Observatório Militar da Praia Vermelha

Coletânea de Artigos - 2019

Escola de Comando e Estado-Maior do Exército

COLETÂNEA DE ARTIGOS - 2019

OBSERVATÓRIO MILITAR DA PRAIA VERMELHA

COLETÂNEA DE ARTIGOS - 2019

Organizador

Coronel Anselmo de Oliveira Rodrigues

Esta coletânea é constituída de artigos confeccionados por colaboradores do OMPV sobre assuntos relacionados à segurança e defesa.

ECEME

2023

COORDENAÇÃO GERAL
General de Brigada Sergio Manoel Martins Pereira Junior
Comandante da Escola de Comando e Estado-Maior do Exército

ORGANIZADOR
Coronel QEMA Anselmo de Oliveira Rodrigues
Coordenador do Observatório Militar da Praia Vermelha

REVISORES DE LINGUAGEM
Tenente-Coronel Carmem Lucia Napoleão Xavier
Professora de Inglês da ECEME

Major Helena Rodrigues Rocha Martins de Oliveira
Professora de Espanhol da ECEME

Major Mônica da Silva Boia
Professora de Espanhol da ECEME

Capitão Kelly Cristina Moraes de Lima
Professora de Inglês da ECEME

1º Tenente Raquel Luciano Gomes
Professora de Inglês da ECEME

1° Tenente Bruna Renova Varela Leite
Professora de Espanhol da ECEME

DIAGRAMAÇÃO E DESIGN GRÁFICO DA CAPA
Coronel QEMA Anselmo de Oliveira Rodrigues
Responsável pela diagramação

Gabriel dos Santos Andrade de Oliveira
Responsável pelo design gráfico da capa

O120 Observatório Militar da Praia Vermelha: Coletânea de artigos - 2019
Organizador: Coronel Anselmo de Oliveira Rodrigues
Rio de Janeiro: ECEME, 2023.

91 p. Inclui bibliografia

ISBN: 978-85-64844-10-0

1. Cibernética. 2. Geopolítica. 3. Estratégia. 4. Movimentos migratórios. 5. DQBRN.

CDD 355

SUMÁRIO

APRESENTAÇÃO

Anselmo de Oliveira Rodrigues [*]

Como Coordenador do Observatório Militar da Praia Vermelha, é com grande satisfação que apresento a Coletânea de Artigos do Observatório Militar da Praia Vermelha - 2019. Fruto de um trabalho realizado ao longo de 10 meses no ano de 2022, esta coletânea apresenta os artigos quer foram publicados no site do OMPV no ano de 2019.

Em seu segundo ano de funcionamento, o Observatório Militar da Praia Vermelha realizou significativas contribuições para a sociedade em assuntos relacionados à segurança e defesa, fomentando o debate e apresentando boas análises em temas como cibernética, DQBRN, geopolítica, estratégia, movimentos migratórios e terrorismo.

A Coletânea de Artigos do Observatório Militar da Praia Vermelha - 2019 está organizada por áreas temáticas e possui um total de 19 artigos, que foram assinados por 14 distintos autores. Em cada área temática, os artigos estão posicionados de acordo com a ordem cronológica de sua publicação no site do OMPV ao longo de 2019.

A área temática ***cibernética*** inaugura esta coletânea e apresenta 7 artigos que foram publicados sobre o tema em 2019, revelando dessa forma, o maior esforço feito pelo OMPV em 2019. A área temática ***DQBRN*** contém dois artigos que foram publicados sobre o assunto em 2019. A área temática ***geopolítica e estratégia*** gerou grandes contribuições em 2019 e apresenta 6 artigos que foram publicados sobre a temática nesse ano. Na sequência, a área temática ***movimentos migratórios*** apresenta dois artigos que foram publicados sobre o tema em 2019. A área temática ***terrorismo*** finaliza esta coletânea e apresenta apenas 1 artigo que foi publicado sobre o assunto em 2019.

Espero que os leitores gostem dos artigos publicados nessa coletânea, da mesma forma que aproveito a oportunidade para convidar todos os integrantes da sociedade a publicarem seus manuscritos sobre defesa e segurança no site do Observatório Militar da Praia Vermelha. Afinal, a Defesa não é exclusiva dos militares, ela é um tema que requer a contribuição de todos os integrantes da sociedade!!!

[*] Coronel do Exército Brasileiro e Coordenador do Observatório Militar da Praia Vermelha.

CIBERNÉTICA

CUSTOS ECONÔMICOS DA GUERRA CIBERNÉTICA*

***Marcos Luiz da Cunha de Souza*[1]**
***Luiz Rogério Franco Goldoni*[2]**

Em matéria publicada na agência de notícias Reuters, em janeiro de 2019, a empresa privada estadunidense *Strategic Cyber Ventures*, que atua oferecendo serviços estratégicos de consultoria em capital de risco, apontou o panorama do campo cibernético, seus perigos e possibilidades (DREYFUSS, 2019). Em seu relatório é demonstrado um aumento de 20% nos investimentos em capital de risco de 2017 para 2018, que, subiram da casa dos 4,4 bilhões de dólares para 5,3 bilhões. Vale ressaltar, que o investimento em capital de risco se trata de uma modalidade alternativa que busca uma participação acionária geralmente minoritária, com objetivo de valorizar as ações para uma posterior saída de operação.

O cientista de dados e diretor da *Strategic Cyber Ventures*, *Chris Ahern*, afirmou que os investimentos em capital de risco se devem sobretudo pela maior ocorrência de "megaviolações" cibernéticas. Contudo, percebe que essa incidência representa uma maior oportunidade para os investidores e se tornou uma preocupação para governos e corporações de todo o mundo, à medida que os crimes cibernéticos de alto vulto crescem, como será visto adiante nos documentos estratégicos dos países envolvidos em casos recentes. Ressalta-se que dados apresentados pela empresa de segurança cibernética *ThreatMetrix* mostraram um aumento percentual de 100% nos ataques cibernéticos desde 2015.

Segundo *Chris Ahern*, a fuga de grandes empresas de tecnologia dos Estados Unidos da América, alvo majoritário dos ataques cibernéticos, é um grande problema para o país; por outro lado, outras nações lucram ao receber empresas que buscam um novo "porto seguro". O cofundador e CEO da *Strategic Cyber Ventures*, *Thomas Hank*, considera que o maior perigo à segurança cibernética do mundo é o Exército Popular de Libertação, as Forças Armadas chinesas. Essa afirmação pode ter sérias implicações, visto que a acusação pode estar relacionada justamente com o "problema central" da migração forçada dessas organizações para outras regiões, como a Ásia e

* Artigo originalmente publicado no dia 25 de janeiro de 2019 no site do OMPV.
[1] Graduando em Defesa e Gestão Estratégica Internacional.
[2] Doutor em Ciência Política e Professor da ECEME.

principalmente a China.

No que se refere a defesa cibernética, o documento da Estratégia Nacional de Defesa dos Estados Unidos de 2018 reconhece a necessidade de se antecipar aos ataques e enxerga a América como principal alvo no campo cibernético. Também afirma que a área cibernética é prioridade para o governo, garantindo investimentos contínuos para reconstituir e assegurar capacidades cibernéticas em todo espectro das operações militares, transformando o espaço cibernético em um domínio de combate (USA, 2018). Dito isto, a estratégia também estabelece a intenção do país de responsabilizar os atores estatais ou não estatais durante ataques cibernéticos.

Portanto, a condenação feita por *Thomas*, CEO de uma empresa que tem a finalidade de mapear e produzir prognósticos sobre o campo cibernético para investimentos em capital de risco, pode ter sérias consequências em caso de se comprovar suas suspeitas, uma vez que a estratégia dos Estados Unidos da América tem o intuito de responsabilizar, por meios legais, os autores de quaisquer ataques cibernéticos a empresas estadunidenses.

O custo dos danos causados por hackers está se tornando cada vez maior para governos e empresas. Um caso que chama atenção é o das seguradoras que passaram a se recusar a cobrir determinados ataques cibernéticos, alegando que muitos dos danos infligidos aos seus segurados são efeitos colaterais oriundos de guerras cibernéticas entre nações; logo, quem deveria arcar com os prejuízos seriam as mesmas. Esse cenário indica, mais uma vez, como o setor privado está enxergando os conflitos nesse campo, fazendo diagnósticos e prognósticos conjunturais e, até mesmo, acusando ou constatando a ocorrência de guerras.

Para ilustrar esse evento, em janeiro de 2019, a CNN publicou uma notícia sobre o confronto entre duas grandes empresas suíças na arena legal. A situação envolvia a recusa da seguradora *Zurich Insurance* em cobrir os ataques cibernéticos sofridos pela empresa alimentícia *Mondelez* (KOTTASOVÁ , 2019). O argumento usado foi o da iminência de uma possível guerra cibernética envolvendo a Rússia.

O temor por parte das seguradoras a ataques cibernéticos surgiu após os acontecimentos de junho de 2017, com o ataque que ficou conhecido como *NotPetya*. Esse ataque foi considerado tanto pelos Estados Unidos quanto pelo Reino Unido como tendo sido provocado por organizações russas, sugerindo um esforço para desestabilizar a Ucrânia. O diferencial desse ataque foi seu caráter generalizado, no qual, muitas organizações que faziam uso do seguro foram afetadas simultaneamente, o que mudou

drasticamente sua atuação, visto que um assalto ou roubo específico dificilmente acontece múltiplas vezes e ao mesmo tempo

Entretanto, ainda não há grandes certezas sobre quem deveria ser responsabilizado em casos de ataques em larga escala ou guerras cibernéticas. A OTAN, na ficha informativa de fevereiro de 2018 se posicionou acerca da questão ucraniana destinando fundos ao país para este ser capaz de promover suas próprias defesas cibernéticas e se manter resiliente diante de ataques como o *NotPetya*. Apesar disso, a Organização, além de afirmar que a maioria dos ataques aos Aliados se destinam às grandes empresas, retira sua responsabilidade e incumbe os próprios países membros por suas defesas (OTAN, 2018). A OTAN se prontifica a atuar apenas mediante auxílio a seus integrantes em caso de ataques, com o compartilhamento de informações, treinamentos conjuntos e cessão de especialistas em casos emergenciais, se necessário.

Por seu turno, a Estratégia Nacional para a proteção da Suíça contra riscos cibernéticos (2018-2022) estabelece que se proteger contra qualquer espécie de risco cibernético é responsabilidade conjunta da sociedade, do setor privado e do Estado (SWITZERLAND, 2018). O governo federal, os cantões e as comunas são diretamente responsáveis pela salvaguarda da infraestrutura crítica, que compreende, os serviços de administração e autoridades públicas. No entanto, uma grande parte do sistema de tecnologia da informação suíça é operada por empresas privadas e essas têm responsabilidade pela proteção dessa infraestrutura crítica e por manter um bom serviço.

Tanto a OTAN quanto a Suíça possuem uma forma semelhante para lidar coma ameaça cibernética: não se responsabilizar diretamente pelos ataques e organizar uma resposta conjunta. Por seu turno, os EUA adotam uma abordagem diferente e arcam com a responsabilidade a fim de minar os esforços de seus adversários e constituir o espaço cibernético como um campo de batalha no qual eles pretendem dominar, o que se justifica por ser o maior alvo do mundo tanto de terrorismo cibernético, sabotagem ou ataques em massa. No meio dessa nova guerra, marcada por incertezas e anonimato, empresas investem bilhões de dólares, custo pago por toda a sociedade.

Referências:

DREYFUSS, Gertrude. **Venture capital funding of cybersecurity firms hit record high in 2018: report.** Reuters, 2019. Disponível em: https://www.reuters.com/article/us-usa-cyber-investment/venture-capital-funding-of-cybersecurity-firms-hit-record-high-in-2018-report-idUSKCN1PB163. Acesso em: 25 de janeiro de 2019.

KOTTASOVÁ, Ivana. **Hacks can cost businesses millions - Insurers may refuseto pay up.** CNN, 2019. Disponível em: https://edition.cnn.com/2019/01/11/business/cyber-attacks-insurance/index.ht ml. Acesso em: 25 de janeiro de 2019.

OTAN. **NATO - Cyber Defence Fact Sheet 2018.** Disponível em: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/20180213_1802-factsheet-cyber-defence-en .pdf. Acesso em: 26 de janeiro de 2019.

SWITZERLAND. **National strategy for Switzerland's protection against cyber risks.** Zurique: Federal Council, 2018.

UNITED STATES OF AMERICA. **National Defense Strategy.** Washington: Department of Defense, 2018.

ESTADOS UNIDOS E RÚSSIA: ESBOÇOS DE TERRITORIALIDADE NO CIBERESPAÇO?*

***Marcos Luiz da Cunha de Souza*[1]**
***Breno Pauli Medeiros*[2]**
***Luiz Rogério Franco Goldoni*[3]**

Em matéria de 12 de fevereiro do corrente, o jornal *The Washington Post* destaca o discurso do Secretário de Estado dos Estados Unidos, *Mike Pompeo*, a respeito da aproximação dos países da Europa Oriental com a empresa chinesa de telecomunicações *Huawei*. Pompeo ressaltou o perigo da influência chinesa e russa na região para os membros da União Europeia e aliados da OTAN (LEE, 2019).

