O dilema da fronteira virtual: Quando os Estados se tornam construtores de ciberfronteiras

Daniel Ventre
Centre de Recherches Sociologiques sur le Droit et les Institutions Pénales, Paris, França

Este artigo discute o "dilema das fronteiras virtuais". É uma reflexão sobre o conceito de fronteira e sua transposição para o ciberespaço. Trata mais especificamente da construção, pelo Estado, de ciberfronteiras ou fronteiras virtuais, em resposta aos desafios securitários específicos impostos pelas redes. Depois de propor algumas definições do ciberespaço e da ciberfronteira, serão abordadas as razões e modalidades de construção de fronteiras virtuais e, em seguida, os seus efeitos na segurança nacional e internacional. O contexto brasileiro ilustra a discussão.

Palavras-chave: cibersegurança, fronteiras virtuais, ciberespaço, guerra de informação, Brasil

Virtual Border Dilemmas: When States Become Cyber Border Builders introduces the concept of 'virtual border dilemma', reflecting upon the concept of border and its transposition into cyberspace. It deals more particularly with the construction of cyber or virtual borders by the state in response to specific security challenges posed by the network. After proposing some definitions of cyberspace and cyber border, the article will focus on the reasons for, and modalities of, building virtual borders, followed by their effects on national and international security. The Brazilian context is used to illustrate the matter.

Keywords: cybersecurity, virtual frontiers, cyberspace, information warfare, Brazil

Introdução

Ao conectarem-se uns com os outros, ao criarem um mundo reticular, os Estados se tornaram interdependentes. Ao inervarem todos os setores de atividade, todas as ramificações da sociedade, com tecnologias informatizadas e redes de comunicação, as nações se tornaram totalmente dependentes do ciberespaço. As sociedades se encontram, portanto, em uma dupla relação, de dependência para com um sistema sociotécnico e de interdependência uns para com os outros.

O funcionamento desse sistema está condicionado à circulação, sem entraves, dos fluxos de dados. Mas se essa fluidez e essa interdependência estão entre os motores essenciais da integração das sociedades modernas ao sistema internacional contemporâneo, elas determinam, ao mesmo tempo, sua exposição a violências veiculadas pelas redes, praticamente inevitáveis. Os Estados sofrem tais violências sem ter condições de antecipá-las, de antevê-las, de enfrentá-las. Elas atingem o próprio seio de suas sociedades, alteram suas economias, sua vida política. Às vezes ameaçam os pontos nevrálgicos dos Estados, suas infraestruturas vitais, sem que eles consigam ativar suas defesas de modo eficaz, sem que consigam rebater, agir, reagir.

É como se os Estados fossem espoliados de grande parte de sua soberania, de seus poderes exclusivos, do domínio da segurança de seus próprios territórios. Na medida em que o ciberespaço não lhes oferece uma transposição precisa de suas fronteiras, os Estados ficam ainda mais fragilizados, pois não têm condições de delimitar estritamente seu território nesse espaço cibernético. Ora, sem essas referências tradicionais do território e da soberania, os Estados não podem exercer seus poderes, ativar suas defesas.

À imensidão da área de ataque – ou seja, do perímetro de vulnerabilidades –, à intensidade das violências cibernéticas, ao caráter furtivo dos ataques e dos agressores, à profundidade dos ataques nos seios das sociedades, à grande assimetria criada pelo meio – que dá aos agressores uma vantagem considerável –, os Estados parecem querer opor soluções soberanas, pressupondo, ainda que implicitamente, a existência ou o reconhecimento da existência de uma fronteira virtual. Ela seria definida como o conjunto de capacidades e poderes de fiscalização, filtragem, bloqueio, vigilância dos fluxos, em pontos que marcam a delimitação entre o interior e o exterior do território nacional.

Mas determinados Estados se valem também da ausência ou da transparência das fronteiras no ciberespaço. Ainda que sofram violências, eles também contribuem com elas e tiram vantagem dessa situação que lhes confere capacidades de exercer seu poder no âmbito internacional, lhes dá condições de projetar seu poder, de realizar operações a grande distância por meio das redes, de maneira anônima, mantendo a incerteza no que se refere à origem dos golpes dados. Para esse tipo de ação, os autores não têm nenhum interesse em tornar claramente delimitadas as fronteiras do Estado, nem em condicionar seu cruzamento a qualquer regra.

Formulamos a hipótese de que os Estados estão presos entre duas lógicas contrárias: por um lado, a obrigação de manter as redes conectadas ao resto do mundo para garantir a continuidade dos fluxos e preservar a integração ao sistema internacional, de modo a serem atores da globalização; por outro, a tentação de impor, à guisa de solução de cibersegurança, mas talvez, nesse caso, em detrimento da integração à rede mundial, o reconhecimento de suas fronteiras nacionais no ciberespaço, desenhando uma separação entre o que seria o território nacional e o exterior. É essa dupla tensão que opõe os interesses de segurança interna e os imperativos de integração com o mundo, quando o que está em jogo, sob o prisma do ciberespaço, é o que chamamos de "dilema das fronteiras virtuais". Seria necessário manter a ausência de fronteiras ou construí-las? Paradoxalmente, elas parecem ser necessárias, mas sua ausência é tão necessária quanto. Os próprios Estados são atores dessas novas formas de violência.

O artigo fará três perguntas: (a) Como definir as noções de ciberespaço, fronteira e fronteira virtual? (b) Quais são as razões capazes de levar os Estados a construírem ciberfronteiras? Um processo de securitização enfatiza a natureza das ameaças próprias ao

ciberespaço. Esse processo insiste no caráter transnacional das violências, que favorece a arquitetura reticular. (c) Como os Estados constroem fronteiras virtuais ou embriões de fronteiras? Uma vez que a erosão de sua soberania no ciberespaço se traduz pela liberdade de ação de que se beneficiam os atores da violência cibernética, os Estados concentram parte de seus esforços, em matéria de cibersegurança, na construção de delimitações territoriais. O direito é uma das principais ferramentas dessa construção, sobretudo quando outorga aos atores estatais poderes de filtragem e de vigilância dos fluxos. Mas eles também constroem suas delimitações quando se impõem na definição das regras de governança da internet, ou por meio da diplomacia.

A conclusão destacará os efeitos da construção de fronteiras virtuais sobre a organização do sistema internacional, sobretudo o da balcanização da internet.

Uma prévia: as definições do 'ciberespaço' e da 'ciberfronteira'

A noção de ciberespaço foi objeto de várias tentativas de definição ao longo das duas últimas décadas (KUEHL, 2009, pp. 24-42). Tomada inicialmente da literatura de ficção científica em que o ciberespaço é uma alucinação consensual (GIBSON, 1984), essa noção e todo um conjunto de formulações construídas em torno do prefixo "ciber" impuseram-se desde o início do século XXI no vocabulário industrial com os atores da cibersegurança, por exemplo, do ensino superior e da pesquisa com cursos de "segurança cibernética" e "defesa cibernética", mas também no discurso das administrações estatais, que publicam as estratégias nacionais de cibersegurança, e das forças de segurança e de defesa – lembremo-nos dos cibercomandos militares.

Um modelo de três dimensões é comumente usado para descrever o ciberespaço. Uma primeira camada é constituída pela arquitetura material, física, *hardware*; ela é feita pelo conjunto de computadores, calculadoras, cabos eletrônicos (*hardware layer*). Uma segunda camada, média, denominada software ou aplicativa, é constituída pelo conjunto de programas, códigos, dados e algoritmos que dão vida ao ciberespaço (*software layer*). E uma terceira camada, informacional, é a do sentido, das informações (*news*), dos conteúdos (*meatware layer*).

