está inserido o *laptop* que nós conduzimos ou o que as crianças levam para a escola ou, ainda, um computador de nosso local de trabalho ou uma tubulação instalada sob uma rua. Para Clarke e Knake (2010), hoje o ciberespaço está em toda parte, em todo lugar em que encontramos um computador, ou um processador, ou um cabo de ligação.

Esses norte-americanos trazem como conceito que o ciberespaço corresponde a todas as redes de computadores em todo o mundo, e tudo que conecte ou controle. Ciberespaço inclui outras redes de computadores além da internet, que, supostamente, não são acessíveis a partir desta (CLARKE; KNAKE, 2010).

Nesse sentido segue Reveron, baseando-se na definição de ciberespaço do Departamento de Defesa dos Estados Unidos da América (EUA), informando que esse espaço é "um domínio global dentro do ambiente de informação que consiste na rede interdependente de infraestruturas de tecnologia da informação, incluindo a internet, redes de telecomunicações, sistemas de computador e processadores embarcados e controladores" (REVERON, 2012, tradução nossa).

---

[6] A obra de Clarke e Knake (2010) e a de Reveron (2012) encontram-se no formato de leitura do *kindle* (*e-book*), razão pela qual não foi possível a definição de uma numeração de página específica.

Prossegue esse autor afirmando que o ciberespaço, assim como o ambiente físico, é muito abrangente, incluindo o *hardware*, como redes e máquinas; as *informações*, como dados e mídia; o *cognitivo*, como o processo mental das pessoas; e o *virtual*, no qual as pessoas se conectam socialmente (REVERON, 2012).

Daniel Ventre, pesquisador do Centro de Investigações Científicas e secretário geral do Grupo Europeu de Pesquisa de Normas (GERN), ambos de Paris, elaborou uma proposta quanto aos componentes do ciberespaço. Para Ventre, esse espaço é composto por três "capas", assim denominada cada parte desse domínio. Colocando em uma tabela, a proposta de Ventre fica assim ilustrada:

**Tabela 1. Espaço cibernético – "capas" e respectiva composição**

| "CAPA" | COMPONENTES |
|---|---|
| **Inferior** | - física, material, condizente com a infraestrutura (hardware, redes,...) |
| **Intermediária** | - softwares de aplicações |
| **Superior** | - cognitiva |

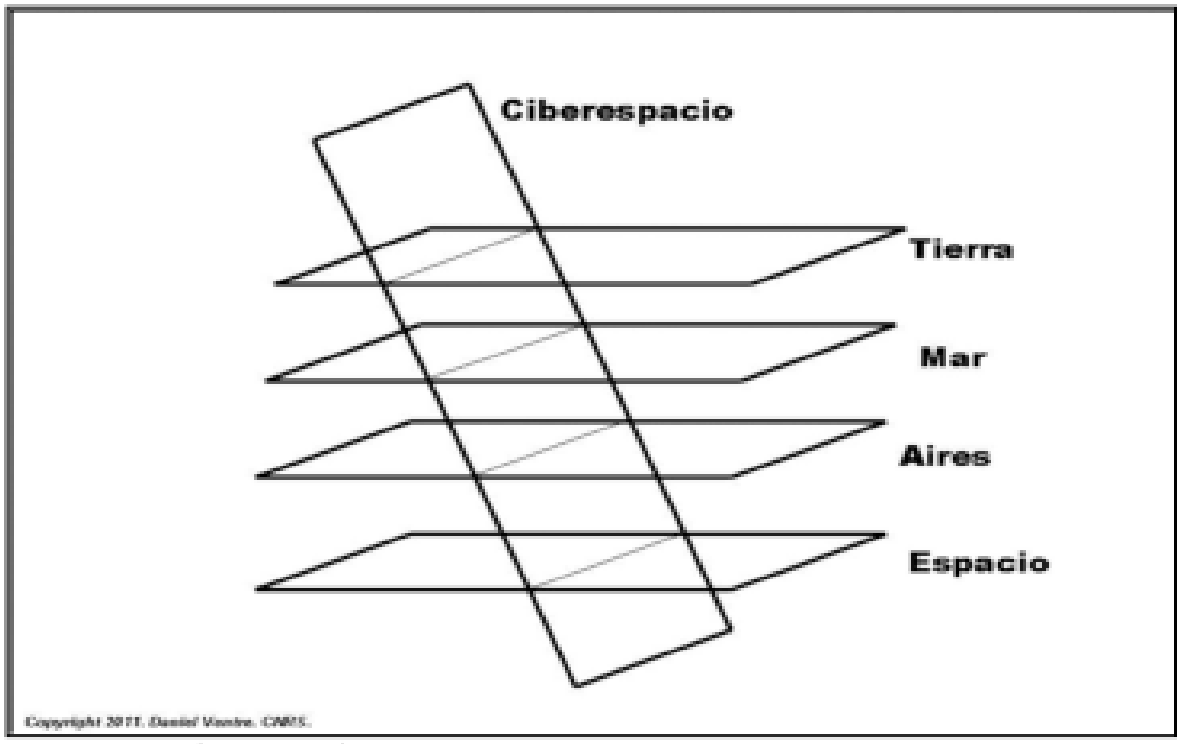
Fonte: elaborado com base em Ventre (2012, p. 34)

A visão do pesquisador do GERN-Paris se coaduna com a tríade formulada por especialistas das áreas de análise de sistemas e de informática, que entendem o *hardware* como a parte rígida ou os componentes do sistema; o *software*, o que diz respeito à programação; e o *peopleware*, referindo-se às pessoas que atuam nesse setor por meio do conhecimento. Além disso, representando graficamente, Ventre (2012, p. 34) expõe o domínio cibernético em face das outras dimensões espaciais, conforme Figura 1, afirmando que uma das características mais marcantes desse novo domínio é a sua transversalidade.

Essa transversalidade torna-se uma característica bem significativa do ciberespaço, uma vez que permite a projeção de poder e seus reflexos nos demais domínios espaciais ou, como é tratado até aqui, o fenômeno da *(re)territorialização*. Ainda se atendo ao ciberespaço, sobretudo quanto às suas características e composição, Nye (2012) enxergou essa dimensão espacial dividida em duas partes principais: o "*intraespaço*" e o "*extraespaço*" cibernético.

Ao se analisar essa forma de simplificação, chega-se à conclusão que muito condiz com a visão do chefe do Comando Cibernético dos Estados Unidos, general Keith Alexander, que vê o ciberespaço "sendo usado por militares no futuro operando de dentro (ou através dele) para atacar pessoal, instalações ou equipamentos [...]" (apud REVERON, 2012, tradução nossa).