Segundo o Secretário de Estado norte-americano, as nações teriam que optar entre manter relações com a *Huawei* ou os Estados Unidos. Tal retórica ganha outro vulto em vista do local da declaração: a Eslováquia. A *Huawei* é percebida como um grande ator cibernético e de comunicações digitais nos países do leste europeu. Por detrás desse discurso pairam apreensões relativas ao iminente advento da internet 5G, tecnologia fornecida pela empresa chinesa na região. A busca pela proeminência dos EUA relativa às tecnologias de comunicação, inclusive, é destacada no documento *National Cyber Strategy of United States of America* de 2018 (USA, 2018a).

O espaço cibernético é compreendido pelos EUA, em sua Estratégia Nacional de Defesa de 2018, como um domínio de combate e prioridade para o governo. Nesse sentido, fica clara a pretensão dos EUA em controlar a tecnologia 5G e a percepção da mesma como uma ferramenta desse novo campo de batalha:

> *"The United States Government will work with the private sector to facilitate the evolution and security of 5G, examine technological and spectrum-based solutions, and lay the groundwork for innovation beyond next-generation advancements"* (USA, 2018b)[4].

O Secretário de Estado também apontou que o período do pós-Guerra Fria, por ele denominado de "década do desacoplamento", criou um vácuo permitindo ações mais

* Artigo originalmente publicado no dia 12 de fevereiro de 2019 no site do OMPV.
[1] Graduando em Defesa e Gestão Estratégica Internacional.
[2] Doutorando em Ciências Militares na ECEME.
[3] Doutor em Ciência Política e Professor da ECEME.
[4] "O Governo dos Estados Unidos trabalhará com o setor privado para facilitar a evolução e a segurança do 5G, examinar soluções tecnológicas baseadas em espectro e estabelecer as bases para a inovação além dos avanços da próxima geração" (USA, 2018b - tradução nossa).

incisivas e incursões na Europa Oriental tanto pela Rússia quanto pela China. Vale ressaltar, que em seu discurso, *Pompeo* deu garantias para o povo eslovaco e demais países, considerados por ele como vítimas do sufocante poder russo e chinês, que os Estados Unidos da América estarão engajados e presentes no local.

Ainda em conformidade com a reportagem do *Washington Post*, a resposta dada pela porta voz do Ministério das Relações Exteriores da China, *Hua Chunying*, salientou que os esforços feitos pelos Estados Unidos da América fazem parte de uma campanha injusta e imoral para desestabilizar os parceiros comerciais chineses, por intermédio da criação de teorias e ameaças como forma de intimidação. Consequentemente, o CEO da empresa *Huawei*, *William Wu*, encorajou que todos os governos observassem de forma objetiva as evidências de quaisquer ameaça e mantivessem uma postura interessada e aberta para a criação das redes 5G. Além disso, afirmou que excluir um fornecedor de desenvolvimento tecnológico em segurança cibernética prejudicará o progresso técnico como um todo e irá gerar distúrbios no mercado em relação à concorrência.

Os acontecimentos mencionados se relacionam com uma temática que vem ganhando proeminência em decorrência da interação humana no ciberespaço: a questão da territorialidade no domínio cibernético. Essa temática se torna ainda mais complexa quando consideradas as lógicas de poder do domínio cibernético e das concepções tradicionais de território.

A ampla compreensão de territorialidade que fundamenta as relações internacionais atuais tende a considerá-la como a "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" (HAESBAERT, 2002, p. 119). Nesse sentido, a delimitação de um recorte espacial no qual o Estado opera internamente e externamente, mediante o controle de fluxos de entrada e saída de pessoas, mercadorias e informações, configura uma lógica zonal de poder.

Por outro lado, apreciada a definição de ciberespaço proposta pelo Dicionário de Termos Militares do Departamento de Defesa Norte-Americano como sendo um domínio global dentro do ambiente de informações que consiste na rede interdependente de infraestruturas de tecnologia da informação e dados residentes, incluindo a Internet, redes de telecomunicações, sistemas de computadores, processadores e controladores integrados (USA, 2019) e que deve ser destacada a concepção do ciberespaço como um domínio composto por camadas físicas (a infraestrutura e *hardware*) e a camada

imaterial (*software*, informações e dados de maneira geral). Nesse contexto, as camadas imateriais se interconectam por intermédio dos fluxos informacionais que compõem a internet e outras redes, correspondendo a uma lógica reticular, dessemelhante da lógica zonal tradicional do território.

No entanto, a compreensão do ciberespaço como domínio de interconectividade global não impediu os Estados Unidos da América e outros países de tomarem medidas de exclusão a certos produtos como uma tentativa de territorializar o espaço cibernético mediante o controle das formas de acesso ao mesmo. Isto é, ao negar a entrada e/ou a utilização de determinados produtos (seja de *software* ou *hardware*), os países de origem dos mesmos não teriam acesso ao território cibernético em questão. Dessa forma, diante da dificuldade de se controlar fluxos digitais e imateriais, Estados tentam aplicar sua territorialidade sobre aspectos mais tangíveis do ciberespaço, proibindo a utilização de determinados produtos oriundos de outros países.

Essa prática carece de certa objetividade, visto que o ciberespaço é composto por uma complexa rede de camadas físicas e imateriais; e devido ao fato de que medidas tradicionais de controle zonal dos fluxos materiais não necessariamente se aplicam à lógica reticular de fluxos digitais do ciberespaço.

Outro evento que ilustra a concepção de exclusão com vistas a origem da empresa ou *software* foi o reconhecimento da ameaça de se ter um *software* russo nos computadores dos civis e militares do governo dos Estados Unidos da América em 2017. Isto se evidenciou pelo banimento dos sistemas da empresa *Kaspersky Lab*, que fornecia proteção cibernética por meio de programas antivírus, por um projeto de lei sancionado pelo senado norte-americano (VOLZ, 2017).

Ainda no que se refere às interferências governamentais no ciberespaço, também em fevereiro deste ano, *Vladimir Putin* reafirmou que seu país se desconectará da internet para testar a resiliência russa em caso de um ataque cibernético. A intenção é avaliar a capacidade de independência da *Runet*, a *internet* russa, das demais redes. O ambicioso projeto proposto pelo parlamento russo, em dezembro de 2018, teria como fim criar conexões próprias mediante pontos de troca de informações gerenciadas pela *Roskomnadzor*, a agência reguladora de telecomunicações e mídia da Rússia.

Devido à intrincada interconectividade das camadas de *hardware* e *software* que permeiam o ciberespaço, é extremamente difícil rastrear ou mapear as conexões e/ou o país de origem dos serviços utilizados. Nesse contexto, o desligamento da internet russa pode resultar em sérias implicações não somente para a Rússia como, também, para o

resto das redes no mundo, como aponta *Paul Barford*, professor da Universidade de *Wisconsin-Madison* que estuda redes de computadores (MATSAKIS, 2019). A interrupção das conexões pode suscitar falhas catastróficas que poderiam extrapolar para além do território russo e até mesmo causar danos sistêmicos, se espalhando pelo ciberespaço e afetando até o funcionamento de sistemas de transportes e hospitais alhures.

Segundo *Andrew Sullivan*, CEO da organização sem fins lucrativos *Internet Society* - que promove o desenvolvimento da internet aberta, a Rússia busca construir um sistema que possua caminhos alternativos e possa ser desligada a qualquer momento. Contudo, para *Sullivan*, isso enfraqueceria a rede russa, visto que, a tornará menos confiável e possível de ser desligada "acidentalmente", já que ela poderá ser desativada propositalmente, facilitando ataques como *shutdowns*, que buscam desligar computadores ou redes em massa (MATSAKIS, 2019).

As medidas de exclusão tomadas pelos estadunidenses provocaram reações diferentes para cada um dos países e seus produtos excluídos nos casos supracitados. A China, por intermédio de seu Ministério das Relações Exteriores, argumenta que a postura adotada no caso da *Huawei* pode ser interpretada como antidemocrática. Por seu turno, a Rússia e o teste do desligamento podem ser encaradas como um reflexo das práticas adotadas pelos Estados Unidos em relação a proibição dos *softwares* russos e discursos proferidos com intuito de construir uma narrativa de ameaça. O teste, para além de uma tentativa de tornar a Rússia independente da internet global, também pode ser interpretado como um reforço das suas capacidades de ciber guerra.

Referências:

HAESBAERT, R. **Territórios Alternativos.** São Paulo: Contexto, 2002.

LEE, Matthew. **Pompeo warns eastern Europe on Chinese and Russian meddling.** The Washington Post, 2019. Disponível em: https://www.washingtonpost.com/business/technology/pompeowarns-eastern-europe-on-chinese-andrussian-meddling/2019/02/12/bd7bb2a0-2ecd-11e9-8781-763619f12cb4_story.html?utm_term=.dcfad946931d. Acesso em: 20 de janeiro de 2019.

MATSAKIS, Louise. **What happens if Russia cut itself off from the internet.** Wired, 2019. Disponível em: https: //www.wired.com/story/russia-internet-disconnect-whathappens. Acesso em: 20 de janeiro de 2019.

USA. **National Cyber Strategy of United States of America.** Washington: White House, 2018a.

USA. **National Defense Strategy.** Washington: Department of Defense, 2018b.

USA. **Dod dictionary of military and associated terms -** 2019. Washington: Department of Defense, 2019.

VOLZ, Dustin. **Trump signs into law U.S. government ban on Kaspersky Lab software.** Reuters, 2017. Disponível em: https://www.reuters.com/article/us-usa-cyber-kaspersky/trumpsigns-into-law-u-s-government-ban-on-kaspersky-lab-softwareidUSKBN1E62V4. Acesso em: 20 de janeiro de 2019.

INFRAESTRUTURA BÁSICA E VULNERABILIDADES CIBERNÉTICAS*

***Marcos Luiz da Cunha de Souza*[1]**
***Breno Pauli Medeiros*[2]**
***Luiz Rogério Franco Goldoni*[3]**

Em matéria de 18 de março do corrente, a revista *Time* noticiou declaração dada por *Nicolás Maduro,* acusando os Estados Unidos da América de terem efetuado ataques cibernéticos contra a Venezuela, que resultaram no blecaute pelo qual o país passou recentemente (GUNIA, 2019). Segundo *Maduro*, "*Donald Trump* é o maior responsável pelo ataque ao sistema elétrico venezuelano". O Presidente venezuelano interpreta que esses esforços são uma tentativa estadunidense de derrubá-lo, uma vez que, na visão dele, *Juan Guaidó* seria "um fantoche dos Estados Unidos".

Conforme a *Al Jazeera*, especialistas norte-americanos discordam que um ataque cibernético tenha causado o problema na rede elétrica venezuelano. Segundo eles, a causa do blecaute foi um impedimento técnico na ligação entre as usinas hidrelétricas do país e a distribuição de energia (AL JAZEERA, 2019). Os danos provocados pela falta de luz no país se alastraram para a indústria de petróleo, interrompendo as exportações do principal terminal petrolífero. Houve também paralisia em hospitais, aeroportos e na vida da população de um modo geral, uma vez que os mercados foram fechados. Além dos danos financeiros, o blecaute resultou em protestos por todo país em oposição a *Maduro*.

No decorrer do mês, a *Reuters* publicou matéria que de certa forma endossa a fala do presidente *Nicolás Maduro* veiculada na revista *Time*. Esse artigo apresenta uma denúncia de um funcionário do governo dos Estados Unidos da América (que preferiu manter o anonimato) sobre a presença de especialistas em cibersegurança no contingente de 100 militares russos que chegaram em dois aviões da força aérea desse país que pousaram no maior aeroporto da Venezuela em *Maiquetia* (SPETALNICK, 2019). Conforme esse funcionário, os Estados Unidos da América estariam convictos de que a missão de parte do contingente russo seria a de apoiar o regime de Maduro na vigilância e proteção da infraestrutura cibernética venezuelana.

---

* Artigo originalmente publicado no dia 18 de março de 2019 no site do OMPV.

[1] Graduando em Defesa e Gestão Estratégica Internacional.
[2] Doutorando em Ciências Militares na ECEME.
[3] Doutor em Ciência Política e Professor da ECEME.

A Rússia é um dos poucos países que ainda apoiam *Maduro* (KURMANAEV, 2019). Dias antes da matéria da *Reuters*, os presidentes dos dois países haviam se reunido; o Ministério das Relações Exteriores da Rússia esclareceu que a chegada de especialistas russos na Venezuela seria fruto de um acordo de cooperação técnico-militar feita entre os dois países (SPETALNICK, 2019).