Pode ocorrer que outras sejam acrescidas ao modelo para completá-lo (camada operacional ou dimensão humana).

O ciberespaço também é chamado de novo campo – da mesma forma que a terra, o mar, o ar e o espaço: "Um domínio global no ambiente informacional que consiste em redes

interdependentes de infraestruturas de tecnologia da informação e dados residentes, incluindo a internet, redes de telecomunicações, sistemas informáticos e processadores e controladores incorporados" (DOD, 2018, p. 59).

Mas qualquer que seja a maneira pela qual se denomine o ciberespaço (arquitetura multidimensional, espaço ou campo), os atores da internet têm em comum o fato de considerá-lo um território, ou seja, de apreendê-lo como tal. O ciberespaço torna-se objeto de lutas; querem apropriar-se dele, dominá-lo, garantir liberdade de ação e dominação em seu âmbito, transpor ali sua soberania. Assim, o ciberespaço, sem ser um território no sentido estrito do termo, na definição de território de Yves Lacoste (2003), fica "submetido a um processo mental de territorialização" (*apud* DOUZET, DESFORFES e LIMONIER, 2014, pp. 173-178).

Qualquer território sobre o qual o Estado impõe sua soberania é delimitado por fronteiras. No ciberespaço, elas devem ser imaginadas, inventadas. Trata-se de construções, de representações. Podemos pensar que as fronteiras virtuais ou ciberfronteiras, como são designadas as fronteiras no ciberespaço, podem ser concebidas de maneira diferente em função de cada uma das camadas citadas acima.

O ciberespaço é geralmente descrito como uma vasta rede de transporte de dados digitais, sem fronteiras, onde a liberdade dos fluxos deve ser total. A ausência de fronteiras foi dada como uma obviedade, uma regra sem discussão: "As comunicações globais na internet levantam a questão das fronteiras no ciberespaço, onde não há limites físicos" (DEIRMENJIAN, 1999, pp. 407-413).

O ciberespaço ignoraria as fronteiras, pois seu funcionamento e sua própria essência teriam como fundamento, precisamente, essa transparência e fluidez. Na ideologia de seus precursores, nele não há o enquadramento formal das fronteiras estatais: "O ciberespaço não se limita às suas fronteiras" (BARLOW, 1996).

Muito cedo, no entanto, já desde os anos 1970-1980, os Estados instituíram, por meio de seu arcabouço jurídico nacional (que cuidava, então, de legislar sobre o tratamento dos dados de caráter pessoal, os ataques aos sistemas de informação, de sancionar o que ainda não passava de um balbuciamento da criminalidade informática), as bases de um corte territorial dessa rede planetária. A territorialidade do direito dos Estados vinha projetar nas redes, no ciberespaço, a arquitetura estatal do sistema internacional.

Foram as considerações securitárias que levaram a pensar no corte territorial do ciberespaço. Sua própria arquitetura (a primeira camada, física) presta-se facilmente a um fatiamento da rede bem próximo do corte do planeta em Estados: os cabos chegam e saem de pontos – instalações que conectam os cabos entre si entram e saem do território, criando uma relação entre a rede interna e o resto do mundo – que poderiam ser os "pontos-fronteiras",

equivalentes aos portos marítimos, aos aeroportos internacionais. Marcadores da separação entre os âmbitos interno e externo devem ser declinados para as outras camadas do ciberespaço.

A fronteira é, acima de tudo, um limite entre o que está dentro e o que está fora, entre duas regiões, dois Estados; sua etimologia remete à linha de frente militar, à ideia de defesa pelas armas. A linha nada mais é do que uma forma de fronteira. Conhecemos também a fronteira-ponto. Mas a fronteira também é definida relativamente à sua função: ela é o controle de fluxos humanos, de mercadorias, capitais e dados. Com a noção de "controle de fluxos", poderemos então pensar em declinar a ideia de ciberfronteira, que poderíamos definir da seguinte forma: lugar de exercício do poder de controle, de medida, de filtragem dos fluxos de dados, situado no interstício móvel, subjetivo, entre um ciberespaço nacional e o ciberespaço global.

Por que os Estados querem construir ciberfronteiras?

A dependência das sociedades dos sistemas informatizados em rede é a causa de sua extrema sensibilidade às violências que ocorrem no ciberespaço. A maneira de definir essa exposição aos riscos, de escolher seus aspectos mais ameaçadores, pode variar em função do lugar e do momento. No entanto, com base na modelização em três camadas do ciberespaço, é possível distribuir as múltiplas variantes dessas ameaças.

Na primeira camada, material, as violências podem ser exercidas contra as infraestruturas, fisicamente (cabos cortados, computadores destruídos). Tais ataques eram frequentes na era do telégrafo. Eles ainda acontecem – piratas no mar ainda cortam cabos para revendê-los e cabos também são cortados em tempos de guerra.

A dimensão do software, no cerne do ciberespaço, lugar de algoritmos e softwares, é também o lugar dos hackers, que manipulam códigos, furtam dados e sabotam o funcionamento dos sistemas. A amplidão do fenômeno hoje é tal que é ilusório pretender fornecer uma medida exata dele, tanto no que se refere à quantidade de ataques, quanto a seus efeitos e custos. Essas violências ultrapassaram, em muito, a violência da criminalidade comum, mas normas de alcance internacional ainda são necessárias para avaliar com precisão a natureza do fenômeno, que assume múltiplas formas.

Os hackers podem ser classificados em várias categorias, sejam eles atores estatais ou não estatais, que persigam objetivos tradicionais do crime organizado ou tenham ambições mais políticas, que usem modos operatórios discretos ou visíveis. Nessa camada encontraremos, portanto, todas as operações criminosas em pequena e grande escala, de *phishing*, por meio de ataques de negação de serviço que paralisam servidores; operações estatais de espionagem cujo

alvo são empresas ou Estados, ou, pelo contrário, de grande amplitude (operações Red October, GhostNet e Dark Caracal); programas de interceptação em massa de dados (programas da National Security Agency [NSA]) de empresas, Estados e cidadãos do mundo inteiro; operações de sabotagem (*Stuxnet*)[1]; ataques em massa contra algum Estado (na Estônia em 2007); propagação de *malwares* em grande escala (WannaCry, NetPetya, KediRAT e Dyn cyberattack).

A dimensão informacional, por sua vez, é o lugar da guerra da informação, das operações de informação: manipular a informação, influenciar, controlar as mídias, censurar, bloquear, são todas práticas ancestrais que o desenvolvimento planetário das redes e o nível de penetração, em profundidade, nas sociedades permitiram redefinir. Situam-se nesse nível as tentativas de manipulação das opiniões em período eleitoral, as operações de desconfiguração dos websites que, ainda que agindo por meio da pirataria na camada de software, fazem todo sentido se considerarmos os conteúdos das mensagens veiculadas.

Para os autores das violências cibernéticas, a ausência de fronteiras virtuais tem vários efeitos imediatos: desinibição, impunidade, golpes a distância, invisibilidade, anonimato, velocidade, assimetria.

Os fluxos livres veicularam um conjunto de violências que os Estados não têm condições de bloquear antes que produzam seus efeitos no território nacional. O ciberespaço, tal como é concebido, põe em dúvida a capacidade que os Estados têm de garantir a segurança em seus territórios, a possibilidade de se protegerem e de se defenderem também, pois as respostas ficam suspensas uma vez atribuídas as responsabilidades, e dependem das possibilidades que o direito internacional oferece em termos de represálias, de contra-ataque (*hack-back*, por exemplo). É essa capacidade que os Estados pretendem reconstruir: como frear esses ataques que usam as mesmas rotas que os fluxos garantidores da integração do país na economia mundial? Como restaurar soberania em um meio desprovido de normas? "Seja qual for o ponto do debate, o conceito de fronteiras é importante porque elas definem o território no qual os governos nacionais podem empregar medidas soberanas" (HARE, 2009, pp. 88-105).