**Figura 1. Ciberespaço e relação com outras dimensões espaciais**




Fonte: VENTRE (2012, p. 35)

Dessa forma, ambos mencionam a possibilidade de operações ocorrerem *dentro* (no *intraespaço*) e *através* (no *extraespaço*) do ciberespaço. Nye chega a comparar o poder advindo da cibernética com o poder marítimo, no qual também se distingue o *poder naval sobre os oceanos* – o que, por sua teorização, corresponderia ao *intraespaço marítimo* – do *poder naval sobre outros domínios*, isto é, o poder projetado do ambiente marítimo para outro domínio espacial, no caso o *extraespaço* cibernético.

No intraespaço de Nye, na "capa" inferior e intermediária de Ventre, ou no que se denominou ao longo do trabalho *espaço cibernético considerado em si mesmo*, algumas ações são efetuadas a partir do, e com reflexos no, próprio espaço, como nos exemplos

dos ataques de negação de serviço (*Distributed Denial of Service – DDoS*[7]), ou do controle de companhias e empresas, no caso da estrutura física do ambiente cibernético, ambas caracterizando formas de utilização *hard* do poder.

Ao mesmo tempo, a relação política e seus conflitos nesse espaço podem ocasionar reflexos externos, diga-se no mundo sensorial humano, como no ataque ao sistema SCADA, em 2010, nas usinas nucleares iranianas ou na possibilidade de rupturas de serviços essenciais à população, como no caso de danos às estruturas estratégicas de um Estado: energia elétrica, distribuição de água, serviço de telecomunicações, sistema financeiro, etc.

Dessa forma, e por suas várias interpretações e possibilidades, o espaço cibernético, apesar de considerado virtual e um *global common*, já há algum tempo o deixou de ser. Alguns atores empoderam-se desse espaço, delimitando-o unilateralmente e dispondo de seu controle. É nesse sentido que se enxerga o espaço cibernético não mais como um espaço comum, e sim como um território. Tentar entendê-lo e teorizá-lo, para saber "jogar", e definí-lo, delimitá-lo e demarcá-lo, com as respectivas responsabilidades advindas, torna-se um pressuposto a ser considerado na formulação de políticas sobre esse tema e sob essa abordagem.

## 2.1 O território cibernético e sua fronteira

Compreensão exige teorização. Teoria exige abstração, que, por sua vez, exige simplificação e ordenamento da realidade (HUNTINGTON, 1996). Esse entendimento é necessário para a compreensão do *constructo* que se fez até aqui. As percepções sobre a confluência da aplicação do conceito de território e da Teoria das Fronteiras no ambiente cibernético se, no início da pesquisa, se deu de forma dedutiva, ao longo desta investigação foi-se confirmando, tanto pela bibliografia consultada quanto pelas notícias e pelos documentos de órgãos públicos, corroborado em entrevistas de agentes, militares e civis.

---

[7] Ou *DoS Attack*, que ocorre a partir da sobrecarga do sistema e não de uma invasão. Geralmente, um computador mestre comanda milhares de computadores denominados *zumbis*, que passam a funcionar como máquinas escravizadas.

Além disso, as ações planejadas e já implementadas para esse domínio seguem esse sentido. A resposta do Estado para essa possibilidade de ação no ambiente cibernético acompanha o fio condutor da territorialização ocorrida outrora com os demais domínios: o terrestre, o marítimo, o aéreo e o cósmico.

Na abertura do III Seminário de Defesa Cibernética, o ministro da Defesa do Brasil, Celso Amorim (2012), argumentou:

> A internet alterou os parâmetros de ação humana. O próprio conceito de realidade foi expandido pelo espaço digital. A cibernética emergiu como um novo domínio para a Defesa, e veio somar-se ao mar, à terra, ao ar e ao espaço. Aberto à ação humana, o domínio cibernético abre-se também ao conflito.

A revista *The Economist* (2010) de certo modo referiu-se aos estudos de Clarke e Knake (2010) sobre a guerra cibernética no artigo Guerra no quinto domínio: o *mouse* e o teclado são as novas armas do conflito?

O general João Roberto de Oliveira (2012), pioneiro na implantação do setor cibernético no Exército Brasileiro e hoje à frente do Sistema de Monitoramento de Fronteiras (SisFron) assim se expressou:

> [...] No campo militar e mesmo no político, considera-se que existem cinco dimensões no conflito moderno: o terrestre, o aéreo, o marítimo, o espacial e o cibernético. Para os três primeiros é possível estabelecer-se limites ou fronteiras físicas. Na dimensão espacial já há dificuldade de se estabelecer limites ou fronteiras, pois o espaço sideral não é regido, ainda, por regras de utilização bem delimitadas. Temos discussões em alguns órgãos internacionais sobre situações focais, como por exemplo, o uso do espaço para a localização de satélites geoestacionários e outros temas de interesse comum (por sinal, o Brasil está muito atrás nessa discussão, pois até agora o País não tem nenhum satélite próprio).

Inúmeros países e outros atores do sistema internacional, dos diversos tabuleiros e posições do jogo do poder, participam dessa reação, tentando ora delimitar unilateralmente esse novo espaço, ora elaborar normas para a garantia de seu funcionamento:

• os Estados Unidos, por meio do Departament of Defense (DoD), da Defense Information Systems Agency, da National Security Agency (NSA), do Departament of Homeland Security, da Defense Intelligence Agency e de um Comando específico criado em 2010 para a cibernética (o USCYBERCOM) (OLIVEIRA, 2011, p. 116-117) (Quadro 1):

• o Reino Unido, com a primeira estratégia nacional de segurança cibernética (*Cyber Security Strategy of the United Kingdon: safety, security and resilience in cyber space*), lançada em 2009, com a previsão do Office Cyber Security (OCS), órgão responsável pela macrocoordenação, o Cyber Security Operations Center (CSOC), para monitorar o espaço cibernético e coordenar respostas aos incidentes (CANONGIA; MANDARINO JÚNIOR, 2009, p. 30-34);

• a China, anunciando a criação de uma unidade específica de segurança e defesa na Província de Cantão (VENTRE, 2012, p. 43), no que segue Clarke e Knake (2010), e até mesmo de uma Força Armada específica, "guerreiros cibernéticos", com a Coreia do Norte também seguindo essa mesma linha (SANTOS, 2011);

• o Canadá, com a Canada's 2010 Cyber Security Strategy (CCSS-CAN), pela qual foram enfatizados três pilares: 1) sistemas de segurança de governo; 2) parceria com o setor privado; e 3) segurança aos canadenses no acesso *on-line* por meio de medidas de sensibilização. A estratégia canadense para o ciberespaço também atribuiu inúmeras responsabilidades entre os ógãos da administração pública, civis e militares daquele país (DEIBERT, 2012, p. 3);

• na Europa, além da Inglaterra, destaca-se a Alemanha, por meio da Cyber Security Strategy for Germany (CSSG-ALE), e a França, pela *Défense et sécurité des systèmes d'information: stratégie de la France*;

• com relação aos organismos internacionais, a atenção é para a reação da OTAN, com o Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), e da ONU, conforme relatado em momento anterior, que realizou, inclusive, exercícios reais entre países da região do sudeste asiático próximos ao gigante chinês.

