A Rússia, o Ciberespaço e uma estratégia nacional[1]

Danniel Garcia Barbosa de Figueiredo[2]
Eduardo de Rê[3]
Thássia Barbosa de Menezes[4]

De acordo com o portal Internet World Stats[5], a Rússia é o maior país da Europa em termos de usuários conectados à internet. São mais de 116 milhões de pessoas em território russo com acesso a rede. Mas esse número, por si só, não expressa a realidade digital do país. Para entendermos a visão da Rússia sobre ter tantas pessoas com acesso a uma infinidade de informações e sobre o ciberespaço em geral, em primeiro lugar, precisamos entender o contexto no qual o país está inserido atualmente e, após isso, analisar alguns dos principais documentos russos referentes ao setor cibernético.

Após o final da URSS - da qual era o centro - a Federação Russa enfrentou uma série de dificuldades econômicas e políticas. Esse contexto passa a se modificar no final dos anos 1990, com o *boom* dos preços das commodities energéticas em conjunto com a reformulação regulatória e acionária da cadeia de petróleo e gás no governo Putin (2000-2008) (SANTANA, 2015). Vale lembrar que a Rússia tem grandes reservas de petróleo e as maiores reservas de gás natural do mundo, fundamentais para o abastecimento da Europa.

Durante os governos Putin (2000-08 e 2012 até atualmente) e de Medvedev (2008-2012) esse foi o principal caminho para a recuperação da economia. O petróleo e o gás natural que, somados, em 1999 correspondiam a 20% das receitas tributárias federais, em 2011 passaram a representar 49% - paralelamente, de 1999 a 2008 o PIB russo cresceu em média 6,9% ao ano (SANTANA, 2015).

Apesar de a recuperação econômica ter ocorrido, o poderio global do país - ou ao menos a visão que se tem dele - não é o mesmo dos tempos soviéticos. Um bom ilustrativo disso é a famosa fala do então presidente dos Estados Unidos, Barack Obama, em 2014, classificando o

---

[1] Este trabalho é fruto da pesquisa conjunta realizada no de 2019 pelo GEPPIC – Grupo de Pesquisa em Estudos Estratégicos e Política Internacional Contemporânea.
[2] Graduando em Relações Internacionais pela Universidade Federal de Santa Catarina – UFSC e pesquisador no GEPPIC.
[3] Graduando em Relações Internacionais pela Universidade Federal de Santa Catarina – UFSC e pesquisador no GEPPIC.
[4] Graduanda em Relações Internacionais pela Universidade Federal de Santa Catarina – UFSC e pesquisadora no GEPPIC.
[5] Disponível em: https://www.internetworldstats.com/stats4.htm#europe. Acesso em 10 de maio de 2020.

país como um "*Regional Power*"[6]. Ainda assim, a ascensão de Putin deu forças a uma corrente na Rússia que visa a restauração do poder e do papel russo no mundo (SVARIN, 2016). Mais detalhadamente, de acordo com Bobo Lo (2018), a política internacional da Rússia de Putin é marcada por 4 elementos: (1) uma identidade e ideologia tipicamente russas, segundo as quais o país se entende como "especial", destinado a ser um *great power*, e não apenas um *rule-taker* - e que se sustenta na sua presença no Conselho de Segurança, na grandeza de território e em seu poderio militar; (2) uma cultura estratégica que prioriza o uso do *hard power*, e é marcada por ações friamente calculadas. Isso se reforçou através da decepção com o Ocidente no pós-Guerra Fria. Enquanto acreditava que receberia igual *status* na nova ordem pós Guerra Fria e tentava estabelecer cooperação estratégica com os Estados Unidos e Europa, a Rússia enxerga que foi deixada na mão, se vendo atacada economicamente e através das tentativas de expansão da OTAN; (3) um forte componente da visão do próprio Putin, que é o "árbitro final" do que se constitui o interesse nacional russo e que visa, com seus atos (como o da invasão da Crimeia), passar uma imagem de Rússia forte para o mundo; (4) uma forte capacidade de improvisação tática em meio a oportunidades, exemplificada na aproximação com a China em meio a crise de 2008, para diminuir sua dependência do Ocidente e na própria anexação da Crimeia, em 2014, em meio às instabilidades na Ucrânia. (LO, 2018).

Contudo, por mais que boa parte desses elementos (forte nacionalismo, sentimento de grandeza, busca por status de igualdade) tendem a apontar para um certo saudosismo do cenário da posição e do respeito a Rússia no século XX, também não há dúvidas de que o país tem plena ciência dos elementos que diferenciam o cenário mais recente. Em famoso artigo em 2013, o general russo Valery Gerasimov apontou o mundo do século XXI como marcado por fragilidades, com conflitos podendo partir de instabilidades internas (GERASIMOV, 2013).