Caso comprovado, o ataque cibernético à rede elétrica venezuelana não seria o primeiro desse gênero a acontecer contra um país. Em 2016, a rede elétrica ucraniana foi alvo de ataques cibernéticos que causaram um blecaute em *Kiev* (ZETTER, 2016). Relatórios de segurança cibernética realizados pelas empresas *ESET* e *Dragos*, revelaram que hackers haviam desenvolvido um malware chamado "*Crash Override*", que teria a capacidade de desativar redes elétricas a distância. O mesmo havia acontecido em 2015, também na Ucrânia, quando hackers foram capazes de acessar fisicamente a rede e sobrecarregar a grade elétrica (CHEREPANOV, 2017; DRAGOS INC, 2017).

O caso de 2015 foi associado ao de 2016 pela empresa de segurança cibernética *Honeywell*, que atribuiu o ataque ao grupo "*Sandworm*" (ZETTER, 2017). O contexto do incidente foi durante a ocupação russa na Crimeia, região que, na época, ainda fazia parte da Ucrânia. Outra empresa de segurança cibernética a responsabilizar os russos pelo ataque foi a *FireEye*, que por intermédio de seu diretor de análise de inteligência, *John Hultquist*, afirmou que o ataque foi perpetrado por agentes de segurança contratados ou funcionários do governo russo (GREENBERG, 2017).

A atuação russa no domínio cibernético também foi comentada em análise feita previamente neste espaço, que abordou a declaração de *Putin* sobre o teste de desligamento da internet russa por um dia. Os argumentos a favor do teste remetem à tentativa de garantir a independência russa da internet global, se resguardando de eventuais ataques. Contudo, o mesmo também demonstraria a capacidade da Rússia de operar suas infraestruturas sem a dependência da infraestrutura cibernética internacional, o que reforçaria sua defesa contra um ataque do gênero.

A maior interconectividade das infraestruturas sensíveis de diferentes países representa um avanço tecnológico e é tida como positiva; entretanto, pode acarretar dependências e eventuais vulnerabilidades. Nesse contexto, governos vêm priorizando a defesa do ciberespaço nos documentos de defesa da última década e sobretudo a resiliência de suas infraestruturas em rede (BRASIL, 2016; USA, 2018; GERMANY, 2016; FRANCE, 2013).

Infraestrutura básica e vulnerabilidades cibernéticas

Nos documentos brasileiros que abrangem o setor cibernético, é possível perceber a atenção dada para a proteção das infraestruturas básicas. O Livro Verde: Segurança Cibernética no Brasil, publicado em 2010, elenca os principais níveis de ação que envolvem a defesa cibernética, dentre os quais: político-estratégico, econômico, social e ambiental, cooperação internacional e segurança das infraestruturas críticas. No referido documento, também fica clara a intenção de fomentar a capacitação dos recursos humanos e estimular a cooperação internacional para aumentar a resiliência dessas infraestruturas (BRASIL, 2010).

Outro documento importante lançado dois anos depois, em 2012, é o Livro Branco de Defesa Nacional (LBDN), que atribui ao Exército a defesa do espaço cibernético (BRASIL, 2012). Em decorrência, foi criado o Centro de Defesa Cibernética (CDCiber), a Escola Nacional de Defesa Cibernética (ENaDeCiber) e o Comando de Defesa Cibernética (ComDCiber) estabelecido na versão mais recente do LBDN de 2016. Todos esses esforços fazem parte da percepção de novas ameaças. As agências supracitadas têm como dever resguardar o espaço cibernético por meio da capacitação de recursos humanos e proteção de infraestrutura básica do Estado (BRASIL, 2016).

Os Estados Unidos, por sua vez, abordam a questão das infraestruturas críticas no documento *National Cyber Strategy of United States of America* (2018), reconhecendo sua participação em uma corrida armamentista contínua no ciberespaço, contra adversários estatais e não estatais.

> *"The Administration recognizes that the United States is engaged in a continuous competition against strategic adversaries, rogue states, and Terrorist and criminal networks. Russia, China, Iran, and North Korea all use cyberspace as a means to challenge the United States, its allies, and partners, often with a recklessness they would never consider in other domains. These adversaries use cyber tools to undermine our economy and democracy, steal our intellectual property, and sow discord in our democratic processes. We are vulnerable to peacetime cyber attacks against critical infrastructure, and the risk is growing that these countries will conduct cyber attacks against the United States during a crisis short of war. These adversaries are continually developing new and more effective cyber weapons"* (USA, 2018)[4].

[4] A Administração reconhece que os Estados Unidos estão engajados em uma competição contínua contra adversários estratégicos, Estados párias e redes terroristas e criminosas. Rússia, China, Irã e Coréia do Norte usam o ciberespaço como um meio de desafiar os Estados Unidos, seus aliados e parceiros, muitas vezes com uma imprudência que jamais considerariam em outros domínios. Esses adversários usam ferramentas cibernéticas para minar nossa economia e democracia, roubar nossa propriedade intelectual e semear discórdia em nossos processos democráticos. Somos vulneráveis a ataques cibernéticos em tempo de paz contra infraestruturas críticas, e o risco é crescente de que esses países realizem ataques cibernéticos contra os Estados Unidos durante uma crise antes da guerra. Esses adversários estão continuamente desenvolvendo armas cibernéticas novas e mais eficazes" (USA, 2018 - tradução nossa).

O ciberespaço tem se tornado um campo de assimetrias que suscita conflitos que antes seriam impensáveis. Isto ocorre devido ao caráter anônimo e desterritorializado dos ataques, nos quais não se sabe a origem dos atacantes. Além disso, outro ponto importante que o documento cita é a corrida armamentista contínua não somente entre Estados, mas com outros atores não-estatais, como empresas e grupos particulares.

O blecaute na Venezuela pode ser visto como um ponto de inflexão e reforça a necessidade de se olhar para o ciberespaço como uma fonte de novas ameaças. Ainda não há provas de que o apagão tenha sido causado por um ataque cibernético, mas não teria sido o primeiro do gênero.

O Brasil e os Estados Unidos da América, abordados aqui, já possuem em seus respectivos documentos de defesa a intenção de se proteger contra ataques cibernéticos às infraestruturas básicas. Além disso, é notável que há uma corrida armamentista cibernética acontecendo e que países como a Rússia, Brasil e Estados Unidos da América já estão se precavendo e reforçando suas capacidades de se defender contra uma possível guerra cibernética (SOUZA; MEDEIROS; GOLDONI, 2019).

Referências:

AL JAZEERA. **Venezuela's Maduro: Blackout due to cyber-attack, infiltrators.** Al Jazeera, 2019. Disponível em: https://www.aljazeera.com/news/2019/03/venezuela-maduroblackout-due-cyber-attack-infiltrators-190310065500250.html. Acesso em: 20 de março de 2019.

BRASIL. MINISTÉRIO DA DEFESA. **Livro Verde: Segurança Cibernética no Brasil.** Brasília: Ministério da Defesa, 2010.

BRASIL. MINISTÉRIO DA DEFESA. **Livro Branco de Defesa Nacional.** Brasília: Ministério da Defesa, 2012.

BRASIL. MINISTÉRIO DA DEFESA. **Livro Branco de Defesa Nacional.** Brasília: Ministério da Defesa, 2016.

CHEREPANOV, Anton. **WIN32/INDUSTROYER - A new threat for industrial control systems.** ESET, 2017. Disponível em: https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32 _ Industroyer.pdf. Aceso em: 20 de março de 2019.

DRAGOS INC. **CRASH OVERRIDE - Analysis of the Threat to Electric Grid Operations.** Dragos, 2017. Disponível em: https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf. Acesso em: 20 de março de 2019.

FRANCE. **French White Paper on Defence and National Security.** Paris: République Française, 2013.

GERMANY. **White Paper on German Security Policy and the Future of the Bundeswehr.** Berlim: The Federal Government, 2016.

GREENBERG, Andy. **CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID.** Wired, 2017. Disponível em: https://www.wired.com/story/rashoverride-malware. Acesso em: 20 mar. 2019.

GUNIA, Amy. **Venezuela Blames U.S. for Record Blackout and Orders American Diplomats to leave.** Time, 2019. Disponível em: http://time.com/5550481/venezuela-maduro-blackout-cyber-sabotage. Acesso em: 20 de março de 2019.

KURMANAEV, Anatoly. **Russia Stands With Maduro (While Hedging Its Bets).** New York Times, 2019. Disponível em: https://www.nytimes.com/2019/03/08/world/americas/russiavenezuela-maduro-putin.html. Acesso em: 27 de março de 2019.

USA. **National Cyber Strategy of United States of America.** Washington: White House, 2018.

SOUZA, Marcos; MEDEIROS, Breno; GOLDONI, Luiz. **Estados Unidos e Rússia: Esboços de Territorialidade no Ciberespaço?** Observatório Militar da Praia Vermelha, 2019. Disponível em: http://ompv.eceme.eb.mil.br/docs/defesa_cibernetica/EUARussiaCiberespaco.pdf. Acesso em: 20 de março de 2019.

SPETALNICK, Matt. **Russian deployment in Venezuela includes 'cybersecurity personnel': U.S. official.** Reuters, 2019. Disponível em: https://www.reuters.com/article/usvenezuela-politics-russian s-idUSKCN1R72FX. Acesso em: 27 de março de 2019.

ZETTER, Kim. **Inside the cunning, unprecedented hack of Ukraine's power grid.** Wired, 2016. Disponível em: https://www.wired.com/2016/03/insidecunning-unprecedented-hack-ukraines-power-grid. Acesso em: 20 de março de 2019.

ZETTER, Kim **The Ukrainian Power Grid Was Hacked Again.** Motherboard, 2017. Disponível em: https://motherboard.vice.com/en_us/article/bmvkn4/ukrainianpower-station-hacking-december-2016-report. Acesso em: 20 de março de 2019.

A PERCEPÇÃO DE AMEAÇAS CIBERNÉTICAS NO DISCURSO NORTE-AMERICANO*

***Marcos Luiz da Cunha de Souza*[1]**
***Breno Pauli Medeiros*[2]**
***Luiz Rogério Franco Goldoni*[3]**

Em matéria de 4 de abril do corrente, a agência de notícias *Reuters* publicou as declarações feitas pelo Secretário de Estado dos Estados Unidos, *Mike Pompeo*, no âmbito da reunião de comemoração do 70º aniversário da OTAN. No discurso, Pompeu solicita que aliados se adaptem a ameaças emergentes, entre elas: intervenções militares da Rússia em lugares como a Venezuela; competição estratégica chinesa, figurada, principalmente pelo avanço da infraestrutura de telecomunicações 5G; migração descontrolada e riscos à segurança energética.

A temática cibernética foi central na fala de *Pompeo*, contribuindo para a narrativa securitária que categoriza China e Rússia como países que representam ameaças também no campo cibernético, como evidenciado em análises anteriores publicadas nesse portal.

A análise em tela foca no conceito de ameaças e como ele tem sido moldado ao longo dos discursos oficiais dos Estados Unidos da América e em seus mais recentes documentos estratégicos. Dentre as adversidades listadas no encontro supracitado, *Pompeo* destacou a competição estratégica chinesa referente à infraestrutura de telecomunicações, ilustrada no caso da expansão da rede de 5G da empresa chinesa *Huawei*.

A ampliação da narrativa para outros problemas de segurança internacional relaciona-se com a chegada recente de militares russos na Venezuela, após o blecaute de dez dias no país, supostamente ocasionado, nas palavras de *Maduro*, por um ataque cibernético perpetrado pelos Estados Unidos da América. Ainda, segundo informantes, acredita-se que dentre o efetivo militar russo, também se encontram especialistas em guerra cibernética para auxiliar na proteção da infraestrutura venezuelana, como tratado na análise do mês de março.

---

* Artigo originalmente publicado no dia 04 de abril de 2019 no site do OMPV.
[1] Graduando em Defesa e Gestão Estratégica Internacional.
[2] Doutorando em Ciências Militares na ECEME.
[3] Doutor em Ciência Política e Professor da ECEME.

Em resposta ao posicionamento dos Estados Unidos da América, o Ministro das Relações Exteriores da Venezuela, *Ivan Gil*, afirmou que as forças russas permanecerão no país o quanto for necessário. Contudo, *Pompeo*, em conversa com jornalistas após a reunião, afirmou que os membros da OTAN concordam que as tropas russas devem se retirar. Além disso, o chefe da Aliança, *Jens Stoltenberg*, aponta que as violações da Rússia ao Tratado de Forças Nucleares de Alcance Médio fazem parte de uma postura desestabilizadora que esse país vem construindo (WROUGHTON; BRUNNSTROM, 2019).

No caso da China, o Secretário de Estado pediu para que a OTAN se posicione contra a crescente influência chinesa nas telecomunicações europeias propiciada pela expansão da rede de 5G da empresa *Huawei Technologies* (WROUGHTON; BRUNNSTROM, 2019). Anteriormente, *Washington* já havia declarado que não fará parcerias com países associados a essa empresa. Além disso, asseverou que nem os Estados Unidos da América ou a OTAN poderão compartilhar informações, caso haja o envolvimento da *Huawei* no setor de comunicações dos países membros, devido aos indícios de ligações da empresa com setores de inteligência no governo chinês (LEE, 2019).