O Brasil confrontado às ciberameaças

O Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil, CERT.br,[2] fornece dados estatísticos que, ainda que não sejam exaustivos, nos permitem ter uma ideia do fenômeno da cibercriminalidade no país.

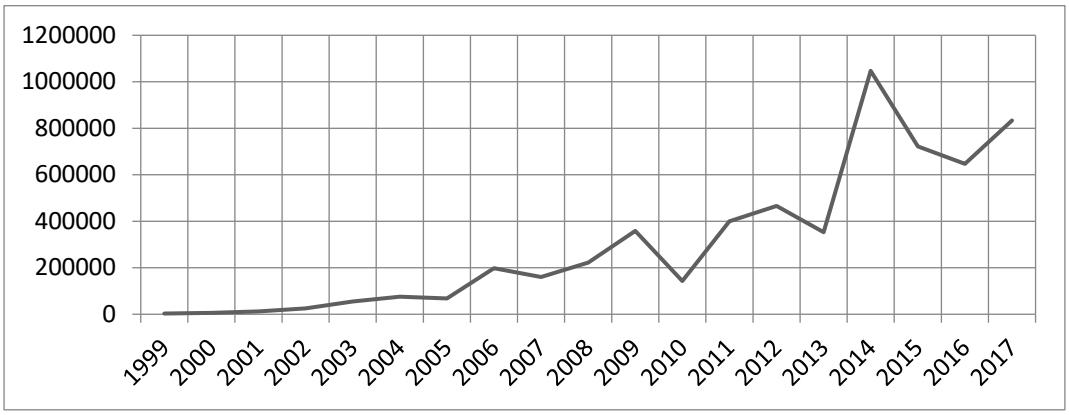
Tabela 1: Incidentes reportados (1999-2017)

Ano	Número de incidentes reportados ao CERT.br	% de ataques com origem no Brasil[3]
1999	3107	-
2000	5997	-
2001	12301	-
2002	25097	-
2003	54607	-
2004	75722	27
2005	68000	21,17
2006	197892	21,18
2007	160080	37,32
2008	222528	68,43
2009	358343	82,27
2010	142844	46,40
2011	399515	82,18
2012	466029	77,26
2013	352925	61,36
2014	1047031	75,38
2015	722205	54,02
2016	647112	55,49
2017	833775	51,77

Fonte: CERT.br.

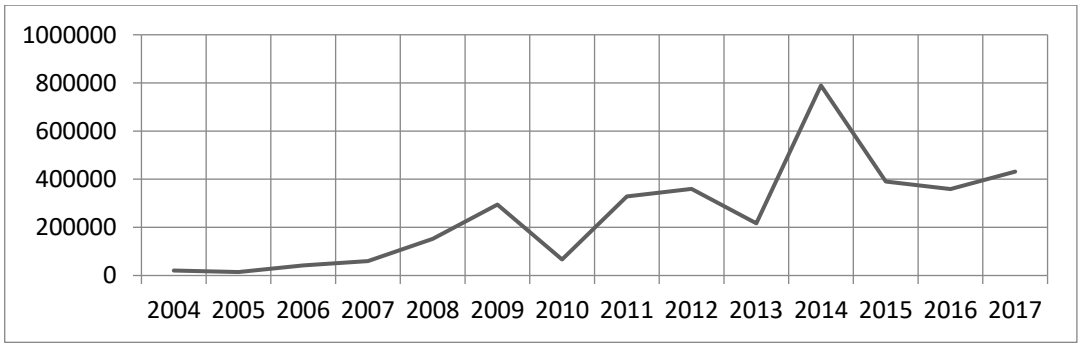
Considerando o valor absoluto do número de incidentes reportados ao CERT.br, qualquer que seja a origem geográfica dos incidentes recenseados, 2014, ano em que a Copa do Mundo de futebol ocorreu no Brasil, apresenta um pico de intensidade específico. Além dessas variações, vamos destacar o crescimento contínuo do fenômeno há cerca de 20 anos.

Gráfico 1: Curva dos incidentes reportados em valor absoluto (1999-2017)



Fonte: CERT.br.

Gráfico 2: Curva de incidentes com origem no Brasil em valor absoluto (cibercriminalidade endógena) (2004-2017)



Fonte: CERT.br.

A parte de ataques com origem no Brasil (dados integrados pelo CERT.br a partir de 2004) ilustra o nível de exposição do país à sua própria cibercriminalidade. Essa criminalidade endógena ocupa um lugar essencial, com uma média de 52% no período de 2004 a 2017 e de 65% entre 2008 e 2017, com picos de mais de 82%. A curva desses ataques "internos" segue o mesmo perfil da curva geral.

As estatísticas do CERT.br não conseguem, todavia, refletir de maneira exaustiva o fenômeno da ciberinsegurança. A organização não tem condições de recensear tudo, e só baseia suas estatísticas nos incidentes que lhe são reportados. A medida da cibercriminalidade, e mais amplamente dos fenômenos de ciberataque, permanecem um desafio por si só (quem produz os dados, o que é medido, com quais ferramentas e métodos, fiabilidade dos dados). Essas estatísticas poderiam ser complementadas por dados produzidos pela indústria da cibersegurança. Notadamente, em 2016, a empresa Fortinet mediu um forte aumento da atividade cibercriminosa (sites falsos e *malwares*) no mundo e particularmente no Brasil, a alguns meses das Olimpíadas do Rio. Essa recrudescência não chegou a transparecer nos dados do CERT.br.

Aos fenômenos de cibercriminalidade se acrescentam "ataques" feitos nas redes por Estados (serviços de inteligência, militares) sob a forma de operações de espionagem ou sabotagem.

Quadro 1: Alguns ciberataques mediatizados que ocorreram no Brasil

	Data	**Natureza do ataque**
Interrupção de sistemas de distribuição elétrica	2005 (janeiro)	Sabotagem
Interrupção de sistemas de distribuição elétrica	2007 (setembro)	Sabotagem
Divulgação das interceptações das comunicações da presidente Dilma Rousseff pelos serviços de inteligência americanos; espionagem de empresas brasileiras pelos EUA.	2012	Espionagem

Fonte: CERT.br.

As políticas de cibersegurança no Brasil têm muitos desafios a vencer: proteger-se das ciberameaças oriundas do exterior e tratar o fenômeno da cibercriminalidade brasileira de controlar uma violência que vem do exterior, mas também uma violência brasileira que está sendo exportada. As autoridades são obrigadas a integrarem a ideia de que o Brasil é um santuário da cibercriminalidade. O país vem sendo regularmente "classificado" entre os Estados que, no mundo, produzem mais ciberataques. Essa tomada de consciência do papel do Brasil na cibercriminalidade é ilustrada pelas palavras de um juiz que, após o desmantelamento de uma vasta rede de pornografia infantil no Brasil, declarou: "

Nós não conhecíamos a escala desse problema no Brasil até uma investigação da '*deep web*' em 2014. Até então, pensávamos que o Brasil era apenas um consumidor. Se tivéssemos mais capacidade operacional, teríamos mais alvos e teríamos feito mais prisões" (CABRAL, 2018).

No entanto, o fenômeno não é recente. Assim, podíamos ler, no início dos 2000: "O país está se tornando um laboratório para o cibercrime, com hackers – capazes de colaborar com relativa impunidade – especializando-se em roubo de identidade e dados, fraude de cartão de crédito e pirataria, bem como vandalismo on-line" (SMITH, 2003).