**Quadro 1. Estrutura de segurança e defesa cibernética dos EUA**

| Órgão | Funções de Interação com o Comando Cibernético |
|---|---|
| National Secutity Council | • planejar e coordenar as ati vidades gerais ligadas à segurança cibernética (natureza política); |
| Departament of Defense | • providenciar a capacitação e o adestramento profissional em Segurança e Defesa Cibernética em ligação com o Homeland Secutity e o Director of National Intelligence; |
| Defense Information Systems Agency | • planejar, instalar, operar e manter, com segurança, a estrutura de TIC necessária para apoiar as operações conjuntas das Forças Armadas, líderes nacionais e outras missões envolvendo parcerias internacionais (coalizões) em todo o espectro de ações militares; |
| National Security Agency | • assegurar as atividades de inteligência do sinal[8] nos EUA, as quais enquadram a inteligência da área cibernética; |
| Departament of Homeland Securitv | • providenciar um estado de prontidã o nacional em face das ameacas cibernéticas às infraestruturas críticas do país; |
| Departament of Education e Office of Science and Technology Policv | • providenciar ações relativas à educação formal do cidadão a respeito da ameaça cibernética em todos os ní veis e em diferentes graus de intensidade; |
| Office of Personnel Menagement | • conscientizar os servidores públicos federais no que se refere ao seu papel no combate às ameaças cibernéticas. |

Fonte: elaborado com base em Oliveira (2011)

O fato é que esse "novo" domínio traz consigo uma série de questionamentos e, por consequência, incertezas.

Para o general José Carlos dos Santos, comandante do Centro de Defesa Cibernética do Exército Brasileiro (CDCiber/EB), em entrevista à revista *Época*, de 18 de julho de 2011: "No espaço cibernético a fronteira não existe [...]. O inimigo é difícil de identificar". Para Mandarino Júnior, diretor do Departamento de Segurança da Informação e Comunicações do GSI/PR: "Aqui (no espaço cibernético), a exemplo do espaço real, também são estabelecidas relações sociais e políticas, no tempo e no espaço" (MANDARINO JÚNIOR, 2011). Essas duas afirmativas demonstram bem os pontos de vista e as discussões a respeito do ambiente que envolve a cibernética, sobretudo no tocante à delimitação do poder nesse espaço, por ora desafiador.

[8] Inteligência de sinais – resulta da coleta, da avaliação, da integração e da interpretação dos dados relativos às emissões eletromagnéticas, compreendendo as inteligências de comunicações e eletrônica (BRASIL, 2007).

A primeira afirmativa, feita pelo comandante do CDCiber/EB, é propensa a declarar a inexistência de uma fronteira no espaço cibernético atualmente. Contudo, *in fine*, o mesmo militar admite que há um inimigo, porém de difícil identificação. Na verdade, como uma inferência, o que o general quis indicar, mesmo ciente da existência de um poder contrário – um oponente – nesse tipo de espaço, foi a impossibilidade de um encaixe do *constructo* voltado para a fronteira terrestre, uma fronteira tradicional, no ambiente cibernético.

Isso ocorre, também, em face da dificuldade de se detectar a origem, a autoria e a materialidade do ataque. Essas são, sem dúvida, algumas questões postas. De antemão, é preciso ter em conta que o espaço nesse ambiente não é natural nem pertence a uma geografia clássica. Esse espaço é específico, obedece a outras regras, e não a que considera o território mero substrato físico. O território do domínio cibernético é artificial, produto do homem e fruto do nível tecnológico atual, e é, originariamente, um "território-rede", ou melhor, uma "rede-território".

Da segunda afirmação, de Mandarino Júnior, diretor do DSIC/GSI/PR, apreende-se uma intenção de delimitar esse espaço em face das relações sociais e das políticas existentes, isto é, de poder, tal como acontece no espaço natural. O que ocorre, então, é que esse inimigo, relembrando a afirmativa do general, é um oponente que consegue se valer das características desse ambiente para não ser detectado ou, pelo menos, dificultar ao máximo sua detecção. Todavia, ele está lá, atuando e jogando com o poder, ocupando assim um espaço, interagindo e exercendo influência.

Ao contrário, portanto, do que se possa pensar inadvertidamente, parece haver um território cibernético, havendo desse modo uma delimitação política espacial – uma fronteira – no denominado ciberespaço, ainda que por ora não regulamentada, ou não tendo todas as suas fases de regulamentação percorridas formalmente.[9]

---

[9] *Definição*, *delimitação* e, por fim, *demarcação* são as fases formais exigidas pelo Direito Internacional Público para o estabelecimento de uma fronteira. "A linha fronteiriça só é de fato estabelecida quando a demarcação se processa. 'De fato estabelecida' significa não estar mais sujeita à contestação por parte de um dos Estados que tivessem essa fronteira em comum. Pela demarcação, elimina-se não um conflito geral, mas um conflito do qual a fronteira pudesse ser o pretexto" (RAFFESTIN, 1993; MAGNOLI, 1997, p. 240).

No ambiente cibernético do globo, os Estados definem seus territórios "nitidamente", isto é, apropriam-se de um espaço comum (*global common*) por meio do poder. Como exemplos imediatos, mas não únicos, tem-se os domínios dos sítios ".br"; ".us"; ".uk"; ".it";..., que indicam perfeitamente os respectivos territórios.