Seguindo essa linha, Charles Bartle (2016) evidenciou com mais clareza a questão trazida pelo general russo. De acordo com ele, o elemento chave que podemos adquirir a partir do texto de Gerasimov é a percepção de que, para a Rússia, no mundo pós Guerra-Fria, a soberania de regimes não ocidentais se encontra ameaçada por políticas de controle estadunidense, tais como uso massivo de propaganda, da internet e de mídias sociais. Ou seja, o elemento da informação, já forte na guerra fria, é agora ainda mais relevante na estratégia do Ocidente. Conforme aponta Bartle *"*A Rússia acredita que o padrão de mudança forçada patrocinada pelos EUA tem sido amplamente substituído por um novo método. Em vez de uma evidente invasão militar, os primeiros atos de um ataque dos EUA vêm da parcela de uma

[6]Disponível em: https://www.theguardian.com/world/2014/mar/25/barack-obama-russia-regional-power-ukraine-weakness. Acesso em 20 de junho de 2020.

oposição política através de propaganda estatal (por exemplo, CNN, BBC), a Internet e mídias sociais e organizações não governamentais (ONGs). Após introduzir a dissidência política, o separatismo e/ou o conflito social com sucesso, o governo legítimo tem uma dificuldade crescente em manter a ordem." (BARTLES, 2016, p. 32)[7].

Assim, ao mesmo tempo em que passa por um processo de reafirmação político-econômica, e demonstra força na corrida militar tradicional - como com seus mais recentes testes de mísseis hipersônicos[8] - o país também se vê ameaçado por elementos que partem de um conflito informacional, no qual aquelas 116 milhões de pessoas com acesso à internet se tornam possíveis fragilidades.

O próprio presidente Putin, em entrevista à jovens jornalistas russos em 2014, declarou que a internet é "um projeto da CIA" e alertou sobre os perigos que existem ao fazer buscas na plataforma[9]. Da mesma forma, o Coronel aposentado A.A.Bartosh (2018) em revista do Ministério da Defesa do país[10], afirmou que *"*as enormes consequências destrutivas do uso de armas cibernéticas em uma guerra híbrida permitem hoje comparar a extensão de seu impacto nas forças armadas, na indústria, nos transportes e na população do país com os resultados do uso de armas nucleares. Isso sugere a necessidade de elevar a chamada dissuasão cibernética a par da nuclear*"* (BARTOSH, 2018, s. p.)[11]. Dessa forma, não é de se estranhar os diversos elementos referentes a proteção de informação presentes nos documentos russos sobre o tema.

O que dizem os documentos russos?

Os documentos oficiais do governo russo são promulgados em sua grande maioria através de decretos presidenciais e possuem caráter de leis federais. Suas diretrizes projetam a

[7] [Tradução nossa] Texto original: Russia believes that the pattern of forced U.S.-sponsored regime change has been largely supplanted by a new method. Instead of an overt military invasion, the first volleys of a U.S. attack come from the installment of a political opposition through state propaganda (e.g., CNN, BBC), the Internet and social media, and nongovernmental organizations (NGOs). After successfully instilling political dissent, separatism, and/or social strife, the legitimate government has increasing difficulty maintaining order.
[8] Disponível em: https://www.nytimes.com/2019/12/27/us/politics/russia-hypersonic-weapon.html. Acesso em 20 de junho de 2020.
[9] Disponível em: <https://exame.com/mundo/internet-e-projeto-da-cia-diz-vladimir-putin/2/>. Acesso em: 04 de Junho de 2020.
[10]Disponível em: https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248

[11] [Tradução nossa] Texto original: "Огромные разрушительные последствия использования кибероружия в гибридной войне позволяют уже сегодня сравнивать масштабы его воздействия на вооруженные силы, промышленность, транспорт и население страны с результатами применения ядерного оружия. Это говорит о необходимости выдвижения так называемого кибернетического сдерживания на один уровень с ядерным"

organização social, econômica e política do país para se adaptar ao novo domínio. A visão que a Rússia possui sobre o âmbito cibernético diverge da visão ocidental tradicional de livre circulação de informações, especialmente no que diz respeito à percepção de ameaças (GILES, 2011). O ciberespaço é denominado pela Federação Russa como "espaço da informação" e a conceituação possui um fundamento holístico que passa por uma análise dos efeitos psicológicos e sociológicos que a disseminação de informações causa na sociedade (GILES, 2012).

No ano de 2011, o governo outorgou o documento "Convenção sobre Segurança Internacional da Informação"[12], responsável por indicar os objetivos do país no âmbito do ciberespaço e da segurança cibernética na esfera internacional. Nele, fica destacado o desejo do país em assegurar a livre troca de informações e tecnologias entre as nações, desde que isso não afete a soberania nacional e as características políticas, históricas e culturais da nação.