O crescimento contínuo do fenômeno, a implicação do Brasil na cibercriminalidade mundial, os ataques sofridos por atores econômicos e políticos traduzem a amplitude da área de ataque que os atores da segurança e da defesa devem proteger.

Como os Estados constroem fronteiras virtuais?

Em *Rise of a Cybered Westphalian Age*, os pesquisadores Chris C. Demchak e Peter Dombrowski (2011) formulam a constatação de um ciberespaço sob o crescente domínio dos Estados que nele se engajaram, em uma fase de afirmação de sua soberania e de construção de suas fronteiras virtuais.

> Embora não seja reconhecido como tal nem publicamente endossado pela maioria dos líderes democráticos, um processo de regulação do ciberespaço está acontecendo, construindo os blocos iniciais de cercas virtuais nacionais emergentes. Uma nova "era vestefaliana cibernética" está lentamente emergindo à medida que os líderes de Estado se organizam para proteger seus cidadãos e suas economias individualmente e, inconscientemente, iniciam o caminho para as fronteiras no ciberespaço... (DEMCHAK e DOMBROWSKI, 2011, pp. 32-61)

O processo seria uma tomada de consciência dos Estados, no mundo inteiro, após o ataque Stuxnet em 2010. "Stuxnet marca o começo oficial de um novo mundo cibernético vestefaliano

de fronteiras virtuais e comandos cibernéticos nacionais como elementos normais de governos ciberizados modernos" (DEMCHAK e DOMBROWSKI, 2011, pp. 32-61).

Concretamente, no entanto, de que maneira os Estados tornam reais as fronteiras virtuais?

A capacidade de se desconectar da internet mundial

O responsável por uma empresa privada americana de cibersegurança fez referência, há alguns meses, às capacidades chinesas de desconexão de sua rede nacional, vendo nela um modelo de prática que garante a definição de ciberfronteiras:

> Um bom exemplo de um país com bons perímetros de "fronteira cibernética" é a rede e a unidade de ciberguerra da China, cuja existência o governo reconheceu em 2015, para surpresa de ninguém. Ela é configurada como uma gigantesca rede corporativa com sub-redes e redes virtuais. A China está preparada para se desconectar efetivamente da internet no caso de um ataque cibernético detectado contra a nação. Pode-se concluir que o país também tem a capacidade de detectar ataques externos, mas escolhe não os prevenir ou deter (ORLOFF, 15/03/2017).

A fronteira virtual consistiria na capacidade de se desconectar da internet mundial, complementada por capacidades de detecção externa, por antecipação.

Essa capacidade de desconexão poderia ser definida como a forma mais elementar de ativação da fronteira virtual.

Nesses últimos anos, foram observados vários cortes propositais da internet em diversos países. A ativação da fronteira, que passou a ser barreira e deixou de ser filtro, proibindo qualquer dado de entrar ou de sair, mas também podendo ser mais seletiva, bloqueando aplicativos específicos – as mídias sociais são regularmente objeto de tais bloqueios –, ocorre em contextos peculiares: crises, revoluções, conflitos. A China, por exemplo, cortou a província de Xinjiang da internet, isolando-a, em diversas oportunidades, por razões políticas – durante motins, para perturbar a organização dos insurgentes, para garantir a Pequim o monopólio da informação pelas mídias tradicionais, como o rádio ou a televisão. Durante as Primaveras Árabes, governos bloquearam a internet dentro de suas fronteiras, com fins idênticos: perturbar a organização das revoltas, monopolizar a informação no país e no exterior.

Mas os efeitos dessa ativação da fronteira virtual não conseguiram impedir as táticas de desvio, às vezes até com a ajuda de potências estrangeiras, como a criação de redes de internet por satélite com a ajuda de soluções móveis, em regiões onde as conexões foram cortadas, o deslocamento dos indivíduos para regiões não isoladas da internet etc. O corte da internet nacional é a expressão do poder estratégico do Estado, da centralização do poder nas redes

nacionais. Mas essa fronteira virtual "estratégica" choca-se com as alternativas dos atores táticos, que passam a levantar, de certa forma, as barreiras baixadas pelas autoridades. Essa situação de assimetria remete às noções de ator estrategista e tático de Michel de Certeau.

> A estratégia tende a valorizar a estabilização do espaço dentro de quadros que pretende controlar por uma série cada vez mais enriquecida de estratos discursivos, simbólicos, racionais, tecnológicos, ou até mesmo rituais. (...) a tática é inserida no espaço a partir de e com meios oficialmente fracos ou considerados como tais (MBOUKOU, 2015).

Instaurar sistemas de controle, filtragem, vigilância dos fluxos de dados

Com o objetivo de melhorar a luta contra a cibercriminalidade no Brasil, uma comissão parlamentar foi criada, tendo por missão a produção de um relatório contendo uma série de propostas de emendas ao Marco Civil. O relatório (CÂMARA DOS DEPUTADOS, 2016) foi publicado em março de 2016. Suas propostas ensejaram imediatamente reações, pois põem em dúvida alguns dos princípios fundamentais inseridos no Marco Civil: a neutralidade da internet e a liberdade de expressão nas redes, por exemplo.

Soluções idênticas foram inseridas em outros países do mundo, que atribuem grandes poderes às autoridades no tocante ao controle da internet, à vigilância das comunicações, para o bloqueio de conteúdos e de sites, para a identificação de pessoas, ou ainda em matéria de acesso aos conteúdos criptografados. Dentro de seus territórios, os Estados impõem aos operadores privados normas mais rígidas para garantir a segurança de suas redes, de seus dados, e cooperar com a Justiça em um contexto de luta contra o terrorismo.

Impor uma governança da internet mundial

A governança da internet era historicamente dominada pelos EUA. O questionamento desse status por um grande número de países decorre de uma reivindicação de partilha em torno de um modelo multiatores (*multi-stakeholders*), por um lado, e de um modelo de governança centrado no papel maior das soberanias no funcionamento da rede, por outro.

A segunda corrente é simbolizada pelas reivindicações da China e da Rússia, soberanistas. Suas posições foram formuladas, notadamente, quando da Conferência Mundial de Telecomunicações Internacionais (CMTI-12) de Dubai, em 12 de dezembro de 2012. Essa opção afasta ou coloca em segundo plano o papel da sociedade civil, dos cidadãos, das empresas e o multilateralismo.

Já a primeira corrente, da qual o Brasil é um dos porta-vozes, contesta a dominação americana e oferece um lugar de mais destaque ao resto do mundo na governança da internet,

notadamente aos países emergentes. Desde 2003, na Cúpula Mundial da Sociedade da Informação em Genebra, o Brasil exprime essa posição. Sua postura antiamericana contesta uma injustiça de fato: o ciberespaço já não está mais centrado nos EUA, a população mundial conectada foi radicalmente redistribuída desde a criação da internet. Portanto, é justo distribuir novamente as cartas, a fim de melhor levar em conta a realidade da internet. Mas ele permanece ligado ao modelo multiatores e multilateral, que defenderá em várias ocasiões, notadamente quando do NetMundial de São Paulo em abril de 2014.

Percebemos, tanto no soberanismo quanto na contestação à dominação americana, o desejo de reconhecimento do papel dos Estados, suas visões do cenário internacional que ambos tentam transpor para a governança e o funcionamento do ciberespaço. Os Estados buscam interferir na definição do ciberespaço e a ele impor suas visões próprias, correspondentes a seus interesses nacionais, contribuindo para projetar algo "nacional" no ciberespaço.