Ainda nesse sentido, os Estados Unidos delimitaram não só o território de atuação do seu poder, como, internamente, distribuíram competências e atribuições acerca de cada domínio: o ".mil" ficou sob o encargo do comando combatente (USCYBERCOM), enquanto os ".gov" e ".com" foram atribuídos ao Departament of Homeland Security e às empresas privadas, respectivamente (CLARKE, 2010; ZUCCARO, 2011, p. 64), ao que também segue Oliveira (2011, p. 116-118) quanto às atribuições dos órgãos e das agências norte-americanos. A estrutura montada e que funciona nesse ambiente também sofre influência do poder. A segurança dos *backbones*, dos *data centers*, dos *firewalls*[10] e demais elementos de filtragem e da hospedagem de sítios são alguns dos exemplos de que há "nitidamente" um exercício de poder no espaço cibernético, portanto há um território e, por conseguinte, sua respectiva fronteira.

Ocorre que, diferentemente das fronteiras delimitadas até então (terrestre, marítima, aérea), todas perceptíveis, incluindo-se, de certo modo, o limite extra-atmosférico, uma nova fronteira desafia homens e Estados devido à sua virtualidade, velocidade, versatilidade, flexibilidade, ambiguidade e, porque não dizer, "volatilidade".

O fluxo que "navega" por essa fronteira não é tão perceptível – pelo menos a olho nu e nem por equipamentos como luneta, binóculo, radar, etc. –, eis que o que flui nessa rede são, sobretudo, informações por meio de caracteres simbólicos dentro de pacotes[11] que, muitas vezes, fogem da imediata apreensão e compreensão. A delimitação de poder e de responsabilidades no espaço cibernético torna-se, doravante, a meta perseguida visando à garantia, sobretudo, da segurança, da harmonia e da paz, seja no ambiente interno seja no internacional.

---

[10] Em uma rede de computadores, *backbone* designa o esquema de ligações/conexões centrais de um sistema mais amplo, tipicamente de elevado desempenho. Dentro de um sistema de capilaridade global, como a internet, há uma hierarquia, uma escala dessas ligações/conexões: a intercontinental, a internacional e a nacional, alcançando as empresas de telecomunicações, que representam, apenas, a periferia do *backbone* nacional. *Data centers* – centros de processamento e de armazenamento de dados. *Firewalls* – filtros de "pacotes" de informações.

[11] Termo que nessa área científica indica um grupo de informações sendo transportadas unitariamente.

Nesse novo cenário, os conceitos geográficos de rede, de ponto e de "nós", outrora estudados nos espaços terrestre, marítimo e aéreo, serão de suma importância. Sua aplicação guiará os Estados e os Organismos Internacionais reguladores do direito na formulação dos limites do espaço cibernético, ou melhor, do seu território. Se antes já existiam formas de controle e de monitoramento para as fronteiras tradicionais, nessa "nova" os contornos não se mostram muito claros nem precisos. Entretanto, é certo que essa "nova fronteira" não existe de hoje.

### 2.1.1 Da "fronteira-zona" à "fronteira-ponto"

Como um dos fatores que provocaram a corrida por esse "novo" espaço encontra-se a internet: a instalação e a operação da rede mundial de computadores na escala global. Outro fator como consequência desse anterior é caracterizado pelo exponencial aumento do número de pessoas que passaram a ter acesso a esse meio e que vem, portanto, ocasionando uma "pressão" nesse espaço. Meira Mattos (2011[1977]) já apontava para esse fenômeno e seus possíveis reflexos ainda nos idos da década de 1970, denominando-o "*cibernetização*":

> O grau de cibernetização indica, atualmente, o padrão tecnológico da sociedade. As atividades dos grandes complexos empresariais ou educacionais estão relacionadas, hoje, com os computadores, cujas memórias realizam cálculos […]. Os números – 70 mil computadores nos EUA e 1.500 no Brasil – revelam o profundo gap, em termos de avanço tecnológico entre ambos os países (MEIRA MATTOS, 2011[1977], p. 310).

Esse processo de pressionamento assemelha-se bastante ao que deu origem à construção das fronteiras do espaço terrestre. Para ilustrá-la, também é Meira Mattos (1990) quem faz um resumo histórico sobre a Teoria das Fronteiras, no qual agora pode ser acrescentado mais um estágio, buscando representar o que se entende como uma nova fase dessa teoria, aplicada também ao ciberespaço, simultaneamente uma rede e um território, desde sua origem.

**Quadro 2. Resumo histórico – evolução das fronteiras e proposta**

| Fases/estágios | | Descrição |
|---|---|---|
| 1º | Vazios de ecúmene | • característico do mundo antigo, pouco povoado, quando os núcleos geo -históricos eram separados por enormes vazios demográficos; |
| 2º | Largas zonas inocupadas ou fracamente ocupadas | • estas zonas não abrigavam nenhum p oder político capaz de perturbar os interesses dos núcleos geo -históricos de que eram separadores; |
| 3º | Faixas relativamente estreitas, chamadas *fronteiras-faixa* | • nas áreas em que o povoamento dos países limítrofes não chega a pressionar um sobre o outro; |
| 4º | *Fronteira-linha*, estabelecida sob critérios vários (natural, artificial, astronômica, étnica) | • nas áreas em que a densidade populacional colocou em contato permanente o *interesse* das partes; |
| 5º | *Fronteira-ponto*, acompanhando o atual estágio tecnológico | • no ciberespaço, em sua estrutura física e/ou na imaterial, em que os interesses, por meio do fluxo de informações, podem colidir e causar danos a "pontos" escolhidos no território ou fora deste. Selecionam-se "*nós*" da rede e " *pacotes*" de informação que por esta trafegam. |

Fonte: adaptado de MEIRA MATTOS (1990, p. 17)[12]

Se se observar mais atentamente, além da *pressão demográfica* (MEIRA MATTOS, 1990) e da *centralização do poder pelo Estado* (GIDDENS, 2001), outro fator é responsável pela evolução das fases ou estágios das fronteiras: *o fator tecnológico*. À medida que se desenvolveram instrumentos que capacitaram um maior poder de monitoramento dos espaços, por meio do controle e do armazenamento das informações, mais nítida tornava-se sua delimitação, passando-se de uma forma de zona para a de faixa até chegar à de uma linha.

Acredita-se que, no atual estágio tecnológico, os Estados são capazes de delimitar seus interesses à escala de um "ponto", alcançando-se, assim, a fase ou o estágio da "*fronteira-ponto*", como um reflexo da trajetória histórica da capacidade de monitoramento e controle do sistema de Estados, caracterizando-se, dessa forma, a 5ª fase ou estágio da evolução das fronteiras.

[12] O 5º estágio está sendo proposto por nós.