Os documentos de defesa dos Estados Unidos da América, Reino Unido e da OTAN embasam os discursos e a percepção de ameaças reforçada por *Pompeo*. No *National Cyber Security Strategy 2016-2021* do Reino Unido, no que tange o contexto estratégico e as ameaças, os grupos organizados de origem russa são apontados como os principais criminosos cibernéticos atuantes contra o Reino Unido em práticas como roubo, extorsão e fraudes. Não há clareza sobre uma suposta acusação contra o Estado russo, contudo, o documento afirma que os grupos agressores e os cibercriminosos são majoritariamente da Europa Oriental (UK, 2016).

Já no *National Cyber Strategy of United States of America*, há uma maior objetividade quanto aos atores, as ameaças e os desafios. Nele, é citado a Rússia, o Irã e a Coreia do Norte como as principais origens dos ataques cibernéticos às empresas norte-americanas. Além disso, o documento também estabelece que os ataques perpetrados por esses países ou de origem neles, estão livres de consequências e responsabilidade legal, justamente por esses Estados não terem uma rígida legislação ou interesse em responsabilizar os criminosos (USA, 2018a).

No mesmo documento, a China é percebida como um dos países mais envolvidos em espionagem econômica e roubo de propriedade intelectual, cujo prejuízo é estimado

em um trilhão de dólares. A ameaça cibernética também é reconhecida como advinda de atores não estatais pelo referido documento, dentre eles incluem-se grupos terroristas e criminosos de forma geral. A atuação dessas organizações se concentra tanto no aspecto psicossocial por meio do recrutamento e da propaganda para atacar os EUA, quanto nos ataques cibernéticos com fins econômicos (USA, 2018a).

No que se refere a OTAN, os EUA enfatizam a mesma narrativa que o Secretário de Estado apresenta em seus discursos. Isto fica claro no ponto "*Strengthen Alliances and Attract New Partners*"[4]:

> "Uma Europa forte e livre, vinculada por princípios comuns de democracia, soberania nacional e comprometimento ao Artigo 5 do Tratado do Atlântico Norte é vital para nossa segurança. A aliança irá dissuadir o aventureirismo russo, derrotar os terroristas que procuram assassinar inocentes e abordar o arco de instabilidade que se desenvolve na periferia da OTAN. Ao mesmo tempo, a OTAN deve adaptar-se para permanecer relevante e adequada para o nosso tempo - com propósito, capacidade e tomada de decisão responsável. Esperamos que os aliados europeus cumpram seus compromissos de aumentar os gastos com defesa e modernização para fortalecer a aliança em face de nossas preocupações comuns de segurança" (USA, 2018b, p. 9 - tradução nossa)[5].

O Departamento de Defesa dos Estados Unidos da América também destaca que a competição estratégica com a China e a Rússia são suas principais prioridades no longo prazo. A magnitude dessas ameaças representadas hoje exige investimentos maiores e assegurados para que os Estados Unidos da América possam prosperar no futuro (USA, 2018b).

Nota-se, portanto, um esforço securitizador para a questão cibernética não só no reconhecimento de ameaças, mas também no que se refere à infraestrutura básica de telecomunicações. Ainda, é relevante que essa temática engendre tensões internas na OTAN, em decorrência da interconectividade do ciberespaço, de forma que se alguns países optarem por adotar a infraestrutura 5G chinesa, estarão, na prática, se distanciando dos Estados Unidos da América e de outros aliados em termos de cooperação.

---

[4] Fortalecer alianças e atrair novos parceiros (USA, 2018 - tradução nossa).

[5] *A strong and free Europe, bound by shared principles of democracy, national sovereignty, and commitment to Article 5 of the North Atlantic Treaty is vital to our security. The alliance will deter Russian adventurism, defeat terrorists who seek to murder innocents, and address the arc of instability building on NATO's periphery. At the same time, NATO must adapt to remain relevant and fit for our time—in purpose, capability, and responsive decision-making. We expect European allies to fulfill their commitments to increase defense and modernization spending to bolster the alliance in the face of our shared security concerns.*

Referências:

LEE, Matthew. **Pompeo warns eastern Europe on Chinese and Russian meddling.** Washington Post, 2019. Disponível em: https://www.washingtonpost.com/business/technology/pompeowarns-eastern-europe-on-chinese-and-russian-meddling/2019/02/12/bd7bb2a0-2ecd-11e9-8781763619f12cb4_story.html?utm_term=.dcfad946931d/. Acesso em: 20 de janeiro de 2019.

UK. **National Cyber Security Strategy 2016-2021.** Washington: Department of Defense, 2016.

USA. **National Cyber Strategy of United States of America.** Washington: White House, 2018a.

USA. **National Defense Strategy.** Washington: Department of Defense, 2018b.

WROUGHTON, Lesley; BRUNNSTROM, David. **Pompeo calls on NATO to adapt to new threats from Russia, China.** Reuters, 2019. Disponível em: https://www.reuters.com/article/us-usa-nato/pompeo-calls-on-nato-to-adapt-to-newthreats-from-russia-china-idUSKCN1 RG1JZ/. Acesso em: 24 de abril de 2019.

ATAQUES FISICOS COMO RESPOSTA IMEDIATA À ATAQUES CIBERNÉTICOS*

***Marcos Luiz da Cunha de Souza*[1]**
***Breno Pauli Medeiros*[2]**
***Luiz Rogério Franco Goldoni*[3]**

Em matéria de 6 de maio do corrente, a revista *Forbes* reportou que as Forças de Defesa de Israel (IDF) realizaram um ataque cinético em resposta às ações cibernéticas do *Hamas* durante a intensificação do conflito entre Israel e Palestina. As Forças israelenses afirmaram ter parado um ataque on-line antes de realizar seu ataque aéreo às instalações onde supostamente estariam operando os *hackers* do *Hamas* (FLAHERTY, 2019). A IDF alegou que teria eliminado as capacidades cibernéticas do grupo. Em declaração na rede social *twitter*:

> "Nós frustramos uma tentativa de ofensiva cibernética do Hamas contra alvos israelenses. Seguindo nossa bem-sucedida operação de defesa cibernética, alvejamos um prédio onde os agentes do Hamas trabalham. O HamasCyberHQ.exe foi removido" (ISRAEL DEFENSE FORCES, 2019 - tradução nossa).

A atuação israelense ilustra o segundo caso de resposta cinética às ações cibernéticas, tendência que pode ser interpretada como uma mudança tática no que diz respeito às operações cibernéticas. A primeira ocorrência de uma resposta física à atuação cibernética ocorreu em 2015, quando o *hacker* de origem britânica *Junaid Hussain* foi eliminado em um ataque aéreo com Veículos Aéreos Não-Tripulados (VANTs[4]) por forças norte-americanas (ACKERMAN et al, 2015). Contudo, diferente do ataque realizado por Israel, esse contou com um maior planejamento e não foi uma reação imediata.

O chefe de segurança da *AmTrust Europe*, empresa de seguros internacionais que atua em diversos níveis de segurança incluindo a cibernética, *Ian Thornton-Trump*, comentou sobre o acontecimento e afirmou que Israel não teria atacado o prédio se não tivesse certeza de quem estaria nele (FLAHERTY, 2019).

---

* Artigo originalmente publicado no dia 31 de maio de 2019 no site do OMPV.
[1] Graduando em Defesa e Gestão Estratégica Internacional.
[2] Doutorando em Ciências Militares na ECEME.
[3] Doutor em Ciência Política e Professor da ECEME.
[4] Comumente referidos como "drones".

Na visão desse especialista, o processo ISTAR (inteligência, vigilância, aquisição de alvos e reconhecimento) contaria com a localização do alvo e a verificação das informações adicionais, estas muitos provavelmente não cibernéticas. Além disso, ele acredita que a ação israelense faz parte da estratégia militar para demonstrar uma resposta esmagadora a fim de dissuadir o inimigo.

O coronel de reserva da inteligência militar britânica, *Philip Ingram*, concorda com *Ian Thornton-Trump* e afirma que o conflito tem várias camadas. Segundo o coronel, diferentemente do que o senso comum acredita, a ação não teria sido um ataque ao acaso ou uma mera resposta imediata, mas sim um projeto mais elaborado de inteligência e vigilância (FLAHERTY, 2019). *Philip Ingram* igualmente assinala que esse tipo de reação faz parte de uma preocupação atual que todos os Estados-nação passam a ter com os efeitos reais das ações no ciberespaço. De fato, como visto em análises anteriores publicadas neste espaço, a postura dos documentos de defesa de diferentes países prevê respostas cinéticas às ações cibernéticas (USA, 2018).

Jason Healey, ex-funcionário da Casa Branca durante os mandatos de *George W. Bush* e atualmente pesquisador de ciber-conflitos da *Columbia University*, aponta que respostas físicas para agressões no ciberespaço já eram vislumbradas pelos Estados Unidos da América desde 1999. A partir de 2011, os norte-americanos passaram a se reservar ao direito de retaliar ataques cibernéticos com força militar.

Por outro lado, o antigo membro do grupo *Tailored Acces Operations*, da Agência de Segurança Nacional dos Estados Unidos da América, *Jake Williams*, afirma que os hackers estão desarmados e não devem ser considerados alvos de bombardeios. Para ele, existe uma grande diferença entre um terrorista e alguém que está longe do campo de batalha não oferecendo riscos físicos - inclusive no que diz respeito à opinião pública (NEWMAN, 2019).

Na visão de *Jake Williams*, um *hacker* pode provocar danos sérios a infraestrutura crítica, mas nem sempre esse é seu objetivo. Muitas vezes ele pode estar montando o que parece ser um ataque, mas sem executá-lo, apenas para fins de reconhecimento e coleta de informações.

O professor de estudos estratégicos da Universidade *John Hopkins*, *Thomas Rid*, tem uma opinião diferente. Segundo ele, o bombardeio israelense não teria nada a ver com uma guerra cibernética ou ciber dissuasão, uma vez que o edifício era utilizado por agentes da inteligência do Hamas, o que por si só o torna um alvo tradicional e legítimo para Israel.

Corroborando com *Thomas Rid*, o pesquisador associado do Centro de Tecnologia de *Oxford*, *Lukasz Olejnik*, reconhece que a resposta cinética imediata a um ataque cibernético é um caso sem precedentes. Contudo, não oferece grandes surpresas, tendo em vista a tendência de os países começarem a considerar o ciberespaço como um domínio de guerra (NEWMAN, 2019).

O caso supracitado contribui para o cenário de incerteza e insegurança global que advém da operacionalização do ciberespaço. Nesse contexto, a Rússia é acusada amplamente de atacar seus vizinhos como a Ucrânia, Geórgia e Estônia (WINDREM, 2016). Israel e EUA já foram capazes de interromper as centrífugas nucleares iranianas com o *malware Stuxnet*. A China, por sua vez, também é acusada de espionar inúmeros governos e corporações para roubar propriedade intelectual (MELMAN, 2019).

Apesar desses fatos, os países evitam escalar os conflitos para o domínio físico e mantém a retórica diplomática, de maneira a evitar a utilização da própria terminologia "guerra". Contudo, a crescente operacionalização do ciberespaço por uma miríade de atores advém dos baixos custos econômicos e militares de se realizar ações agressivas no ciberespaço, tendo em vista que o equipamento e treinamento de *hackers* é significativamente mais barato do que soldados e armamentos tradicionais. Ainda, a incerteza e complexidade do ciberespaço permitem que diferentes atores o utilizem sem serem rastreados, lhe garantindo uma eventual plausibilidade para negar determinadas ações. Resta saber como os tradicionais players das relações internacionais irão se comportar e reagir diante dos desafios impostos pelo novo domínio de poder.

Referências:

ACKERMAN, Spencer; MACASKILL, Ewen; ROSS, Alice. **Junaid Hussain: British hacker for Isis believed killed in US air strike.** The Guardian, 2015. Disponível em: h ttps://www.theguardian.com/world/2015/aug/27/junaid-hussain-british-hacker-for-isis-b elieved-killed-in-us-airstrike/. Acesso em: 8 de maio de 2019.

FLAHERTY, Kate. **Israel Retaliates To A Cyber-Attack With Immediate Physical Action In A World First.** Forbes, 2019. Disponível em: https://www.forbes.com/sites/ kateoflahertyuk/2019/05/06/israel-retaliates-to-a-cyber-attack-with-immediate-physical-action-in-a-world-first/#1e3c529df895/. Acesso em: 8 de maio de 2019.

MELMAN, Yossi. **China Is Spying On Israel to Steal U.S. Secrets.** Foreign Policy, 2019. Disponível em: https://foreignpolicy.com/2019/03/24/china-and-russia-are-spying -on-israel-to-steal-u-s-secrets-putin-netanyahu-xi-haifa-ashdod-iai-elbit/. Acesso em: 20 de maio de 2019.