A voz brasileira que contesta a postura dominante americana foi também ouvida no cenário internacional após as revelações de Edward Snowden relativas às práticas de espionagem da NSA e, mais especificamente, quando foram divulgadas as escutas das comunicações da então presidente Dilma Rousseff, bem como as interceptações das comunicações eletrônicas das grandes empresas brasileiras. Dilma Rousseff discursou em 2013 perante a Assembleia Geral das Nações Unidas para denunciar essas interceptações, que constituem violações à soberania nacional, assim como à vida privada dos cidadãos. Ao fazer o discurso, ela apresentou o Marco Civil como potencial modelo para um tratado internacional, que contemplaria os princípios de neutralidade da internet, de liberdade de expressão, de respeito à vida privada e de proteção contra as intrusões governamentais (ROUSSEFF, 2013). No ciberespaço, as soberanias devem, portanto, ser respeitadas.

O Brasil parece estar oferecendo uma reconstrução da arquitetura da internet para afirmar esses direitos das soberanias: quando presidente, Dilma Rousseff anunciou um novo cabo submarino internacional ligando o Brasil ao continente europeu (Portugal), buscando evitar o olhar espião de Washington. Ela também pediu a criação de caixas postais eletrônicas criptografadas e queria obrigar as empresas americanas como Facebook e Google a estocar os dados dos brasileiros em servidores localizados no Brasil. À soberania dos dados, acrescenta-se ainda a estratégia de soberania tecnológica, que tem por objetivo desenvolver uma indústria "nacional" do ciberespaço (empresas de cibersegurança, indústria de software, hardware, fabricantes de cabos, concepção de satélites etc.). O elo entre o ciberespaço e a soberania é estreito. Os diversos métodos evocados (soberania dos dados, controle sobre os servidores de empresas estrangeiras...) constroem o território no ciberespaço e, portanto, suas fronteiras.

A militarização do ciberespaço

Militarização e construção de fronteiras mantêm uma ligação íntima. Ainda que a militarização de um espaço, de um território, não implique a construção de uma fronteira, ela afirma, todavia, a presença do Estado, sua vontade de defender um território soberano.

A presença militar no ciberespaço é anterior ao advento da internet comercial. A primeira rede planetária de transporte de fluxos, elétricos, foi o telégrafo, no século XIX. Ainda que as linhas telegráficas tenham sido construídas graças aos capitais privados, os Estados sempre estiveram implicados nos projetos, decidindo por quais caminhos passariam os cabos ou, ainda, as regras de exploração da atividade. O telégrafo foi o instrumento dos impérios colonizadores. O militar ocupou um lugar essencial, central, até por ter monopolizado o uso dessas infraestruturas em tempos de guerras – que, por sinal, foram muitas no século XIX.

O telégrafo permitiu ligar os governos das colônias às capitais europeias, colocar em contato as forças armadas distribuídas nesses vastos territórios – ele foi essencial para a evolução da arte da guerra e para o fim dos conflitos, lembremos a Guerra de Secessão americana. Permitiu criar redes de postos de defesa militares (guarnições) ao longo das fronteiras afastadas do poder político centralizado – lembremos a experiência chilena do século XIX (MARTLAND, 2014, pp. 283-308).[4] Os exércitos também foram usados para proteger infraestruturas telegráficas – quando foi necessário, por exemplo, que os militares fizessem a segurança das estações de aterramento em períodos de guerra. As forças armadas foram, portanto, mobilizadas para a defesa e proteção das infraestruturas das redes.

No século XX, as forças de defesa integraram rápida e naturalmente as novas tecnologias de comunicação, a informática e as redes de internet no desenvolvimento de suas capacidades. Os Estados, em suas estratégias nacionais de cibersegurança, implicam ao mesmo tempo atores civis e militares, atribuindo, de acordo com os modelos, maiores poderes a uns ou aos outros.

Parece-nos que essa lógica é oriunda do dilema de segurança (HERZ, 1951): os desenvolvimentos das capacidades ofensivas de um Estado, o aumento dos investimentos militares, suas posturas políticas (seus discursos), suas ações (deslocamentos de tropas para a fronteira, militarização de territórios disputados por outros Estados, envio de arsenais militares para zonas sensíveis, exercícios militares de grande alcance, testes de novos armamentos) revelam intenções que os Estados vizinhos ou mundo afora percebem como um perigo significativo.

Para enfrentar essa ameaça e reequilibrar as relações de força, os países por ela atingidos começam, por sua vez, a investir no aumento de sua capacidade de defesa. Essa percepção de ameaças e a escalada de capacidades, ou até mesmo de violência, encontra seu equivalente no ciberespaço. Os exércitos desenvolvem capacidades defensivas e ofensivas, dotando-se se

unidades dedicadas à "ciberguerra" (o Cyber Command americano e o CDCiber brasileiro, por exemplo), de novas ciberarmas (*malwares* que permitem espionar o adversário ou destruir seus sistemas) e formulam novas estratégias de defesa cibernética. O ataque Stuxnet (pirataria das centrais nucleares iranianas) foi um dos fatos notáveis da história recente de um ciberespaço militarizado.

Um dos maiores desafios para os Estados é, portanto, definir, no âmbito do ciberespaço, o que tem natureza jurídica de ato de guerra, de ataque contra a soberania, e trazer respostas adequadas, de acordo com os princípios do direito internacional. A fronteira está no cerne dessas considerações, já que os ciberataques usam redes e cabos que passam, fisicamente, por territórios soberanos. O ataque militar às redes, assim como o ataque cibercriminoso, revela ou supõe a existência de pontos de fronteira.

Quadro 2: Recenseamento de fatos essenciais na cronologia do ciberespaço no Brasil

Fato (evento, publicação importante, declarações, criação de instituições etc.)	**Descrição/ comentários**	**Data**
1964 governo militar até 1985		1964-1985
Presidência de José Sarney	Partido do Movimento Democrático Brasileiro (PMDB).	1985 (março) - 1990 (março)
Lançamento da Internet	Projeto universitário entre Rio de Janeiro e São Paulo.	1988
Presidência de Fernando Collor	Partido da Reconstrução Nacional (PRN).	1990 (março) - 1992 (dezembro)
Presidência de Itamar Franco	Partido do Movimento Democrático Brasileiro (PMDB).	1992 (dezembro) - 1994 (dezembro)
Presidência de Fernando Henrique Cardoso	Partido da Social Democracia Brasileira (PSDB).	1995 (janeiro) - 2002 (dezembro)
A Internet torna-se pública	Internet Service Law abre o mercado para as empresas privadas.	1995
Política Nacional de Defesa (PND) - 1ª edição	Pela primeira vez no Brasil, as prioridades de segurança são tornadas públicas.	1996
Lei nº 9.296/96	Sanciona, em seu artigo 10, a interceptação de comunicações telefônicas e informáticas.	1996
Lei nº 9.504/97	Sanciona, em seu artigo 72, as violações aos sistemas de processamento de dados eleitorais.	1997 (setembro)