A *fronteira*, nessa visada, passa a ser *ponto* (*fronteira-ponto*) não simplesmente pelo objeto a ser defendido, pois isso já ocorria nas outras dimensões que não a cibernética, como no caso dos castelos, das fortalezas, dos fortes, de cidades, portos, estreitos e ilhas, ainda na Idade Média (MEIRA MATTOS, 1990; RAFFESTIN, 1993; NYE, 2012; BUZAN; HANSEN, 2012) ou pelos Estados tradicionais (GIDDENS, 2001, p. 67-86). Nem também se está referindo à fronteira cibernética (*cyber boundary*) indicada por Clarke e Knake (2010) em seu glossário; nem ao *ponto* que esses autores indicam dentro dessa fronteira. Para eles, *fronteira cibernética* é empregada no sentido do limite entre o mundo *cyber* e o cinético, e o *ponto* diz respeito ao momento em que o comandante deverá decidir se (e como) passar de uma guerra puramente cibernética para uma envolvendo forças convencionais ou com armas cinéticas.

Como um dos resultados desta investigação científica, tem-se o *ponto*, ou melhor, a "*fronteira-ponto*", como reflexo de uma maior capacidade de controle das informações e de monitoramento, de maior precisão e velocidade de tomada de decisão entre o sensoriamento (detecção, vigilância), o processamento e a atuação (D-P-A), os quais correspondem à (ao): *detecção* – obtenção de informação sobre possíveis ameaças; *processamento* – trabalho da informação com vistas à tomada de decisão e implementação; e *atuação* – implementação da decisão e neutralização da ameaça (AMARANTE, 2010, p. 4-7).

Esses pontos, a título de exemplo, significam: 1) as informações digitalizadas em seus "pacotes" transitando por uma rede, localizada dentro ou fora do território terrestre (pelos *backbones* e cabos, pelas ondas *hertz* e fibra ótica), sendo processadas ou armazenadas em um computador (*datacenter*) (ativos da informação[13]); 2) os "nós", isto é, os pontos de conexão da rede pelos quais trafegam esses fluxos ("pacotes"); e 3) as estruturas estratégicas (infraestruturas críticas) com interesses vitais para o Estado. Este último caracteriza o "*extraespaço*", enquanto os dois primeiros correspondem ao "*intraespaço*" ou ao "*ciberespaço considerado em si mesmo*".

[13] Ativos de informação – meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso (BRASIL, 2010).

No caso das informações e de seus "pacotes", a abstração contida no princípio do direito sobre a extraterritorialidade diz respeito, por exemplo, a hipóteses em que, mesmo não estando situadas no território terrestre, no mar territorial ou no espaço aéreo do país, pessoas ou coisas são salvaguardadas. Como origem desse postulado, pode ser citada a obra de Hans Kelsen (apud DALLARI, 1995, p. 74-76), a partir do momento em que esse autor desvincula o objeto de interesse do Estado do seu *locus* de atuação de poder – seu território. Assim sendo, em alguns casos a personalidade jurídica do Estado fica assegurada juridicamente para o "além terra": o "*território-competência*".

O resultado dessa construção teórica pode ser visto, de forma exemplificativa e sintetizada, no artigo 7º do Código Penal Brasileiro, quando ficam submetidos à legislação brasileira, embora cometidos no estrangeiro, crimes contra o presidente da República, o patrimônio ou a fé pública da União e demais entes federativos. Além disso, encontram-se sob essa proteção as empresas públicas, as sociedades de economia mista, as autarquias ou as fundações instituídas pelo poder público e a própria administração pública. Em todos esses, a finalidade perseguida é a salvaguarda da personalidade jurídica estatal e seus interesses, isto é, a proteção da instituição, mesmo fora de seu território físico.

No mais, objetos ou coisas também são colocados sob essa condição, embora com algumas nuanças (extraterritorialidade condicionada), como é o caso de aeronaves e de embarcações brasileiras, mercantes ou privadas, quando em território estrangeiro. Essa é uma das soluções que o sistema de Estados pode adotar a fim de determinar fronteiras no espaço cibernético.

É dessa forma que se pode concluir que no espaço cibernético, considerado em si – em muitas ocasiões imperceptível, com estrutura micro ou nano –, vem ocorrendo uma territorialização, uma vez que a disputa pelo controle de informações e da possibilidade de seu fluxo vem sendo objeto de poder. Ao mesmo tempo, também se infere que há uma (re)territorialização ocorrendo nos demais domínios espaciais, fruto das possibilidades advindas desse recurso.

Como exemplos localizados no domínio terrestre, as usinas hidrelétricas e as centrais de distribuição de energia, as estações de tratamento de água e o setor financeiro, considerados essenciais para o Estado e para seu sistema, são selecionados a fim de uma atenção maior no que tange à segurança e à defesa.

Mais uma vez, portanto, a delimitação dessa fronteira, de forma clara e precisa, torna-se crucial para a manutenção da harmonia, da segurança e da paz. Com as pressões exercidas nessa nova dimensão e a busca pelo seu empoderamento, há a transformação do conceito *espaço* para o de *território*, vez que, intrinsecamente, circula e se confronta poder.

Como mais um aspecto, a informação, em si, não tem valor caso não se tenha capacidade de processá-la ou de torná-la inteligível, em certo tempo, para determinados fins. Assim, o conhecimento mais detalhado das características dessa fronteira torna-se primordial, pois proporciona condições de defender tanto as informações quanto alguns pontos de uma rede e de um país.

### 2.1.2 Fronteira cibernética: classificação, realidade e representação

De forma semelhante aos estágios registrados, a teoria de Meira Mattos, com base no estudo de alguns dos principais pensadores geopolíticos, permitiu a classificação das fronteiras segundo vários critérios. Partindo dessa classificação, essa "nova" fronteira, objeto de nosso estudo, pode ser tida como *artificial*, *ocupada*, *esboçada*, *planejada ou de construção* e *antropogeográfica*. Segue descrição correspondente a cada uma dessas características.

Quanto a ser *artificial*, esta se refere à natureza da fronteira e ao ambiente criado e manipulado pelo homem; *ocupada*, devido ao grau de ocupação, dado pelo fluxo material ou imaterial, mas com reflexos no mundo físico que a perpassa; *esboçada*, quanto ao grau de evolução (BRUNHES; VALLAUX apud MEIRA MATTOS, 1990, p. 31), pois ainda não se impõe uma demarcação clara. No entanto, aqui cabe um destaque: pelo que constatamos ao longo da pesquisa, devido às pressões exercidas ultimamente nesse espaço, podemos enquadrar essa fronteira na transição entre a forma esboçada e a de fronteira *viva* ou *de tensão* em face do confronto real e constante de interesses.