NEWMAN, Lily. **What Israel's strike on Hamas hackers means for cyberwar.** Wired, 2019. Disponível em: https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/. Acesso em: 8 de maio de 2019.

UNITED STATES OF AMERICA. **National Defense Strategy.** Washington: Department of Defense, 2018.

WINDREM, Robert. **Timeline: Ten Years of Russian Cyber Attacks on Other Nations.** NBC News, 2016. Disponível em: https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111/. Acesso em: 20 de maio de 2019.

ESTADOS UNIDOS, RÚSSIA E CHINA: INDÍCIOS DE UMA GUERRA FRIA DIGITAL?*

***Marcos Luiz da Cunha de Souza*[1]**
***Breno Pauli Medeiros*[2]**
***Luiz Rogério Franco Goldoni*[3]**

Como evidenciado em análises prévias feitas por estes autores no portal do OMPV[4], as vulnerabilidades oriundas da inserção da infraestrutura básica no ciberespaço são cada vez mais consideradas um assunto a ser securitizado sob a perspectiva da Defesa Nacional, constatação corroborada por diferentes documentos de defesa (BRASIL, 2010; BRASIL, 2012; BRASIL, 2016). O exemplo mais recente e talvez de maior proeminência na mídia internacional, refere-se à expansão da rede chinesa de 5G pela Ásia e Europa. Em represália à expansão da infraestrutura de telecomunicações de 5G oferecida pela empresa chinesa *Huawei*, os Estados Unidos proibiram a utilização dos produtos da empresa em seu território e recomendaram que seus parceiros não utilizem a infraestrutura de comunicações chinesa, argumentando que esta estaria comprometida pela inteligência desse país (LEE, 2019).

Represálias à *Huawei* estão em conformidade com o esforço norte-americano de proteger suas infraestruturas críticas ao passo que estas se inserem no domínio cibernético. O reconhecimento norte-americano de ameaças capazes de explorar vulnerabilidades na infraestrutura básica foi evidenciada no Sumário do documento *National Defense Strategy* de 2018:

> "A América é um alvo, seja de terroristas que procuram atacar nossos cidadãos; de atividade cibernética maliciosa contra infraestrutura pessoal, comercial ou governamental; ou de subversão política e de informação. Novas ameaças estão surgindo, enquanto o aumento da conectividade digital em todos os aspectos da vida, negócios, governo e forças armadas cria vulnerabilidades significativas. Durante o conflito, os ataques contra nossa

* Artigo originalmente publicado no dia 03 de julho de 2019 no site do OMPV.
[1] Graduando em Defesa e Gestão Estratégica Internacional.
[2] Doutorando em Ciências Militares na ECEME.
[3] Doutor em Ciência Política e Professor da ECEME.
[4] Disponível em: http://ompv.eceme.eb.mil.br/masterpage_assunto.php?id=123 e disponível em: http://ompv.eceme.eb.mil.br/masterpage_assunto.php?id=124.

> infraestrutura crítica de defesa, governo e economia devem ser antecipados" (USA, 2018a, p. 3, tradução nossa)[5].

O posicionamento norte-americano para com o ciberespaço corresponde à um contexto sociopolítico mais amplo no qual a inserção social no meio técnico-científico informacional suscita a evolução da percepção de ameaças e valorização estratégica das infraestruturas inseridas no domínio cibernético.

Enquanto a *National Defense Strategy* de 2018 evidencia o reconhecimento a ameaças à infraestrutura norte-americana, a reportagem do jornal *The New York Times* publicada em junho do corrente ilustra o tom da retórica cibernética dos Estados Unidos.

Segundo autoridades governamentais norte-americanas, os Estados Unidos da América obtiveram acesso a rede elétrica russa, demonstrando como o *Cyber Command*, que teve suas capacidades operacionais recentemente ampliadas, irá se posicionar diante de ameaças cibernéticas no futuro. Segundo as fontes do jornal, os Estados Unidos da América conseguiram infiltrar a infraestrutura energética russa a ponto de desabilitá-la em caso de ações contra os Estados Unidos da América.

A demanda por novas capacidades operacionais do *Cyber Command* é consequência dos indícios de que a Rússia deteria capacidades de atacar redes elétricas desde 2015[6]. Além disso, em 2018, o jornal supracitado já havia relatado denúncias tanto do Departamento de Segurança Interna quanto do FBI de que a Rússia já teria enviado *malwares* capazes de sabotar usinas de energia, gasodutos, oleodutos ou até mesmo suprimentos de água dos Estados Unidos da América em qualquer conflito futuro.

A ampliação da capacidade operacional no ciberespaço por parte do governo norte-americano foi autorizada pelo *National Security Presidential Memoranda 13*, de caráter parcialmente confidencial, em fevereiro do corrente, com o objetivo de dar mais liberdade ofensiva ao *Cyber Command* sem que este necessite da aprovação presidencial para tal (USA, 2019).

---

[5] "A*merica is a target, whether from terrorists seeking to attack our citizens; malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion. New threats to commercial and military uses of space are emerging, while increasing digital connectivity of all aspects of life, business, government, and military creates significant vulnerabilities. During conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated*" (USA, 2018, p. 3).

[6] Para mais informações sobre as capacidades russas de ataques a infraestruturas críticas, ver análise "Infraestrutura básica e vulnerabilidades cibernéticas." neste site.

Trata-se de uma ramificação prática e estratégica de uma política dissuasória para fazer frente à possível exploração das vulnerabilidades da rede norte americana, e desencorajar futuras ações contra os Estados Unidos da América. Nas palavras do Conselheiro de Segurança Nacional do Presidente, *John R. Bolton*: "Vamos impor custos a você até que você consiga entender"[7] (SANGER; PERLROTH, 2019). Ainda segundo *Bolton*, atualmente, os Estados Unidos da América têm uma visão mais ampla de seus alvos cibernéticos e tais ações fariam parte de um esforço para afirmar à Rússia ou a qualquer país do mundo que ataques cibernéticos contra os Estados Unidos da América serão acompanhados de altos custos para os perpetradores (SANGER; PERLROTH, 2019).

Nesse contexto, o comandante do *Cyber Command*, General *Paul M. Nakasone*, afirmou publicamente que era de interesse de seu país estar apto a defender-se dentro da rede do adversário para mostrar que é capaz de reagir a agressões cibernéticas futuras (SANGER; PERLROTH, 2018). Portanto, ao colocar um *malware* potencialmente incapacitante no sistema russo, os Estados Unidos da América reforçam o discurso dissuasório de que qualquer passo em falso poderia resultar em uma escalada de ataques cibernéticos em massa contra as infraestruturas críticas russas.

É pertinente ressaltar que, conforme matéria do *The Guardian* que o presidente russo *Vladimir Putin* recebeu o presidente chinês *Xi Jinping* em Moscou, no início do mês de junho, para assinar um acordo com a *Huawei*, no intuito de desenvolver a tecnologia 5G no país em parceria com a empresa russa de telecomunicações MTS (THE GUARDIAN, 2019). Esse acordo corrobora com a interpretação do Secretário de Estado dos Estados Unidos, *Mike Pompeo*, de que ambos os países estariam se unindo em uma oposição aos EUA no ciberespaço.

Dada sua estrutura interna e as diferentes tecnologias utilizadas para facilitar o anonimato, o ciberespaço configura um domínio de inerente incerteza; e a forma como diferentes atores exploram essa característica, corresponde à uma dinâmica de poder diferente dos demais domínios. Logo, as decisões tomadas pelos envolvidos possuem alto valor estratégico - sendo, portanto, classificadas - de forma que é improvável determinar quais ações foram tomadas primeiro. Isto é, assim como o posicionamento norte americano mais ofensivo contra a Rússia pode ser interpretada como um reflexo

[7] *"We will impose costs on you until you get the point".*

do acordo estratégico com a China; a aproximação entre China e Rússia pode ter sido ocasionada justamente pela postura mais agressiva pelos Estados Unidos da América.

O contexto supracitado coloca em voga a questão da equidade das respostas no ciberespaço. Estas podem resultar em uma escalada descontrolada e perigosa de ataques cibernéticos de ambos os lados, podendo progredir para um conflito cinético nos domínios tradicionais que pode, ainda, recorrer a alternativas nucleares (USA, 2018b). Nesse sentido, como as ações são dificilmente detectadas e/ou rastreadas aos reais perpetradores, múltiplos atores - não necessariamente estatais - perseguem seus interesses no ciberespaço.

O efeito político disso é observado em discursos e acusações inflamatórias mais frequentes mesmo sem embasamento em circunstâncias observáveis e/ou comprováveis. Fato que, considerando as consequências cinéticas de ataques cibernéticos, engendra preocupações para os diferentes setores de defesa e segurança.

Referências:

BRASIL. Ministério da Defesa**. Livro Verde: Segurança Cibernética no Brasil.** Brasília: Ministério da Defesa, 2010.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional.** Brasília: Ministério da Defesa, 2012.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional.** Brasília: Ministério da Defesa, 2016.

LEE, Matthew. **Warns Eastern Europe on Chinese and Russian Meddling.** U.S News, 2019. Disponível em: https://www.usnews.com/news/world/articles/2019-02-12/ pompeo-warns-easterneurope-on-chinese-and-russian-meddling/. Acesso em: 15 de junho de 2019.

SANGER, David; PERLROTH, Nicole. **U.S. Escalates Online Attacks on Russia's Power Grid.** The New York Times, 2019. Disponível em: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?searchResultPosition=1. Acesso em: 15 de junho de 2019.

SANGER, David; PERLROTH, Nicole. **Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says**. The New York Times, 2018. Disponível em: https: //www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html?module=inline. Acesso em: 15 de junho de 2019.

THE GUARDIAN. **China's Huawei signs deal to develop 5G in Russia.** The Guardian, 2019. Disponível em: https://www.theguardian.com/technology/2019/jun/06/

chinas -huawei-signs-deal-to-develop-5g-network-in-russia. Acesso em: 15 de junho de 2019.

USA. **Nuclear Posture Review.** Washington: Department of Defense, 2018b.

USA. **Summary of National Defense Strategy.** Washington: Department of Defense, 2018a.

USA. **National Defense Authorization Act for Fiscal Year 2019.** US Congress Gov, 2019. Disponível em: https://www.congress.gov/bill/115th-congress/house-bill/5515/text. Acesso em: 15 de junho de 2019.

O ATAQUE CIBERNÉTICO DOS EUA AO IRÃ: PARA ALÉM DA GUERRA CIBERNÉTICA*

***Marcos Luiz da Cunha de Souza*[1]**
***Breno Pauli Medeiros*[2]**
***Luiz Rogério Franco Goldoni*[3]**

As tensões entre Estados Unidos e Irã atingiram novo patamar no final do mês de junho. Após o Irã derrubar um Veículo Aéreo Não-Tripulado (VANT) norte-americano e atacar dois navios petroleiros, os EUA retaliaram de forma cibernética, incapacitando o sistema de comando e controle iraniano, especificamente os sistemas de lançamento de foguetes e controle aéreo. Meios de comunicação, como *The Washington Post*, *Associated Press*, *The New York Times* e *Al Jazeera*, confirmaram o ocorrido e, posteriormente, o presidente *Donald Trump* também comentou a respeito da incursão cibernética na infraestrutura iraniana por intermédio de sua conta no *Twitter*.

Quando informado a respeito do número de mortos que uma ação cinética tradicional propiciaria, *Trump* cancelou os anteriormente planejados ataques aéreos, optando por um ataque cibernético (AFP, 2019). O alvo era um grupo de inteligência iraniano suspeito de estar ligado à Guarda Revolucionária Iraniana. Segundo relatórios do *The Washington Post*, esse grupo esteve envolvido em recentes ataques a navios comerciais na região do Estreito de *Ormuz*.

De acordo com a revista *Times*, o sistema de controle de mísseis iranianos seria o alvo de um ataque planejado há semanas pelo Comando Cibernético dos Estados Unidos da América (BOHN, 2019). A retaliação menos convencional por parte dos Estados Unidos da América, com poucos danos colaterais, quando comparado a uma incursão cinética tradicional, ilustra a opção estratégica norte-americana em envolver-se persistentemente com adversários no ciberespaço de forma ofensiva, mas evitando a escalada dos conflitos para os domínios tradicionais.

A recém-saída dos Estados Unidos da América do acordo nuclear de 2015 com o Irã marca o agravamento das tensões entre os dois países, tendo como um dos principais pontos de atrito, as sanções econômicas impostas ao Irã pelo governo norte-americano

---

* Artigo originalmente publicado no dia 27 de agosto de 2019 no site do OMPV.
[1] Graduando em Defesa e Gestão Estratégica Internacional.
[2] Doutorando em Ciências Militares na ECEME.
[3] Doutor em Ciência Política e Professor da ECEME.