Lei nº 9.609/98	Sanciona, em seu artigo 12, a violação aos direitos autorais no âmbito dos softwares.	1998
Privatizações no setor das telecomunicações	Privatização da Telebrás e emergência de companhias privadas (Telefônica, Telemar e Brasil Telecom).	1998
Criação do Ministério da Defesa	O Ministério é dirigido por um civil: controle civil exercido sobre o militar, para consolidar a democracia. Essa criação está inscrita na NPD de 1996.	1999
Aparecimento do ADSL		2000
Luiz Inácio (Lula) da Silva, presidente do Brasil	Partido dos Trabalhadores (PT).	2003 (1° de janeiro) - 2011 (1° de janeiro)
O "fenômeno da internet brasileira"	Os brasileiros seriam os internautas que passam mais tempo conectados no mundo.	2003
SMSI (Genebra)	O Brasil participa da Cúpula Mundial sobre a Sociedade da Informação, na qual se torna um dos porta-vozes da contestação contra a dominação americana da internet.	2003 (10 a 12 de dezembro)
Política Nacional de Defesa (PND) - 2ª edição	Essa PND foi o primeiro documento nacional a mencionar o *ciber*. Vontade de reduzir a vulnerabilidade aos ciberataques dos sistemas de defesa.	2005
Glossário das forças armadas - 4ª Edição	Documento do Ministério da Defesa. MD35-G-01. Fornece as definições de ciberguerra: "Guerra Cibernética - Conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil" (MINISTERIO DA DEFESA, 2007). O glossário também classifica os ciberataques como ameaças assimétricas. Encontramos, além disso, entre os termos, conceitos que refletem uma influência do pensamento dos EUA sobre as doutrinas militares. Prova disso é, por exemplo, a noção de Guerra Centrada em Redes.	2007
Lei n° 6.703 Estratégia Nacional de Defesa - END	Cria a Estratégia Nacional de Defesa. O ciberespaço é considerado um setor estratégico da mesma forma que o nuclear e o espacial. O texto prevê a criação de organizações encarregadas do desenvolvimento de capacidades cibernéticas, industriais e militares. Ela confere poderes ao exército em matéria de cibersegurança.	2008 (18 de dezembro)
Livro Verde Segurança Cibernética no Brasil	Institui as bases de uma futura política de cibersegurança. Considera a cibersegurança um assunto internacional, e remete, a título de exemplo, às estratégias propostas pela Organização dos Estados Americanos (OEA), pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE), ou ainda pela International Telecommunications Union (ITU). Propõe medidas de proteção do ciberespaço, considerando a cibersegurança como uma pauta transnacional e não estritamente nacional. Essa abordagem orientada para o âmbito internacional, associa igualmente a opção *multi-stakeholders* (que consiste em associar à cibersegurança atores de vários setores da sociedade). "Chama a atenção que o chamado espaço cibernético, que não tem suas fronteiras ainda claramente definidas, impacta o dia-a-dia de todos os dirigentes governamentais, de empreendimentos privados e dos próprios cidadãos" (MANDARINO, 2010).	2010 (dezembro)
Portarias normativas n° 666 e nº 667	Criam o NU CDCiber (Núcleo do Centro de Defesa Cibernética). O CDCiber (Centro de Defesa Cibernética) passa a ser operacional em 2012.	2010

(Comando de Operações Terrestres)	A primeira tarefa do Centro será a proteção das redes durante a conferência das Nações Unidas sobre o desenvolvimento sustentável, no Rio de Janeiro, em 2012.	
Dilma Rousseff, presidente do Brasil	Partido dos Trabalhadores (PT).	2011 (janeiro) - 2016 (31 de agosto)
Política de Defesa Cibernética Brasileira. Ministério da Defesa.	Pensa os aspectos táticos e estratégicos da defesa cibernética.	2012
Política Cibernética de Defesa (Estado-Maior Conjunto das Forças Armadas)	Desenvolve medidas de proteção do ciberespaço.	2012
Conferência das Nações Unidas sobre o Desenvolvimento Sustentável	Rio de Janeiro. O exército, através de seu Centro de Defesa Cibernética, garante a segurança cibernética dos sistemas de telecomunicação contra os ciberataques.	2012 (13 a 22 de junho)
Livro Branco de Defesa Nacional (LBDN)	Esse texto prevê a criação do CDCiber (Centro de Defesa Cibernética). O CDCiber deve ser criado por decreto presidencial com o objetivo de mudar a estrutura do exército. O documento define os objetivos da política de defesa nacional durante os próximos 20 anos. Desenvolve as medidas de proteção do ciberespaço. Aloca 200 milhões de dólares para a defesa cibernética entre 2011 e 2035.	2012 (julho)
Lei Carolina Dieckmann. Tipificação Criminal de Delitos Informáticos (lei n° 12.737/2012)	Define determinados crimes cibernéticos, como a pirataria, o furto de dados de usuários, o ataque aos sites de internet etc. O *hacking* torna-se formalmente um crime.	2012 (dezembro)
Conferência mundial das telecomunicações internacionais (CMTI-12) (Dubai)	Participação do Brasil.	2012 (3 a 14 de dezembro)
Política de Defesa Cibernética (MD) (Portaria Normativa n° 3.389/MD)	Afirma o caráter estratégico da defesa cibernética. Os níveis tático e operacional da defesa cibernética devem contribuir para reforçar a segurança das redes públicas. O país deve desenvolver capacidades dissuasivas e reforçar as capacidades de inteligência.	2012 (21 de dezembro)
Revelações de E. Snowden	Em 6 de junho de 2013, começa uma longa série de divulgações de documentos que demonstram a existência de programas de interceptação em massa de dados no mundo inteiro, por parte da NSA.	2013 (6 de junho)
Revelação de E. Snowden: espionagem visando o Brasil	Informações segundo as quais a NSA espionou empresas e cidadãos brasileiros.	2013 (7 de julho)
Revelações de E. Snowden: espionagem visando a presidente Dilma Rousseff	O jornalista Glenn Greenwald revela que a NSA espionou as comunicações da presidente Dilma Rousseff.	2013 (1° de setembro)
Revelações de E. Snowden	O jornalista Glenn Greenwald revela que a NSA espionou empresas brasileiras.	2013 (9 de setembro)
Reações da presidente Dilma Rousseff às práticas de espionagem	Ao fazer um discurso na ONU, a presidente clama pela criação de laços independentes com o resto do mundo. Faz-se necessário sair da dependência para com os EUA. Ela propõe a instalação de novos cabos transatlânticos ligando o Brasil à Europa.	2013 (24 de setembro)

americanas reveladas por E. Snowden	Ao adotar um discurso que também acabou sendo desenvolvido em outros continentes, sobretudo na Europa, ela propõe a criação de uma indústria de tecnologias soberanas e de fortes sistemas de criptografia.	
Dilma Rousseff cancela uma visita aos EUA	Em reação às revelações de E. Snowden, Dilma Rousseff cancela o encontro com o presidente B. Obama, programado para Washington, em 23 de outubro de 2013.	2013 (23 de outubro)
E. Snowden pede asilo político ao Brasil	Em carta aberta ao Brasil, E. Snowden pede asilo político.	2013 (dezembro)
Cabos submarinos de Internet internacionais	Acordo entre o Brasil e a União Europeia para instalar cabos submarinos de internet entre Fortaleza e Lisboa (Portugal). Objetivo alegado: limitar a dependência do Brasil com relação aos EUA. A defesa da soberania implica soluções de substituição, rotas alternativas fora dos EUA. Mas essas "soluções", na realidade, não entram no mérito dos projetos de conexão direta entre o Brasil e os EUA (cabo Faster).	2014 (24 de fevereiro)
NetMundial Conferência Global sobre o Futuro da Governança da Internet		2014 (23 e 24 de abril)
Marco Civil da Internet, lei n° 12.965	Assinado durante a NetMundial – Conferência Global sobre o Futuro da Governança da Internet. A lei regula o uso da Internet e reconhece os direitos fundamentais (acesso para todos, liberdade de expressão online, direito ao respeito à vida privada, à segurança, à neutralidade da internet, censura proibida). O Brasil é o primeiro país do mundo a adotar uma lei como essa.	2014 (23 de abril)
Copa do Mundo de Futebol		2014 (12 de junho - 13 julho)
Cabos submarinos de Internet internacionais	Anúncio da construção de uma nova conexão submarina ligando o Brasil aos EUA. O cabo FASTER, que deve se tornar operacional no fim de 2016, será construído pelas empresas Google, ISP Algar Telecom (Brasil), Antel (Uruguai) e Angola Cables. O cabo ligará Santos e Fortaleza (Brasil) e Boca Raton (EUA).	2014 (13 de outubro)
Cabos submarinos de Internet internacionais	Novo cabo submarino AMX-1, ligando o Brasil aos EUA (operacional no fim de 2014).	2014
Cabos submarinos de Internet internacionais	Novo cabo submarino Seabras-1, ligando o Brasil aos EUA (operação realizada pela empresa americana Seaborn Networks).	2017 (setembro)
Doutrina militar de defesa cibernética (Estado-Maior Conjunto das Forças Armadas)	Desenvolve medidas de proteção do ciberespaço. Missão: lutar contra as ameaças cibernéticas externas, preparar as forças armadas para responder a essas ameaças provenientes de Estados, organizações ou pequenos grupos. Organiza a defesa cibernética com seus níveis táticos e estratégias.	2014
Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal – 2015/2018, versão 1.0	Tem o objetivo de aprimorar as práticas em matéria de segurança da informação e segurança cibernética.	2015