Com relação à fronteira *planejada ou de construção*, consoante Rudolf Kjéllen (apud MEIRA MATTOS, 1990, p. 32), isso se dá devido ao sentido de obedecer à finalidade e ao traçado dado pelo homem. É classificada como *antropogeográfica* porque obedece ao critério realístico ou existente, na concepção de Whitemore e Boggs (apud MEIRA MATTOS, 1990, p. 33), devido às características do fluxo (linguístico, cultural, estratégico ou militar). É por possuir qualidades intrínsecas à fronteira do tipo *antropogeográfica* que a delimitação da fronteira cibernética, em si, torna-se muito complexa e altamente conflitante.

Meira Mattos (1990, p. 34) afirma que fisicamente é até mesmo impossível o estabelecimento de fronteira quando esta é do tipo antropogeográfica. Todavia, ressalva esse autor que as fronteiras, mesmo as naturais – que até hoje são as mais claramente delimitadas –, nem sempre o são fisicamente. Grande parte, por sinal, ocorre por convenção ou acordo entre as partes (convencionalidade). É como afirma Lacoste (1989): as fronteiras são delimitações políticas. Foi o que ocorreu inicialmente com a terrestre, a marítima e a aérea.

Em relação à marítima, este tipo de fronteira foi inicialmente considerado por F. Ratzel (apud MEIRA MATTOS, 1990, p. 37) "a fronteira ideal", pois separaria, protegeria, isolaria ou uniria de acordo com a conveniência do Estado. Quanto à aérea, elaborada após o desenvolvimento da aviação (pós-I GM), o escritor francês Victor Hugo chegou a escrever para seu conterrâneo, o balonista Félix Nadar, afirmando que, além do fim das guerras, o uso do espaço aéreo pelo avião ocasionaria a "imediata, instantânea, universal e perpétua abolição das fronteiras" (ISAAC, 2001, p. 214). Em ambos os casos, contudo, isso parece que não se concretizou.

O desafio, então, no que diz respeito à fronteira cibernética passa a ser a compreensão de que essa fronteira não é em forma de zona ("*fronteira-zona*"), nem de faixa ("*fronteira-faixa*"), nem de linha ("*fronteira-linha*"), como ocorre com o espaço geográfico tradicional, natural. A delimitação de um território cibernético se dá sob outra lógica, por sinal obedecendo às próprias características desse ambiente, em que território e rede perfazem originalmente um binômio de coexistência.

A fronteira cibernética, por conseguinte, obedece à forma de "pontos" ("nós") ou "pacotes" de informações eleitos pelos Estados devido ao seu grau de interesse – sistemas de defesa, infraestruturas críticas ou estruturas estratégicas e a informação em si são alguns dos exemplos. Com isso, nesse ambiente, a fronteira apresenta-se sob a forma de "*fronteira-ponto*", um prosseguimento contínuo, embora com certas interrupções, que acompanha o contexto histórico da formação do sistema internacional pautado no princípio da territorialidade estatal: da "*fronteira-zona*" (faixa) dos Estados tradicionais às "*linhas*" do Estado moderno e em grande parte do atual sistema de Estados-Nação, alcançando no (e com o) espaço cibernético a meticulosidade da "*fronteira-ponto*" em face da capacidade inovadora das ferramentas de TIC à disposição, que foge ao visível, que é aparentemente virtual, mas de grande reflexo no mundo real.

Esse território cibernético existe e coexiste com os demais domínios tradicionais, e já é, inclusive, mapeado, isto é, objeto de representação e, por conseguinte, de projeção de poder. Dessa forma, esse território é transformado materialmente em objeto de apreensão pela mente humana, ultrapassando a ideia de mera metafísica ou de coisa intangível. Esse território é real e também palco de intensas disputas de (e pelo) poder, com fulcro no seu controle, no seu domínio. É desse modo que enxerga também Vesentini, ao apresentar a obra de Yves Lacoste (1989) que aborda a relação de uma representação (um mapa) com o poder:

> Assim como o grande pensador de Iena proclamava que tudo que é real é racional e tudo que é racional é real, pode-se dizer que para Lacoste o "real", o espaço geográfico, é tão-somente aquilo que pode ser mapeado, colocado sobre a carta, delimitado portanto com precisão sobre o terreno e definido em termos de escala cartográfica (VESENTINI, 1988).[14]

[14] Apresentação da obra de Yves Lacoste (1976), publicada no Brasil em 1989.

Para garantir o funcionamento desse sistema à sombra do conflito, Clarke e Knake (2010) apontam para a necessidade, em face dessa composição do domínio cibernético, de se estabelecer prioritariamente a defesa com base em uma tríade – *Defensive Triad Strategy* – que focaria três setores bem definidos:

1) o que envolve os *backbones*, e pelo qual o governo e algumas empresas estipulariam uma atenção especial à segurança. Dentre as empresas, no caso norte-americano destacam-se a AT&T, a Verizon, a Level 3, a Qwest e a Sprint, responsáveis por grande parte da estrutura de fibra ótica usada pela internet no interior dos EUA e no ambiente submarino ao longo do globo;

2) o que corresponde à garantia de uma rede de energia segura, tendo em vista a dependência de energia elétrica para ocorrer o fluxo de informações no (e pelo) ciberespaço; e

3) o que diz respeito à própria defesa, constituindo-se na elaboração de medidas de defesa e de ataque a partir do Departamento de Defesa (*DoD*) daquele Estado. Envolve, entre outros, as redes do próprio *DoD* e os sistemas de controle de efetivos e de armas.

Quanto a este último setor, pode ser vista a preocupação do Brasil com o funcionamento de seu Sistema Militar de Comando e Controle (SISMC[2]), materializada em projetos como o CDCiber, o SisFron, o Sistema de Gerenciamento da Amazônia Azul (SisGAAz) e o Sistema de Defesa Aeroespacial (Sisdabra) e as novas atribuições do Centro Integrado de Telemática do Exército (Citex).

No tocante aos outros dois setores dessa tríade proposta por Clarke e Knake (2010), visualiza-se exatamente a preocupação do domínio cibernético, ora tido como *espaço em si mesmo* (*backbone*, por exemplo), ora como recurso do poder, quando os autores citados demonstram a preocupação com uma estrutura estratégica para o Estado: a estrutura energética.

Ainda quanto à importância desses dois setores – informação e energia e sua interligação –, parece que esses autores estão em consonância com o que expôs Raffestin (1993, p. 53-54) com relação ao poder e a suas fontes: "Sendo toda relação um lugar de poder, isso significa que o poder está ligado muito intimamente à manipulação dos fluxos que atravessam e desligam a relação, a saber: a energia e a informação".