O governo russo demonstra vontade em cooperar internacionalmente de maneira a contribuir na construção de relações saudáveis entre os Estados no âmbito cibernético. Porém, ressalta que preza pela liberdade estatal no desenvolvimento do seu ciberespaço, sem interferências externas para determinar os seus interesses, métodos e o potencial militar que será utilizado para combater as ameaças e ações agressivas no espaço cibernético, de modo a garantir a sua segurança cibernética (FEDERAÇÃO RUSSA, 2011).

Um dos argumentos utilizados no documento são os esforços que a Rússia tem despendidos na Organização das Nações Unidas (ONU) para que a organização multilateral seja a principal responsável pela governança global da internet. Como principal exemplo empírico, o governo enfatiza a primeira Cúpula Mundial relacionada à governança da internet que ocorreu em 2003 e ficou conhecida como a Cúpula Mundial sobre a Sociedade da Informação (Cúpula Mundial da WSIS), realizada sob o gerenciamento da ONU. O maior resultado da Cúpula foi o estabelecimento do Grupo de Trabalho em Governança da Internet (WGIG), que contou com a participação ativa da Rússia (KASSENOVA, 2013).

Após dois anos, o governo russo elaborou o documento "Conceito da Estratégia de Segurança Cibernética Russa (2013)"[13], expondo que a natureza transfronteiriça do ciberespaço, sua dependência em tecnologias da informação e o seu uso pelos cidadãos russos ocasionam novas oportunidades, como a digitalização de serviços e modernização de processos administrativos, mas ao mesmo tempo desenvolvem novas ameaças ao país, como possíveis

[12] [Tradução nossa] Texto original: Convention on International Information Security.
[13] [Tradução nossa] Texto original: КОНЦЕПЦИЯ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ.

danos aos direitos, interesses e meios de subsistência de um indivíduo, organização e/ou órgãos governamentais (FEDERAÇÃO RUSSA, 2013, p. 1)[14].

O Estado, o setor privado e a sociedade civil são elencados como os setores fundamentais na estratégia russa. O documento delimita as funções desses atores, sendo o Estado responsável pela regulação legal da segurança cibernética e pela coordenação entre os atores; as corporações privadas são encarregadas por garantir a segurança cibernética das infraestruturas críticas de propriedade privada, implementando os padrões de segurança definidos pelo poder público; e a sociedade civil tem a responsabilidade de aumentar a sua consciência digital e fornecer feedbacks aos esforços governamentais e empresariais (FEDERAÇÃO RUSSA, 2013).

Sendo assim, a cooperação entre os três setores é levada em consideração pelo governo russo para atingir uma segurança cibernética capaz de salvaguardar a nação, pois a parceria entre eles estimula e promove o desenvolvimento tecnológico do país (FEDERAÇÃO RUSSA, 2013). No documento "Doutrina da Segurança da Informação na Federação Russa (2016)"[15], é avaliado que a dependência em componentes eletrônicos, *softwares*, computadores e equipamentos de telecomunicação do exterior pode comprometer o desenvolvimento socioeconômico do país e colocar a Rússia em uma situação de vulnerabilidade perante os interesses geopolíticos dos outros países (FEDERAÇÃO RUSSA, 2016).

Dessa forma, as metas para o ciberespaço estabelecidas pelo governo são apresentadas na publicação oficial "Estratégia para o Desenvolvimento da Sociedade da Informação na Federação Russa para 2017-2030 (2017)"[16], consistindo: "(i) na formação de um espaço da informação que leve em consideração as necessidades dos cidadãos russos em obter informações confiáveis e de qualidade; (ii) no desenvolvimento da infraestrutura de informação e comunicação na Federação Russa; (iii) na criação e aplicação de tecnologias da informação e comunicação russas, assegurando sua competitividade internacional; (iv) na formação de uma nova base tecnológica para o desenvolvimento das esferas econômicas e sociais; (v) na garantia dos interesses nacionais na área da economia digital" (FEDERAÇÃO RUSSA, 2017, p. 5)[17].

---

[14] [Tradução nossa] Texto original: нанесения урона правам, интересам и жизнедеятельности личности, организации, государственных органов.

[15] [Tradução nossa] Texto original: Doctrine of Information Security of the Russian Federation.

[16] [Tradução nossa] Texto original: О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы.