Glossário das forças armadas - 5ª edição	Ministério da Defesa, MD35-G-01. Integração do *Ciber* nas forças armadas, suas doutrinas e estratégias, é o que transparece nesse documento, no qual o número de ocorrências do termo "ciber" é bem maior do que na versão de 2007.	2015
Relatório Parlamentar sobre cibercriminalidade	O relatório, com o objetivo de lutar contra as ameaças cibernéticas, formula um conjunto de propostas inspiradas em "soluções" experimentadas em outros países: questiona a neutralidade da internet, os controles, bloqueios... O relatório visa modificar o Marco Civil de 2014.	2016 (março)
Carta aberta de Tim Berners-Lee aos legisladores brasileiros	A carta aberta alerta os legisladores brasileiros contra o questionamento dos princípios fundamentais determinados pelo Marco Civil, em nome da luta contra os cibercrimes (após o relatório parlamentar de março de 2016): riscos para a neutralidade da Internet, bloqueio de aplicativos, vigilância, identificação policial de indivíduos sem mandado judicial.	2016 (11 de abril)
Relatório Parlamentar sobre cibercriminalidade - 2ª versão	Após as críticas, foi publicada uma versão revisada do relatório parlamentar sobre cibercriminalidade, afastando algumas das propostas.	2016 (11 de abril)
Olimpíadas		2016 (5 a 21 de agosto)
Michel Temer chega à presidência do Brasil	Movimento Democrático Brasileiro (MDB).	2016 (31 de agosto) – 2018 (31 de dezembro)
Brasil e Europol assinam um acordo	Acordo de cooperação para a luta contra o cibercrime e outras formas de criminalidade transnacionais.	2017 (abril)
Guia de ciberdefesa, publicado pelo Ministério da defesa brasileiro		2017 (23 de agosto)
Brazil Cyber Defence Summit and Expo (Brasília)	Promover o diálogo entre Exército, LEA, indústria, instituições públicas e privadas, mundo acadêmico, governo. Conferência voltada para as forças armadas, com vários palestrantes militares brasileiros.	2018 (23 a 26 de abril)
Desmantelamento de uma vasta rede brasileira de pornografia infantil	Vasta operação policial no Brasil contra redes de pornografia infantil: 251 prisões, 2.500 policiais mobilizados, centenas de computadores e milhares de arquivos apreendidos.	2018 (maio)

Fontes: Variadas, com elaboração própria.

Conclusão

A transparência da fronteira cibernética é essencial para a integração do Estado no sistema internacional contemporâneo. A contrapartida é essa sujeição à vulnerabilidade da qual os Estados ainda não sabem se defender. "Alguns Estados estão claramente à vontade: trata-se de uma arena em que os jogadores podem 'bater uns nos outros' com cada vez mais força, não há atribuição formal, portanto não há consequências", colocou Guillaume Poupard (*apud* GUITON, 2017).[5]

A evolução que tende à construção de fronteiras virtuais, como uma das respostas ao ambiente de insegurança, parece inexorável. Como o centro do poder mundial está se deslocando para a Ásia, sob a liderança da China, a ideia de espaços soberanos e de Estados que dominam o ciberespaço, exaltada pelos Estados da região, está progredindo.

O corte do ciberespaço em Estados, em territórios soberanos, supõe mais controle de fluxos, mais militarização para construir o território nos limites da fronteira, para consolidá-la. O ciberespaço estaria em vias de "balcanização", um espaço cada vez mais aberto à probabilidade de novos conflitos futuros:

> Necessita-se urgentemente de uma estrutura viável para um mundo ciberizado conflituoso. (...) Ela deve ser uma que aceite o crescimento da soberania cibernética entre nações que, em um futuro próximo, não serão sociedades civis – se é que alguma vez o foram. (...). O conflituoso e eventualmente pós-ocidental sistema internacional cibernético vestefaliano está crescendo muito rapidamente (DEMCHAK, 2016, pp. 49-74).

Os partidários da Internet aberta, sem fronteiras, chamam de "balcanização" a tendência ao recorte da internet em espaços nacionais, que leva o mundo a uma governança centrada no Estado, afastando a sociedade civil. Essa estratégia centrada nas soberanias levaria a dúvidas sobre a organização da internet, pois haveria vários pesos e várias medidas, os Estados se conectariam e se desconectariam dela, ou fariam alianças com parceiros privilegiados, desenhando um ciberespaço recortado em subespaços, em regiões. A balcanização, neste contexto, designa a explosão, a fragmentação de um *global commons* que continua sendo, de qualquer forma, uma utopia. O ciberespaço não é – não é mais e sem dúvida jamais foi – um espaço liso, uniformemente partilhado por todos, no qual as regras comuns e consensuais são respeitadas.

> (...) a expressão "balcanização", embora seu uso tenha se tornado comum desde os conflitos iugoslavos dos anos 1990, não é neutra e se refere a todo um imaginário da violência e do caos político. Ela parece pressupor uma fragmentação sem fim do mundo, uma "proliferação estatal", levando a Estados fechados em si mesmos, a sistemas autoritários ou a Estados não funcionais (CATTARUZZA *et al*., 2014).

Este primeiro trabalho sobre a criação de fronteiras no ciberespaço poderá ser completado de três maneiras. Uma delas é estudando o papel dos atores privados no processo de construção das fronteiras e da securitização do ciberespaço não restrito, sendo que eles construíram seus mercados, em grande parte, considerando a ideia de um ciberespaço globalizado. As empresas de cibersegurança vendem "soluções soberanas" e interagem com os Estados ao usarem ferramentas de controle de fluxos. Trata-se, portanto, de atores que, junto com os Estados, constroem as fronteiras virtuais.

O segundo eixo de reflexão aborda a dinâmica criada entre os interesses nacionais e as posturas dos Estados no cenário diplomático. As forças em jogo podem gerar tensões entre os dois polos. Essa questão poderá, notadamente, mobilizar a teoria dos jogos de dois níveis de Putnam (1988).[6] Enfim, se os Estados construírem fronteiras dentro do ciberespaço, caberá a eles também explorar amplamente suas tecnologias para manter a segurança, defender, construir suas fronteiras territoriais terrestres, marítimas e aéreas. Sejam essas funções atribuídas aos atores estatais ou parcialmente aos atores privados, na área civil ou militar, a reflexão deverá observar o caráter um pouco paradoxal da segurança das fronteiras do espaço de soberania com a ajuda das tecnologias que as enfraquecem.