A preocupação dos Estados não só com o setor cibernético em si mesmo, mas, e principalmente, com a interligação e a dependência dos outros setores a partir deste é bem plausível, pois os danos causados a partir do ciberespaço podem transbordar para outros, como no caso das estruturas estratégicas, o que inclui a energética.

Concretamente, embora não seja especificamente voltada para questões de defesa (relação entre Estados), temos em vigor, desde 2004, a Convenção de Budapeste ou a Convenção sobre o Cibercrime, que conta com 43 signatários, sendo apenas 12 o número de Estados que a ratificaram. Contudo, em síntese, essa tentativa de normatização não possui mecanismos de coação bem definidos, isto é, não possui "dentes" (*tothless*). Como exemplo, em face das características inerentes a esse domínio, a Convenção não menciona nada a respeito da perseguição de um criminoso nem sobre sua punição. Isso, portanto, termina por esvaziar muito sua finalidade.

Entretanto, em face dos últimos acontecimentos que envolveram o ciberespaço e as possibilidades que a cibernética vem proporcionando, a normatização do sistema internacional cada vez mais se torna imprescindível, pois em muitos desses casos a utilização desse novo domínio vem ocorrendo realmente na (e para) a guerra.

## 3 Considerações finais

A internet realmente mudou os parâmetros da ação humana, como afirmou o ministro Celso Amorim. Espaço virtual e real intercambiam-se constantemente. Assim, a necessidade de se pensar essa nova dimensão espacial como recurso de poder se torna essencial.

É a partir dessa forma de "saber pensar", envolvendo categorias de análise e conceitos da geopolítica, que as políticas públicas poderão ser formuladas, implantadas, monitoradas e avaliadas com maior probabilidade de êxito.

Como consequência dessa percepção é que se tem hoje projetos que tratam do ciberespaço considerado ora em si mesmo, como os programas, os *softwares*, os antivírus, etc., quanto como projetos que se utilizam da cibernética como mais um recurso à disposição do poder. É nessa visada que vêm surgindo pelo globo, por exemplo, sistemas de monitoramento do espaço terrestre, do marítimo, do aeroespacial.

Derivada dessas possibilidades é que surge a demanda por delimitação, não com o sentido de separação ou de isolamento, e sim pelo contrário, para normatizar responsabilidades no uso dessa "nova" dimensão espacial a fim de se evitar o conflito e até mesmo a guerra.

A delimitação do ciberespaço, em face de suas características, não obedecerá à forma de linha, nem de faixa, nem de zona, mas sim de um ponto, a "*fronteira-ponto*", tendo em vista a atual capacidade do sistema de Estados.

Considerando o ciberespaço em si, esse ponto materializa-se na informação ou no "pacote" de informações e pelos "nós" de uma rede. Ao ser tratada como recurso, a cibernética é capaz de selecionar pontos em outras dimensões do espaço para uma (re)territorialização.

Saber pensar o espaço, como disse Lacoste (1989), para melhor se organizar, para melhor combater, agora pode ser aplicado ao domínio cibernético em um arcabouço geopolítico e jurídico.

## REFERÊNCIAS

ALMEIDA, José Eduardo P. A tendência mundial para a defesa cibernética. *In:* BARROS, Otávio S. R.; GOMES, Ulisses M. G.; FREITAS, Whitney L. de. (Org.). **Desafios estratégicos para a segurança e defesa cibernética**. Brasília: Secretaria de Assuntos Estratégicos, 2011. p. 79-102.

AMARANTE, José Carlos A. do. A batalha automatizada: um sonho exequível? **Cadernos de Estudos Estratégicos**, Rio de Janeiro, n. 9, p. 3-18, Centro de Estudos Estratégicos da Escola Superior de Guerra, jul. 2010.

AMORIM, Celso. Aspectos da defesa cibernética. In: SEMINÁRIO DE DEFESA CIBERNÉTICA, 3., Brasília, 2012. **Palavras do ministro da Defesa**... Brasília: MD, 2012. Disponível em: <https://www.defesa.gov.br/arquivos/2012/Pronunciamentos/Ministro_defesa/discurso_seminario_defesa_cibernetica_out_2012.pdf>. Acesso em: 20/11/2012.

BRASIL. **Glossário das Forças Armadas**. MD35-G-01. 4. ed. Brasília: Ministério da Defesa, 2007. Disponível em: <https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md35_g_01_glossario_fa_4aed2007.pdf>. Acesso em: 20/06/2013.

_____. **Guia de Referência para a Segurança das Infraestruturas Críticas da Informação**. v. 01. Brasília: Gabinete de Segurança Institucional da Presidência da República, nov. 2010. Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf>. Acesso em 08/08/2011.

BUZAN, Barry; HANSEN, Lene. **A Evolução dos Estudos de Segurança Internacional**. São Paulo: Editora Unesp, 2012.

CANONGIA, Claudia; MANDARINO JÚNIOR, Raphael. Segurança cibernética: o desafio da nova sociedade da informação. **Parcerias Estratégicas** – Revista do Centro de Gestão e Estudos Estratégicos do Ministério da Ciência e da Tecnologia, Brasília, v. 14, n. 29, p. 21-46, 2009.

*CLARKE, Richard; KNAKE, Robert.* ***Cyber war****:* the next threat to national security and what to do about it. *New York: CCCO, 2010.*

*CORRÊA, Alexandre José. Operações de informação: um antigo conceito sob um novo paradigma.* ***Coleção Meira Mattos****, Rio de Janeiro, v. 3, n. 27, 2012. Disponível em:* <http://www.eceme.ensino.eb.br/meiramattos/index.php/RMM/issue/view/14/showToc>*. Acesso em: 13/01/2013.*

DALLARI, Dalmo de Abreu. **Elementos de teoria geral do Estado**. 19. ed. atual. São Paulo: Saraiva, 1995.

DEIBERT, Ron. Distributed security as cyber strategy: outlining a comprehensive approach for Canada in cyberspace. **Calgary**: Canadian Defense & Foreign Affairs Institute, August, 2012. Disponível em: <http://ebookbrowse.com/distributed-security-as-cyber-strategy-pdf-d380969236>. Acesso em: 10/12/2012.

FERREIRA, Kelly de Souza. **China e a Ásia Central**: petróleo, segurança e os Estados Unidos. Campinas, 2012. 99f. Dissertação (Mestrado em Relações Internacionais) – Universidade Estadual de Campinas.