(AL JAZEERA, 2019). A pressão também é imposta no domínio cibernético. Não é a primeira vez que os Estados Unidos da América realizam operações cibernéticas contra alvos iranianos. Acredita-se que o *worn*[4] *Stuxnet* tenha sido desenvolvido pelos Estados Unidos da América em parceria com Israel para paralisar as centrífugas nucleares iranianas em 2010 (SANGER; MAZZETTI, 2016). Em 2016, foi relatado que os Estados Unidos da América haviam criado um plano chamado *Nitro Zeus*[5], que poderia ser usado contra a infraestrutura iraniana, embora o projeto tenha sido arquivado (SANGER; MAZZETTI, 2016).

Os esforços cibernéticos são mútuos, com o Departamento de Segurança Interna dos Estados Unidos relatando um aumento de atividades cibernéticas maliciosas praticada por agentes iranianos, após sua saída do acordo nuclear (BOHN, 2019). A *Microsoft* chegou a alertar mais de 10 mil de seus clientes que poderiam ter sido afetados. Contudo, a empresa esclareceu que embora muitos desses ataques não estejam relacionados ao processo democrático, os dados demonstram a extensão significativa com que os estados-nação continuam a confiar nos ataques cibernéticos como uma ferramenta para obter inteligência, influenciar a geopolítica ou alcançar outros objetivos (BURT, 2019).

De acordo com representantes das empresas de segurança cibernética *CrowdStrike* e *FireEye* (VOLZ; YOUSSEF, 2019), os ataques de origem iraniana, que supostamente são executados com aval do governo, visam atingir setores da economia estadunidense, incluindo finanças, petróleo e gás, por meio de ondas de e-mails de *spear phishing*[6].

Sob outra perspectiva, pode-se argumentar que o conflito com o Irã faz parte de um contexto geopolítico mais amplo decorrente da relevância do Golfo Pérsico e, especificamente, do Estreito de *Ormuz*, no qual os petroleiros foram atacados e onde se encontra cerca de metade das reservas mundiais de petróleo, além de ser o canal pelo

[4] Um worm é um programa autorreplicante, diferente de um vírus. Enquanto um vírus infecta um programa e necessita deste programa hospedeiro para se alastrar, o worm é um programa completo e não precisa de outro para se propagar (NOVAES, 2014).

[5] O *Nitro Zeus* é uma técnica em que os sistemas incorporam recursos de software inerentes a eles durante a fase de projeto e criação, o que torna fácil para os hackers lançarem ataques cibernéticos efetivos contra os usuários do sistema remotamente. Semelhante aos *botnets*, esses dispositivos podem ser usados para lançar ataques como *ransomware*, *DDoS* e distribuição de *malware* de mineração criptografada (GOUD, 2019).

[6] *Spear phishing* é um ataque direcionado, focado em uma pessoa, grupo de pessoas, ou organização específica com o objetivo de penetrar suas defesas. Seu uso é feito com base em engenharia social, utilizando informações sobre a vítima para dar credibilidade ao ataque que consiste em infectar a máquina da organização (ROUSE, 2019).

qual passam diariamente mais de 30% de toda a produção de petróleo mundial (BBC, 2019).

O Estreito de *Ormuz* banha o Irã, incorpora as rotas comerciais existentes na Ásia Central e possui um litoral que se estende do Iraque ao Paquistão, na rota do petróleo. O Golfo Pérsico serve de palco para uma disputa geopolítica entre a Índia e o Irã com a China e o Paquistão para projeção de poder no Golfo de *Omã* e interior da Eurásia, conectando o sudeste iraniano com a Ásia Central, que é rica em energia fóssil (KAPLAN, 2019). Nesse sentido, o Irã ocupa uma posição estratégica central no tabuleiro geopolítico regional, uma vez que mostra ser uma peça valiosa na expansão da influência chinesa pela Eurásia. Pequim pretende intensificar sua presença no Oriente Médio com a construção de uma base naval próxima à fronteira iraniana.

Esses objetivos estão em conformidade com a iniciativa *One Belt, One Road*[7], na qual a China constrói uma rede de infraestrutura e se engaja no comércio dessas regiões para unir o Oriente Médio, o subcontinente indiano e o leste da Ásia.

Como visto anteriormente em outras análises nesse canal, os Estados Unidos da América recorrem à suas tecnologias de ciberguerra em paralelo com esforços políticos e econômicos na disputa hegemônica com a China, fato ilustrado na disputa de mercados de infraestrutura 5G. Esses interesses estadunidenses também estão expostos nos documentos estratégicos mais atuais do governo *Trump* e nos discursos de seus agentes governamentais à mídia internacional (USA, 2018).

Referências:

AGENCE FRANCE-PRESSE. **US launched cyber attacks on Iran after drone shootdown: reports.** Yahoo News, 2019. Disponível em: https://news.yahoo.com/us-launched-cyberattacks-iran-drone-shootdown-reports-232123877.html. Acesso em: 10 de julho de 2019.

AL JAZEERA. **US-Iran tensions: All the latest updates.** Aljazeera, 2019. Disponível em: https://www.aljazeera.com/news/2019/06/iran-tensions-latest-updates-190621103437644.html. Acesso em: 16 de julho de 2019.

[7] A iniciativa *One Belt, One Road*, foi lançada em 2013 e anunciada oficialmente em 2015 pelo presidente chinês *Xi Jinping*. Seu objetivo é restabelecer as antigas rotas de comércio que ligavam a Ásia à Europa, a partir de uma série de investimentos, promovendo o desenvolvimento da infraestrutura e do transporte ao longo dessas rotas. Nesse sentido, o *Belt* se referiria aos investimentos terrestres, que liga a China à Ásia Central e consequentemente à Europa, enquanto o *Road* se referiria à rota marítima que seria da China através do Sudeste Asiático para o Oceano Índico, chegando pôr fim ao Mar Mediterrâneo (D'ATRI, 2017).

BBC**. Por que a tensão entre EUA e Irã no Estreito de Ormuz pode fazer disparar o preço do petróleo?** BBC, 2019. Disponível em: https://www.bbc.com/portuguese/internacional-48622958/. Acesso em: 10 de julho de 2019.

BOHN, Dieter. **US cyberattack reportedly hit Iranian targets.** The Verge, 2019. Disponível em: https://www.theverge.com/2019/6/22/18714010/us-cyberattack-iraniant argets-missilecommand-report. Acesso em: 16 de julho de 2019.

BURT, Tom**. New cyberthreats require new ways to protect democracy.** [S. l.], 17 jul. 2019. Disponível em: https://blogs.microsoft.com/on-the-issues/2019/07/17/newcyberthreats-require-new-wa ys-to-protect-democracy. Acesso em: 19 de julho de 2019.

D'ATRI, Fabiana. **One Belt One Road: uma iniciativa geopolítica e econômica da China.** CEBC Alerta, 2017. Disponível em: http://cebc.org.br/sites/default/files/cebc_alerta_ed_78_obor_final.pdf. Acesso em: 16 de julho de 2019.

GOUD, Naveen. **US to launch 'Nitro Zeus' Cyber Attack on Iran.** Cybersecurity Insideres, 2019. Disponível em: https://www.cybersecurity-insiders.com/us-to-launch-nitro-zeus-cyberattack-on-iran /. Acesso em: 16 de julho de 2019.

KAPLAN, Robert**. This Isn't About Iran - It's About China.** The New York Times, 2019. Disponível em: https://www.nytimes.com/2019/06/26/opinion/trump-iran-china.html?searchResultPositio n=10. Acesso em: 16 de julho de 2019.

NOVAES, Rafael. **O que é um Worm (verme)?** PSafe, 2019. Disponível em: https://www.psafe.com/blog/worm/. Acesso em: 16 de julho de 2019.

ROUSE, Margaret. **Spear phishing.** SearchSecurity, 2019. Disponível em: https://searchsecurity.techtarget.com/definition/spear-phishing?track=NL-1823&ad=922304&src=922304&asrc=EM_NLN_98394539&utm_medium=EM&utm_source=NLN&utm_campaign=20180801_Word%20of%20the%20Day:%20spear%20phishing. Acesso em: 16 de julho de 2019.

SANGER, David; MAZZETTI, Mark. U.S. **Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict.** The New York Times, 2016. Disponível em: https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-irannuclear-negotiations-failed.html. Acesso em: 25 de julho de 2019.

USA. **National Cyber Strategy of United States of America.** Washington: White House, 2018

VOLZ, Dustin; YOUSSEF, Nancy. **U.S. Launched Cyberattacks on Iran.** The Wall Street Journal, 2019. Disponível em: https://www.wsj.com/articles/u-s-launched-cyberattacks-on-iran-1156126345 4. Acesso em: 16 de julho de 2019.

DEFESA QUÍMICA, BIOLÓGICA, RADIOLÓGICA E NUCLEAR

O ENVENENAMENTO DO ESPIÃO RUSSO*

***Anderson Wallace de Paiva dos Santos*[1]**
***André Luiz Bifano da Silva*[2]**

1. Introdução

No rearranjo geopolítico mundial, iniciado a partir de meados do século XVII, a prevalência do modelo *westifaliano* deu origem a Estados nacionais soberanos e independentes, originando um sistema internacional regido por complexas conexões que impactam mutuamente as decisões governamentais.

Além desses sujeitos[3] primários, as relações internacionais passaram a contar também com as idiossincrasias de atores não estatais, constituindo uma sociedade dirigida por um conjunto de regras e instituições que derivam da necessidade de soberania por parte dos Estados em um ambiente onde a liberdade de ação[4] para mantê-la é cada vez mais restrita.

Esse sistema multipolar induz os Estados a atuarem nas expressões política e militar para a consecução de seus interesses. É nesse *background* que o mundo se depara com as repercussões de um incidente de proporções internacionais envolvendo o Reino Unido e a Federação Russa. O envenenamento do ex-espião russo *Sergei Skripal* e de sua filha, *Yulia*, na cidade britânica de *Salisbury*, remete ao argumento maquiavélico de que a política não pode submeter-se aos valores morais quando se trata da proteção dos interesses do Estado.

2. Desenvolvimento

O incidente de *Salisbury*, como ficou notório, é retratado pelo governo britânico como mais uma tentativa do *Kremlin* em eliminar suas discordâncias políticas por meio do emprego dissimulado de substâncias de origem química, biológica, radiológica ou nuclear (QBRN). Em 2006, o dissidente *Aleksander Litvinenko* foi envenenado ao ingerir chá contaminado com Polônio 210 ($Po^{21º}$), um elemento radioativo de elevada

---

* Artigo originalmente publicado no dia 19 de maio de 2019 no site do OMPV.
[1] Major do Exército Brasileiro.
[2] Major do Exército Brasileiro.
[3] Sujeitos das Relações Internacionais são entes presentes no Sistema Internacional, representados, principalmente pelos Estados Nacionais, Organismos Intergovernamentais e Forças Transnacionais.
[4] Capacidade de planejar e executar as ações necessárias à consecução do objetivo estabelecido.

atividade e difícil detecção. No caso *Skripal*, há suspeitas de que o quase desconhecido agente químico *Novichok*[5] tenha sido utilizado.

O choque de versões entre os envolvidos reside no fato de que Moscou alega que o governo britânico não dispõe de evidências para tal suposição. As autoridades do *Kremlin* rejeitam a ideia de uma trama russa, rememorando a questionável postura adotada pelo Reino Unido perante a (in)existência de armas químicas no Iraque, anos atrás.

A fim de legitimar seu discurso, o Reino Unido recorreu a um terceiro sujeito presente nas relações internacionais. A solicitação de assistência técnica à Organização para Proibição de Armas Químicas (OPAQ), amparada pela convenção de mesmo nome (CPAQ), é parte da estratégia britânica para comprovar que não resta dúvida quanto à autoria russa.

O questionamento britânico ao apelar para a assistência da OPAQ tenta colocar em xeque a credibilidade da Rússia como membro da CPAQ ao contestar, à moda grociana[6], o seu grau de comprometimento com as regras e os imperativos morais da Convenção.

Todavia, a assistência da OPAQ tem caráter imparcial. Ela não tem a intenção de responsabilizar ou envolver-se nas discussões de seus Estados-Parte[7], não obstante a análise das amostras coletadas por seus inspetores haver acusado a presença de uma substância de alta pureza, persistência e resistência às condições meteorológicas.

Mesmo assim, como o agente *Novichok* poderia ter sido empregado se a Rússia é signatária da CPAQ e declara suas armas químicas ainda não destruídas? Seus elementos não estariam na lista proibida da convenção? Essas premissas isentariam a Rússia de quaisquer acusações. A menos que o agente tóxico seja considerado uma "arma binária".