Notas

[1] Stuxnet é o nome dado a um *malware* concebido pela NSA, usado pelos EUA com o objetivo de paralisar o funcionamento das centrífugas nucleares iranianas. Por meio desse ciberataque, os EUA queriam destruir as infraestruturas nucleares iranianas e convencer o Irã a abandonar seu programa nuclear. A operação foi descoberta em 2010 em função da propagação internacional do *malware*, que infectou um grande número de sistemas industriais mundo afora. A operação, que inicialmente tinha por único alvo o programa iraniano, foi um relativo fracasso, em razão dos efeitos colaterais produzidos (propagação do *malware* não dominada) e do impacto limitado sobre o programa iraniano (grande parte das centrífugas ficou temporariamente paralisada, mas nem por isso o programa deixou de prosseguir).

[2] Dados oriundos do site do CERT.br. Disponível em: <https://www.cert.br/stats/incidentes/>.

[3] Esses dados só foram produzidos pelo CERT.br a partir do segundo semestre de 2004.

[4] Em 1870, o governo chileno levou a rede telegráfica elétrica até as regiões fronteiriças, distantes da capital. Essa rede serviu para apoiar a conquista da região de Araucanía, ao sul do país, impondo à população Mapuche a dominação militar. Graças à rede, foi possível, em um primeiro momento, transmitir ordens entre diversos postos de comando militar situados ao longo da fronteira. Posteriormente, a rede foi usada para garantir as comunicações entre a capital e os governadores regionais civis. A rede telegráfica era uma ferramenta a serviço do poder político centralizado, que podia assim administrar, comandar as regiões periféricas, graças a uma troca de informações nos dois sentidos (da capital para as regiões e vice-versa).

[5] Guilhaume Poupard é o diretor da Agência Nacional de Segurança dos Sistemas de Informação (ANSSI) da França.

[6] Um Estado engajado em processos diplomáticos deve combinar dois níveis de constrangimentos, às vezes contraditórios: as possibilidades e expectativas da comunidade internacional na qual deseja desempenhar um papel e as expectativas dentro de seu próprio país. Essa teoria dos jogos em dois níveis pode ser útil para a compreensão da postura cibersecuritária dos Estados.

Referências

BARLOW, John Perry. A Declaration of the Independence of Cyberspace. **Eletronic Frontier Foundation**, 8 fev. 1996. Disponível em: https://www.eff.org/fr/cyberspace-independence.

BRASIL. Ministério da Defesa. **Glossário das Forças Armadas.** Brasília, DF: Ministério da Defesa, 2007.

CABRAL, Paulo. Brazil Conducts Large-Scale, Cyber-Crime Operation to Fight Child Porn. **CGTN America**, 22 mai. 2018. Disponível em: https://america.cgtn.com/2018/05/22/brazil-conducts-large-scale-cyber-crime-operation-to-fight-child-porn.

CATTARUZZA, Amael; DANET, Didier; DESFORGES, Alix; DOUZET, Frédérick; NACCACHE, David. **La balkanisation du web**: Chance ou risque pour l'Europe. Direction aux Affaires Stratégiques, Ministère de la Défense, France, 2014. Disponível em: https://www.defense.gouv.fr/content/download/326205/4482503/file/Pages%20de%20EPS2013-LaBalkanisationDuWeb-Part1.11.pdf

CÂMARA DOS DEPUTADOS. **CPI – Crimes cibernéticos**. "Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país". Relatório Final. Brasília, DF, 2016. Disponível em: https://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1449738.

DEIRMENJIAN, John. Stalking in Cyberspace. **Journal of the American Academy of Psychiatry and Law**, v. 27, n. 3, p. 407-413, 1999.

DEMCHAK, Chris. Uncivil and Post-Western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age. **The Cyber Defense Review**, v. 1, n. 1, p. 49-74, 2016.

_____; DOMBROWSKI, Peter. Rise of a Cybered Westphalian Age. **Strategic Studies Quarterly**, v. 5, n. 1, p. 32-61, 2011.

DOD. **Dictionary of Military and Associated Terms**. U.S. Department of Defense (DOD), Washington, DC, 2018. Disponível em: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

DOUZET, Frédérick; DESFORGES, Alix; LIMONIER, Kevin. **Géopolitique du cyberespace**: "Territoire", frontières et conflits. CIST2014: Fronts et Frontières des Sciences du Territoire, Collège international des sciences du territoire (Cist), mar. 2014, Paris, France, , p. 173-178. Disponível em: https://hal.archives-ouvertes.fr/hal-01353455/document

GIBSON, William. *Neuromancer*. Nova York: Ace, 1984.

GUITON, Amaelle. Guillaume Poupard: "Pour certains Etats, le cyberespace est un terrain de jeux". **Libération**, 12 out. 2017. Disponível em: https://www.liberation.fr/futurs/2017/10/12/guillaume-poupard-pour-certains-etats-le-cyberespace-est-un-terrain-de-jeux_1602637

HARE, Forest. Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security? *In*: CZOSSECK, Christian; GEERS, Kenneth. **The Virtual Battlefield**: Perspectives on Cyber Warfare. Amsterdã: IOS Press, 2009, p. 88-105.

HERZ, John. **Political Realism and Political Idealism**. Chicago: University of Chicago Press, 1951.

KUEHL, Daniel. From Cyberspace to Cyberpower: Defining the Problem. *In*: KRAMER, Franklin. **Cyberpower and National Security**. Lincoln: University of Nebraska Press, 2009, p. 24-42.

LACOSTE, Yves. **Dictionnaire de géographie**. Paris: Armand Colin, 2003.

MANDARINO, Rafael; CANONGIA, Claudia. **Livro verde**: Segurança cibernética no Brasil. Departamento de Segurança da Informação e Comunicações (DSIC), Gabinete de Segurança Institucional da Presidência da República (GSI/PR), 2010. Disponível em: http://livroaberto.ibict.br/bitstream/1/639/4/Livro%20verde%20seguran%C3%A7a%20cibern%C3%A9tica%20no%20Brasil.pdf

MARTLAND, Samuel. Standardizing the State while Integrating the Frontier: The Chilean Telegraph System in the Araucania, 1870-1900. **History and Technology**, v. 30, n. 4, p. 283-308, 2014.

MBOUKOU, Serge. Entre stratégie et tactique. **Le Portique**, v. 35, 2015. Disponível em: https://journals.openedition.org/leportique/2820.

ORLOFF, Rick. It's Time for America to Protect Its Cyber Borders. **Nextgov**, Ideas, 15 mar. 2017. Disponível em: https://www.nextgov.com/ideas/2017/03/its-time-america-protect-its-cyber-borders/136167

PUTNAM, Robert. Diplomacy and Domestic Politics: The Logic of Two-Level Games. **International Organization**, v. 42, n. 3, p. 427-460, 1988.

ROUSSEFF, Dilma. **Opening of the General Debate of the 68th Session of the United Nations General Assembly**. Organização das Nações Unidas (ONU), Nova York, 2013. Disponível em: https://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf

SMITH, Tony. Brazil Becomes a Cybercrime Lab. **The New York Times**, Archives, 27 out. 2003. Disponível em: https://www.nytimes.com/2003/10/27/business/technology-brazil-becomes-a-cybercrime-lab.html

DANIEL VENTRE (daniel.ventre@cesdip.fr) é doutor em ciência política, pesquisador no Centre de recherches Sociologiques sur le Droit et les Institutions Pénales (Cesdip) e da Université de Cergy Pontoise (Paris, França). Diretor da coleção *Cybersécurité*, da editora Iste. Seus trabalhos centram-se nas políticas e estratégias dos Estados em matéria de cibersegurança e ciberdefesa. Publicou uma dezena de livros sobre a guerra da informação, a ciberguerra e a cibersegurança. Seu último livro é a segunda edição revisada de *Information Warfare* (2016).

Recebido em: 06/02/2019
Aprovado em: 12/02/2019