GIDDENS, Anthony. **O Estado-nação e a violência**. São Paulo: Edusp, 2001.

HASBAERT, Rogério. **Territórios Alternativos**. Niterói: EdUFF; São Paulo: Contexto, 2002.

HUNTINGTON, Samuel P. **O soldado e o Estado**: teoria e política das relações entre civis e militares. Rio de Janeiro: Biblioteca do Exército, 1996.

ISAAC, David M. Vozes do azul: teóricos do poder aéreo. In: PARET, Peter. **Construtores da estratégia moderna**: de Maquiavel à era nuclear. v. 2. Rio de Janeiro: Biblioteca do Exército, 2001. p. 211-242.

*LACOSTE, Yves. **A geografia**: isso serve, em primeiro lugar, para fazer a guerra. 3. ed. Campinas: Papirus, 1989. Disponível em:* <http://www.geoideias.com.br/geo/images/livros/a%20geografiaIves%20Lacoste.pdf> *Acesso em: 23/07/2012.*

KAPLAN, Marcos. **Formação do Estado nacional na América Latina**. Rio de Janeiro: Eldorado, 1974.

*LÉVY, Pierre. **Cibercultura**. São Paulo: Ed. 34, 1999.*

MAGNOLI, Demétrio. **O corpo da pátria**: imaginação geográfica e política externa no Brasil (1808-1912). São Paulo: Editora da Universidade Estadual Paulista: Moderna, 1997.

MANDARINO JÚNIOR, Raphael. Reflexões sobre segurança e defesa cibernética. *In:* BARROS, Otávio S. R.; GOMES, Ulisses M. G.; FREITAS, Whitney L. de. (Org.). **Desafios estratégicos para a segurança e defesa cibernética**. Brasília: Secretaria de Assuntos Estratégicos, 2011. p. 105-128.

MEIRA MATTOS, Carlos de. **Geopolítica e teoria de fronteiras**: fronteiras do Brasil. Rio de Janeiro: Biblioteca do Exército, 1990.

_____. A geopolítica e as projeções de poder. **Geopolítica**. Vol. I. Rio de Janeiro: Editora FGV, 2011[1977]. p. 305-312.

MORAN, Daniel. Geography and strategy. In: BAYLIS, J.; WIRTZ, J. J.; GRAY, C. S. **Strategy in the contemorary world**: an introduction to strategic studies. 3. ed. New York: Oxford University Press, 2010. p. 124-140.

MOREIRA, Marcílio Marques. Karl Deutsch, a Política e a Cibernética. In: **Deutsch na UNB**: conferência, comentários e debates de um simpósio internacional realizado de 11 a 15 de agosto de 1980. Brasília: Editora da UNB, 1980.

*NYE, Joseph S. **O futuro do poder**. São Paulo: Benvirá, 2012.*

*OLIVEIRA, João Roberto de. Sistema de segurança e defesa cibernética nacional: abordagem com foco nas atividades relacionadas à defesa nacional. In:* BARROS, Otávio S. R.; GOMES, Ulisses M. G.; FREITAS, Whitney L. de. (Org.). **Desafios estratégicos para a segurança e defesa cibernética**. Brasília: Secretaria de Assuntos Estratégicos, 2011. p. 105-128.

_____. ***Fronteira cibernética***. [mensagem pessoal]. Mensagem recebida por <wbfneto@bol.com.br> em 02/10/2012.

POSEN, Barry R. Command of the commons: The Military Foundation of U.S. Hegemony. **International Security**, v. 28, n. 1, p. 5-46, summer 2003. Disponível em: <http://belfercenter.ksg.harvard.edu/files/posen_summer_2003.pdf>. Acesso em: 20/09/2012.

RAFFESTIN, Claude. **Por uma geografia do poder**. São Paulo: Ática, 1993.

REVERON, Derek S. **Cyberspace and national security**: threats, opportunities and power in a virtual world. Washington D. C.: Georgetown University Press, 2012.

RODRIGUES, Alexandre Reis. Portugal e o espaço estratégico de interesse. **Jornal de Defesa e Relações Internacionais**. **Revista Segurança e Defesa**, Loures, Diário de Bordo Editores, 2012. Disponível em: <http://data base e.jornaldefesa.pt/políticas de defesa portugal JDRI%2009%20221112%0Portugal%20%20%20%espa%C3%A7o%20 estrat%C3%A9gico%20de%20interesse.pdf> Acesso em: 27jan.2012.

SANTOS, José Carlos dos. General José Carlos dos Santos: "Podemos recrutar hackers". [Brasília]. **Revista Época**, 15 jul. 2011. Entrevista concedida a Leandro Loyola. Disponível em: <http://revistaepoca.globo.com/Revista/Epoca/0,,EMI249428-15223,00-GENERAL+JOSE+CARLOS+DOS+SANTOS+PODEMOS+RECRUTAR+HACKERS.html>. Acesso em: 20/07/2011.

SAQUET, Marcos Aurelio. **Abordagens e concepções sobre território**. São Paulo: Expressão Popular, 2007.

SILVEIRA, Fernando Malburg da. Cyberwarfare: a nova dimensão da guerra. In: **Revista do Clube Naval**, ano 119, n. 360, out./nov./dez., 2011.

THE ECONOMIST. Cyberwar: war in the fifty domain. 1 jul. 2010. Disponível em: <http://www.economist.com/node/16478792>. Acesso em: 20/06/2011.

VENTRE, Daniel. Ciberguerra. In: XIX Curso Internacional de Defensa, 2011. **Seguridad global y potências emergentes em un mundo multipolar**. Zaragoza: Imprenta Ministerio de Defensa, 2012. p. 32-45.

VESENTINI, José William. Apresentação. In: LACOSTE, Y. **A geografia**: isso serve, em primeiro lugar, para fazer a guerra. Campinas: Papirus, 1988. p. 7-13.

*WIENER, Norbert.* ***Cibernética e sociedade****: o uso humano de sêres humanos. 4. ed. São Paulo: Cultrix, 1973[1954].*

*ZUCCARO, Paulo Martino.* Tendência global em segurança e defesa cibernética: reflexões sobre a proteção dos interesses brasileiros no ciberespaço. In: BARROS, Otávio S. R.; GOMES, Ulisses M. G.; FREITAS, Whitney L. de. (Org.). **Desafios estratégicos para a segurança e defesa cibernética**. Brasília: Secretaria de Assuntos Estratégicos, 2011. p. 49-77.

RECEBIDO - 29/11/2013
APROVADO - 07/04/2014