Os compostos com características binárias possuem propriedades que permitem serem armazenados como dois componentes químicos diferentes e menos tóxicos, mais

[5] O termo *Novichok* significa "recém-chegado" em russo e aplica-se a um grupo de agentes neurotóxicos de 4ª geração (série A-230), desenvolvido sob um programa soviético de codinome *Foliant*, a partir da década de 1970. A versão atual do *Novichok* pertence à série A-234 e foi projetada para ser mais tóxica e sofisticada do que outros agentes, como o próprio neurotóxico britânico VX, podendo ser considerada a 5ª geração das armas químicas.

[6] A tradição grociana, concebida pelo pensamento do holandês *Hugo Grocio*, é uma das teorias das Relações Internacionais que defende a limitação do poder dos Estados por um conjunto de regras e instituições internacionais.

[7] Estados-Parte representam os países que assinaram e ratificaram os dispositivos constantes da Convenção para Proibição de Armas Químicas (CPAQ). Atualmente, Coreia do Norte, Egito e Sudão do Sul ainda não aderiram à Convenção; enquanto o Estado de Israel é signatário mas ainda não a ratificou.

fáceis de transportar e de manusear. Quando combinados, eles reagem para produzir o agente tóxico ativo. Essa parece ser uma das raras explicações plausíveis para o emprego dissimulado do *Novichok*.

Se essa hipótese for factível, a mensagem de Moscou parece deixar claro que os russos ainda são capazes de atacar quando e onde quiserem, sem que seus oponentes esperem ou prevejam, reforçando o enfoque no paradigma realista[8] ao demonstrar habilidade para maximizar a força no sentido de manter seus interesses nacionais.

3. Considerações finais

O atentado contra *Skripal* teve dimensões diplomáticas e implicações de inteligência que culminaram com a expulsão mútua de representantes de ambos os governos. Sua interpretação como violação à soberania britânica abala ainda mais as já sensíveis relações exteriores com a Rússia, a ponto de representar um dos fatores que influenciaram a participação do Reino Unido na ação militar em retaliação ao hipotético emprego de armas químicas pelo governo sírio, aliado do *Kremlin*, contra as forças rebeldes.

Na suposição do uso indireto do agente *Novichok*, percebe-se que a capacidade de coerção russa tenta desequilibrar o poder por meio do emprego cirúrgico de seu *hard power*[9], que continua a impor a razão do Estado acima das considerações éticas, sob um modelo estritamente *hobbesiano*[10]. Nesse contexto, estariam as relações entre essas duas nações degradando-se a ponto de perfazerem um interminável jogo de soma zero[11]? Ou ainda, convém refletir se, em meio às incertezas e opiniões dissonantes, a Federação Russa estaria, de fato, submetida a uma condição restritiva de liberdade de ação?

[8] O Paradigma Realista é um conceito das Relações Internacionais em que há domínio sobre o enfoque estatal na busca constante pelo Poder, fundamentado no pragmatismo pelos interesses nacionais e no desprezo pelo institucionalismo internacional.
[9] Conceito utilizado pela vertente realista das relações internacionais que se refere à capacidade de um Estado em influenciar ou exercer poder sobre o comportamento alheio, mediante o emprego de recursos políticos, militares e econômicos.
[10] A tradição *hobbesiana*, de concepção do filósofo inglês *Thomas Hobbes*, é uma das teorias das Relações Internacionais que expõe a natureza conflituosa das relações entre os Estados, baseada na necessidade de manutenção da soberania e no exercício do poder de coerção.
[11] No jogo de soma-zero o benefício total para os partícipes é sempre nulo, ou seja, um jogador só lucra com base no prejuízo de outro.

TEERÃ E O JCPOA: CONSEQUÊNCIAS DA RETIRADA AMERICANA DO ACORDO NUCLEAR*

***André Nunes*[1]**

No dia 8 de maio de 2018 o presidente *Donald Trump* anunciou a retirada unilateral dos Estados Unidos da América (EUA) do Acordo Nuclear Iraniano - formalmente conhecido como *Joint Comprehensive Plan of Action (JCPOA)* - que havia sido firmado em julho de 2015, durante a administração *Barack Obama* e passado a vigorar a partir do dia 1 de janeiro de 2016, com período de vigência previsto até o ano 2030. A decisão do governo norte-americano será acompanhada de novas sanções econômicas à Teerã.

O JCPOA é um compromisso pactuado pela República islâmica do Irã e o P5+1, grupo de países representado pelos cinco membros permanentes do Conselho de Segurança das Nações Unidas (China, EUA, França, Reino Unido e Rússia) mais a Alemanha. O principal objetivo deste acordo é garantir que o programa nuclear do Irã seja exclusivamente voltado para atividades pacíficas. Mesmo sendo signatário do Tratado de Não-Proliferação Nuclear desde 1968 e tê-lo ratificado em 1970, ainda sob o regime monárquico do Xá *Mohammad Reza Pahlavi*, no documento o Estado persa reafirma que sob nenhuma circunstância buscará, desenvolverá ou adquirirá armas nucleares. Ademais, um dos marcos para implementação do Acordo, previsto no artigo 34 do JCPOA, é o compromisso de que o Irã buscará a ratificação de um Protocolo Adicional de salvaguardas junto à Agência Internacional de Energia Atômica (AIEA).

O Acordo Nuclear de 2015 aborda, entre outras coisas, os seguintes termos: a redução do estoque de urânio iraniano em aproximadamente 98%; o reprojeto de reatores para inibir a produção de plutônio para uso de natureza militar; a proibição da construção de reatores adicionais que possam acumular excesso de água pesada por um período de 15 anos; e a inspeção contínua de peritos da AIEA nas instalações nucleares do país.

A partir de uma perspectiva civil, o Irã tem procurado desenvolver seu programa nuclear com o propósito de diversificar sua matriz energética que, de acordo com os

---

* Artigo originalmente publicado no dia 19 de maio de 2019 no site do OMPV.

[1] Doutor em Ciências Militares.

dados do *BP Statistical Review of World Energy 2017*, é calcada basicamente em fontes fósseis, mais especificamente gás natural e petróleo. Vale ressaltar que o Estado persa com uma população de aproximadamente 82 milhões de pessoas[2], em 2016 apareceu como o nono maior consumidor de energia primária[3] do mundo; o segundo país que mais consome petróleo no Oriente Médio, superado apenas pela Arábia Saudita; e o maior consumidor de gás natural de sua região, com um volume de 202,4 bilhões de metros cúbicos (bmc), quase nove vezes o volume de 23,5 bmc consumido pelo Brasil no mesmo período.

Apesar disso, o discurso oficial do presidente norte-americano deixou transparecer alguns pontos de vista que levaram seu governo a denunciar o acordo. Segundo *Trump*, o acordo permitiu que o Irã continuasse enriquecendo urânio, fato que com o tempo lhe daria a capacidade de produzir armas nucleares rapidamente; contribuiu para que seus gastos militares crescessem cerca de 40% desde 2015 (de cerca de 10.814 bilhões de dólares em 2015 para 14.086 bilhões em 2017, ficando em torno de 30% conforme dados do *Stockholm International Peace Research Institute*); e não aplicou restrições ao programa de mísseis balísticos iranianos e suas "atividades desestabilizadoras no Oriente Médio".

No que tange ao programa de mísseis balísticos iranianos, as informações do *The Military Balance 2018* e do *Missile Defense Project* ligado ao *Center for Strategic and International Studies* (CSIS), com sede em *Washington* nos Estados Unidos da América, demonstram que atualmente o Irã conta com uma longa família de mísseis de curto, médio e longo alcance, com destaque para os já operacionais *Shahab*-3, com um alcance de 1.300 quilômetros (km); o Sejjil, de 2.000 km; o *Korramshahr*, ainda em fase de desenvolvimento e com alcance estimado em 2.000 km; e o *Soumar*, míssil de cruzeiro presumidamente operacional que pode alcançar até 3.000 km. Com exceção do *Khorramshahr*, todos os outros têm capacidade de transportar ogivas nucleares. A preocupação de *Trump* em conter o avanço tecnológico de *Teerã* nesse setor é compartilhada com aliados dos Estados Unidos da América no Oriente Médio como Israel, Arábia Saudita e Emirados Árabes Unidos.

[2] Worldometers: Countries in the world by population (2018). Disponível em: http://www.worldometers.info/world-population/population-by-country/ Acesso em: 2 de junho de 2018.

[3] A BP entende como energia primária os combustíveis comercializáveis, incluindo renováveis utilizados para gerar eletricidade: petróleo; gás natural; carvão; energia nuclear; energia hídrica e fontes renováveis como energia solar e eólica.

Embora os EUA tenham se retirado do Tratado, os outros países do P5+1 reafirmaram o interesse de cumpri-lo até o prazo de sua expiração. Por sua vez, o líder supremo do Irã, Aiatolá *Ali Khamenei*, definiu no dia 24 de maio três principais condições para permanecer no JCPOA: As potências europeias devem continuar comprando petróleo iraniano, protegendo suas exportações desse setor das sanções norte-americanas; não procurar abrir novas negociações envolvendo o programa de mísseis balísticos iranianos e sua presença no Oriente Médio; e garantir que os bancos europeus protejam o comércio com o país, assegurando o recebimento e pagamento de somas relacionadas a transações do Estado e do setor privado com a República Islâmica.

Embora as exigências iranianas possam ser consideradas como um ultimato para continuar aceitando as imposições restritivas ao desenvolvimento do seu programa nuclear determinadas pelos termos do JCPOA, tais reivindicações criam conflitos de interesses entre empresas e governos, visto que com a imposição de novas sanções as companhias europeias, chinesas e russas teriam restrições para investir no Irã. Se por exemplo uma empresa francesa opera nos Estados Unidos da América e no Irã, ela teria que obrigatoriamente se retirar de território sob jurisdição persa, do contrário poderia ficar impedida de realizar negócios nos Estados Unidos da América.

Dessa forma, não é possível afirmar ao certo qual será o futuro do JCPOA sem a participação dos Estados Unidos da América. Para mantê-lo vigente, os outros países do P5+1, em especial os europeus, terão que enfrentar um teste de independência diplomática em relação à *Washington* nas negociações com o Irã e, também, estabelecer mecanismos financeiros à parte do dólar que sustentem relações comerciais com *Teerã*. Embora o Euro seja uma moeda internacional forte, o mercado internacional de hidrocarbonetos é em grande parte pautado em dólares e parte significativa das receitas iranianas é obtida por meio da exportação de petróleo e gás natural.

Um possível esvaziamento do JCPOA pode fazer com que o Irã se retire do acordo e acelere seu programa nuclear com finalidade de obter capacidades para fins pacíficos e militares nesse setor. Tal cenário, poderia gerar uma corrida nuclear no Oriente Médio, pois se os israelenses e persas possuírem armas nucleares (mesmo os israelenses nunca tendo confirmado ou negado oficialmente a posse de tais artefatos), outras lideranças regionais como a Turquia, o Egito e a Arábia Saudita, por temerem por sua segurança, também podem desenvolver seus próprios arsenais nucleares com o intuito de contrabalancear o poder de *Teerã* e deles próprios.

GEOPOLÍTICA E ESTRATÉGIA

GEOPOLÍTICA NO ORIENTE: O HISTÓRICO DA PENÍNSULA COREANA*

***Daniel Mendes Aguiar Santos*[1]**

A Geopolítica estuda a influência dos fatores geográficos na vida e na evolução dos Estados, apoiando a condução da política e orientando a Defesa Nacional (ATENCIO, 1975). *Friedrich Ratzel* (1844-1904) e *Rudolf Kjellén* (1864-1922) pensaram o **território como fonte de poder**, ou seja, quanto mais território, maior a capacidade de um estado. Em particular, o inglês *Mackinder* (1904) detalhou a perspectiva de um centro da massa continental eurasiana denominado ***heartland*** cuja posse, por parte de uma potência terrestre, permitiria o domínio da Eurásia. Já o almirante norte-americano *Mahan* (1900) apresentou a visão de uma **zona oceânica mundial** cujo controle, por parte de uma potência marítima, permitiria o estabelecimento de pontos de apoio nas costas da Eurásia, viabilizando o controle do ***heartland***. Neste diapasão, *Nicholas Spykman* (1893-1943) indicou a necessidade de controlar as **extremidades da Eurásia** para dar conta da tridimensionalidade dos conflitos (terrestre, naval e aéreo), influenciando *Washington* a adotar uma doutrina de segurança baseada na estratégia da contenção e lastreada por uma política externa preemptiva.

Sob este prisma, ao observar o leste asiático, destaca-se a história da península coreana e observa-se o conflito entre os "Três Reinos" - *Koguryo* no norte, *Paekche* no sudoeste e *Silla* no sudeste. Em 668, o Reino de *Silla* derrotou os rivais e unificou a maior parte da península. A Coreia chegou perto de seus limites atuais durante a Dinastia *Koryo* (918-1392), origem do nome "Coreia". A seguir, a Dinastia *Choson* (1392-1910) consolidou as fronteiras e a cultura, com destaque para o alfabeto coreano (*Hangul*), promulgado pelo Rei *Sejong* em 1446. Neste processo, gradualmente, grupos e reinos concorrentes se fundiram em uma identidade nacional comum (CENTER FOR GLOBAL ASSOCIATION, 2019).