[17] [Tradução nossa] Texto original: а) формирование информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных сведений; б) развитие информационной и коммуникационной инфраструктуры Российской Федерации; в) создание и применение российских информационных и коммуникационных технологий, обеспечение их конкурентоспособности на

Outro ponto enfatizado pelo governo russo é o aspecto da soberania nacional. No mesmo documento expressa-se a necessidade de adaptar as regulações estatais da esfera informacional de maneira interna para proteção da soberania, já que os mecanismos legais internacionais são insuficientes para defender as soberanias dos Estados e regulamentar uma sociedade da informação a nível global (FEDERAÇÃO RUSSA, 2017). É importante ressaltar que não há normas e convenções internacionais formais que regulam o ciberespaço global, bem como não há uma governança global da internet. A Federação Russa observa isso como um aspecto desfavorável, visto que considera que muitos países estão construindo e aprimorando suas capacidades tecnológicas da informação perseguindo propósitos militares (FEDERAÇÃO RUSSA, 2016).

Desse modo, enquanto não se estabelece um cenário internacional que passe confiança de estabilidade e cooperação ao governo russo, a tendência é que o país continue se fortalecendo e se organizando internamente nessa área, tanto defensiva quanto ofensivamente. A visão estratégica que possui em relação ao ciberespaço perpassa pela sua grande preocupação com a soberania nacional e com o sentimento de grandeza destacado. Na ausência de regulamentos e normas internacionais para o espaço cibernético, a Rússia considera que o uso irrestrito desse ambiente é capaz de afetar o cenário doméstico e causar instabilidades no país. Isso se torna ainda mais preocupante se adicionado ao aspecto de que a informação tem sido a principal estratégia do Ocidente para desestabilizar regimes não-ocidentais, conforme apontamos. A concepção russa para a proteção das informações em território nacional, portanto, é justificada pela ameaça externa que o ciberespaço global representa na percepção do país.

Referências Bibliográficas

BARTOSH, A.A. *Estratégia de Guerra Híbrida e Estratégia de Construção*. 2018. Disponível em: <https://vm.ric.mil.ru/Stati/item/138034/>. Acesso em: 06 de dezembro de 2019.

BARTLES, Charles K. "*Getting Gerasimov Right".* Military Review, v. 96, n. 1, p. 30-38, 2016.

FEDERAÇÃO RUSSA, Ministério das Relações Exteriores. *Convention on International Information Security (Convenção sobre Segurança da Informação Internacional),* 22 de Setembro de 2011. Disponível em:

международном уровне; г) формирование новой технологической основы для развития экономики и социальной сферы; д) обеспечение национальных интересов в области цифровой экономики.

<https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666>. Acesso em: 14 de Maio de 2020.

FEDERAÇÃO RUSSA, Conselho Federativo. *КОНЦЕПЦИЯ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ (Conceito da Estratégia de Cibersegurança da Rússia).* 2013. Disponível em: <http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf>. Acesso em: 14 de Maio de 2020.

FEDERAÇÃO RUSSA, Decreto Presidencial. *Doctrine of Information Security of the Russian Federation (Doutrina da Segurança da Informação da Federação Russa),* nº 646, 5 de Dezembro de 2016. Disponível em: <https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163>. Acesso em: 14 de Maio de 2020.
.

FEDERAÇÃO RUSSA, Decreto Presidencial. *О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы. (Estratégia para o Desenvolvimento da Sociedade da Informação na Federação Russa para 2017-2030),* nº 203, 9 de Maio de 2017. 2017a. Disponível em: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102431687>. Acesso em: 14 de Maio de 2020.

GERASIMOV, Valery. *"The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations*". Voyenno-Promyshlennyy Kurier online. Disponível em: http://vpk-news.ru/articles/14632. Acesso em: 13 de outubro de 2019.

GILES, Keir. *" 'Information Troops' - a Russian Cyber Command?".* 3rd International Conference on Cyber Conflict. Tallinn, Estonia, 2011, CCD COE Publications.

GILES, Keir. *"Russia's Public Stance on Cyberspace Issue".* 4th International Conference on Cyber Conflict. NATO CCD COE Publications, Tallinn, 2012.

KASSENOVA, Madina. *"Fundamentos da governança da Internet transfronteiriça".* In: M.B; DEMIDOV, O.V. "*Segurança Cibernética e governança da Internet: documentos e materiais - para os reguladores e especialistas russos*". M: Estatuto, 2013, p. 8-46.

LO, Bobo. *Going Legit? The Foreign Policy of Vladimir Putin*. 2018. Lowy Institute. Disponível em: https://www.lowyinstitute.org/publications/going-legit-foreign-policy-vladimir-putin. Acesso em 06 de dezembro de 2019.

SANTANA, Carlos Henrique Vieira. *"Políticas de infraestrutura Energética e Capacidades Estatais nos BRICS".* Instituto de Pesquisa Econômica Aplicada, IPEA, Brasília, nº2045, 2015.

SVARIN, David. *"The construction of 'geopolitical spaces' in Russian foreign policy discourse before and after the Ukraine crisis".* Journal of Eurasian Studies, v. 7, n. 2, p. 129-140, 2016.