Na sequência, a região foi palco de invasões deflagradas pelos japoneses, no final do século XVI, e pelos *manchus* do nordeste da Ásia, no início do Século XVII. Fruto deste quadro conflitivo, a Coreia adotou uma política de contato estritamente limitado.

---

* Artigo originalmente publicado no dia 01 de março de 2019 no site do OMPV.

[1] Tenente-Coronel do Exército Brasileiro.

Os principais contatos estrangeiros eram missões diplomáticas para a China e um pequeno posto avançado de comerciantes japoneses na parte sudeste do seu território. Assim, por cerca de 250 anos, a península esteve em paz e estável internamente, em que pese a agitação camponesa dos anos 1800 (CENTER FOR GLOBAL ASSOCIATION, 2019).

Já no século XIX, a Coreia tornou-se objeto de interesses imperiais concorrentes, à medida que o Império chinês declinava e as potências ocidentais começavam a disputar a ascendência no leste asiático. Nos anos 1860, a Grã-Bretanha, a França e os EUA tentaram estabelecer relações diplomáticas e comerciais na região, mas o Reino Coreano resistiu firmemente. Por sua vez, o Japão, então aberto às relações internacionais com os Estados Unidos da América, impôs um tratado diplomático à Coreia em 1876. No final do Século XIX, Japão, China e Rússia rivalizaram a busca de influência na região. Em particular, o Japão, depois de derrotar militarmente a China e a Rússia, entre 1895 e 1905, tornou-se a influência externa predominante na península coreana (CENTER FOR GLOBAL ASSOCIATION, 2019).

Neste contexto, em 1910, o Japão anexou a Coreia e, no decorrer dos 35 anos seguintes, impôs um governo rígido e restritivo. Se por um lado, as autoridades japonesas tentaram acabar com a língua e a identidade cultural coreana, por outo lado, fomentaram o desenvolvimento industrial na região, instalando siderúrgicas, cimenteiras e indústrias químicas, nos anos 1920 e 1930, especialmente no Norte, servido de recursos de carvão e energia hidrelétrica. Já em agosto de 1945, no epílogo da 2ª Guerra Mundial, quando o governo colonial japonês foi encerrado, a Coreia já era o segundo país mais industrializado da Ásia, logo depois do Japão.

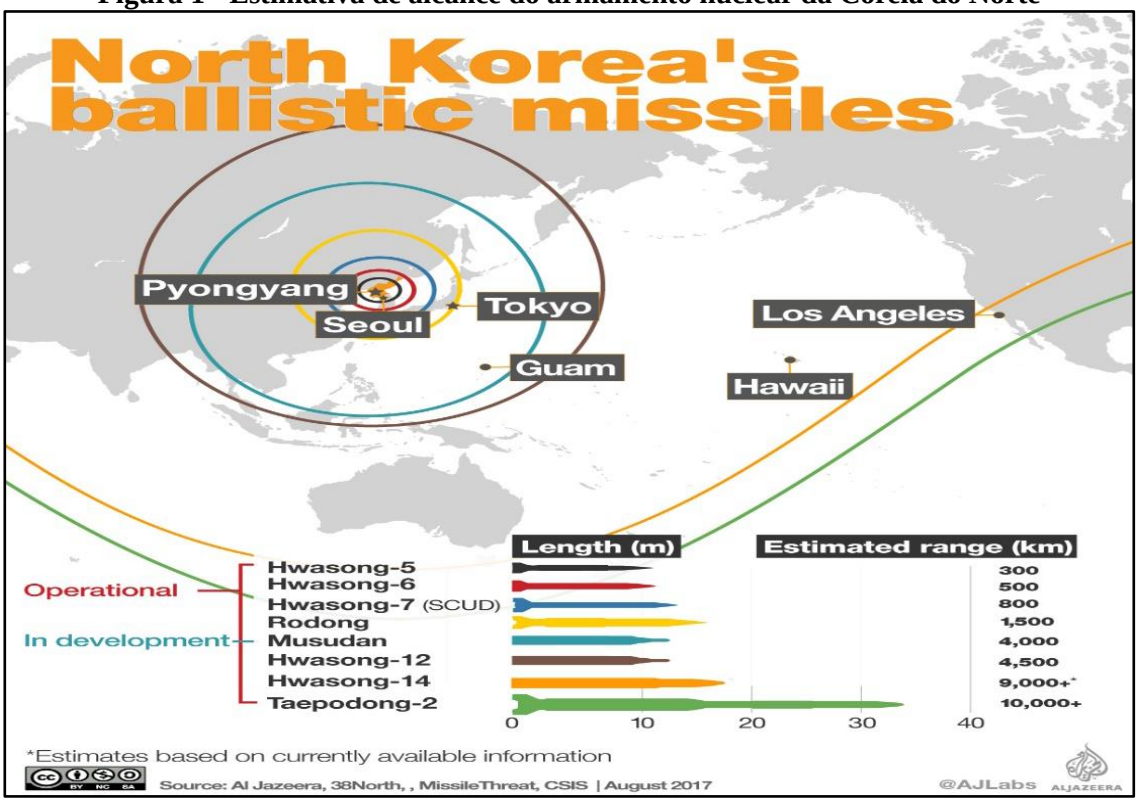
Por ocasião do fim da guerra, os Estados Unidos da América e a ex União das Repúblicas Socialistas Soviéticas (ex-URSS) acordaram a rendição japonesa na Coreia, com a ex-URSS ocupando a região ao norte do paralelo 38, e os Estados Unidos da América ocupando o sul, até que um governo coreano pudesse ser estabelecido. Contudo, em 1947, a geopolítica da Guerra Fria colapsou as negociações em prol de um governo unificado, resultando na divisão da Coreia em dois estados - a República Popular Democrática da Coréia, sediada em *Pyongyang* e pró ex-URSS; e a República da Coreia, sediada em Seul e pró-Estados Unidos da América.

Na fricção bipolar, em junho de 1950, a Coreia do Norte, apoiada pela ex-URSS, invadiu o sul e tentou unificar a península à força. Em contrapartida, sob a égide da Organização das Nações Unidas, uma coalizão liderada pelos Estados Unidos da

América veio em apoio da Coreia do Sul. No conflito, a ex-URSS apoiou a Coreia do Norte com armas e suporte aéreo, enquanto a República Popular da China enviou centenas de milhares de tropas. Finalmente, em julho de 1953, após a perda maciça de vidas, o conflito foi distendido, sendo a Coreia do Norte e a do Sul divididas em territórios, aproximadamente iguais, por uma linha de cessar-fogo (zona desmilitarizada), que ainda delimita a fronteira atual (RINNA, 2018).

Desde então, as duas Coreias evoluíram de uma base cultural e histórica comum para duas sociedades muito diferentes, com sistemas políticos e econômicos contrastantes (RINNA, 2018). A Coreia do Norte passou a ser influenciada pela cultura e política soviética/russa, bem como pela China. Ademais, desenvolveu uma política autodeclarada autossuficiente e armamentista, baseada na centralização econômica, tendo um regime totalitário, conduzido por *Kim Il-Sung* (1948-1994), *Kim Jong-Il* (1994-2011) e *Kim Jong-Un* (desde 2011). Por sua vez, a Coreia do Sul passou a ser influenciada pelos Estados Unidos da América, estreitando laços políticos, militares e econômicos, bem como pelo Japão. Tal relação, permitiu ganhos econômicos expressivos à Coreia do Sul, em especial nos anos 1970 e 1980. Fruto deste desenvolvimento, atualmente, é um dos países mais desenvolvidos do mundo, sendo a terceira maior economia do leste da Ásia, depois do Japão e da China.

Figura 1 - Estimativa de alcance do armamento nuclear da Coreia do Norte



Fonte: ARMACOST, 2001.

Referências:

ATENCIO, Jorge E. **Qué es la Geopolítica**. Buenos Aires: Editorial Pleamar, 1975.

ARMACOST, Michael H. **On the Record. Korea: A Geopolitical Overview**. Brookings, 2001. Disponível em: https://www.brookings.edu/on-the-record/korea-a-geo political -overview/. Acesso em: 09 de fevereiro de 2019.

CENTER FOR GLOBAL EDUCATION. **Korean History and Political Geography**. Disponível em: https://asiasociety.org/education/korean-history-and-political-geography Acesso em: 08 de fevereiro de 2019.

RINNA, Anthony. **The Korean Peninsula and Great Power Geopolitics: Then and Now**. Sinonk, 2018. Disponível em: https://sinonk.com/2018/11/05/the-korean-peninsul a-and-great-power-geopolitics-then-and-now/. Acesso em: 08de fevereiro de 2019.

PÊNDULO DO PODER: GEOPOLÍTICA DO LESTE ASIÁTICO*

***Daniel Mendes Aguiar Santos*[1]**

Quando a Guerra Fria terminou, as realidades no leste da Ásia mudaram. *Moscou* e *Pequim* encerraram vários programas de assistência à *Pyongyang* e passaram a explorar laços comerciais e diplomáticos com *Seul*. Por outro lado, *Washington*, foi incentivado pelo então Presidente da Coreia do Sul, *Roh Tae Woo* (1988-1993), a iniciar ações para tirar *Pyongyang* do isolamento político-econômico. Como consequência, tal geopolítica mudou o equilíbrio de poder na península coreana (ver mapa) em favor de *Seul* e isolou ainda mais o norte, acelerando o seu declínio econômico. Tal cenário instigou *Pyongyang* a avançar no desenvolvimento de armas nucleares, tanto para contrabalancear o crescente poder convencional do sul, como para obter uma alavanca diplomática capaz de forçar concessões por parte dos Estados Unidos da América.

Encapsulado neste dilema, *Washington* descobriu que o mundo pós-Guerra Fria, embora diferente, não era menos perigoso. No início dos anos 1990, ao negligenciar suas relações com Japão, China e Coreia do Sul, percebeu que não poderia modelar uma estratégia efetiva para lidar com o programa nuclear da Coreia do Norte. Desta forma, o fomento de armas nucleares por parte do norte, tanto elevou o risco de guerra, como ativou as negociações para o controle de armamento entre *Washington* e *Pyongyang*.

Pari passu, em 1992, a reunificação da Alemanha alimentou esperanças de que as duas Coreias também pudessem avançar em uma reconciliação. Fruto da degradação econômica vivida pela Coreia do norte calculava-se que a "janela de oportunidade" para reunificação viria, como no caso alemão, da derrocada do regime comunista, principalmente após a morte de *Kim Il-Sung*, em 1994, líder do país desde 1948. Contudo, o Norte não colapsou, bem como as autoridades sul-coreanas preservaram um timing de aproximação e optaram por um processo gradual de reconciliação, atentas aos custos econômicos e sociais da unificação, em especial, devido à crise financeira asiática no final dos anos 1990.

Neste processo, em junho de 2000, ocorreu a histórica reunião entre os líderes do sul e do norte, *Kim Dae-Jung* (1988-2003) e *Kim Jong-Il* (1994-2011), respectivamente. Fruto do encontro, o ambiente de relações diplomáticas mudou: a retórica hostil foi

---

* Artigo originalmente publicado no dia 29 de maio de 2019 no site do OMPV.

[1] Tenente-Coronel do Exército Brasileiro.

atenuada; incursões armadas na zona desmilitarizada cessaram; intercâmbios ministeriais foram iniciados; projetos de cooperação foram ativados (ligação ferroviária norte-sul, nova zona industrial em *Kaesong* e empreendimento turístico em *Mount Kumgang*). Ainda, a possibilidade de reuniões familiares, mesmo limitadas, motivaram as populações, contribuindo para a reconciliação. Lamentavelmente, no ano seguinte, o processo estagnou e os esforços diplomáticos diminuíram, reduzidos a esperanças e incertezas.

Sob a égide de um novo esforço para conter o recrudescimento da capacidade nuclear do Norte, em 12 de junho de 2018, foi realizada a Cúpula de Cingapura, entre a Coreia do Norte e os Estados Unidos da América, promovendo o encontro inédito entre o líder norte-coreano *Kim Jong-Un* e o presidente americano *Donald Trump*. Na ocasião foi assinada uma declaração conjunta, observando: garantias de segurança para o norte; relações pacíficas; a desnuclearização da península; negociações entre funcionários de alto escalão; e a recuperação de restos mortais de combatentes. Desde então, ambos os países têm negociado as garantias de segurança para o norte e o estabelecimento de relações diplomáticas. Ademais, *Pyongyang* tem solicitado o relaxamento das sanções econômicas ao regime de *Kim Jong-Un*. Por sua vez, *Washington* sustenta que as sanções permanecerão em vigor até que o Norte alcance a desnuclearização completa, porém, já nos últimos meses, indicou que poderia relaxá-las parcialmente, caso *Pyongyang* venha a tomar medidas significativas para ratificar seu compromisso de abandonar os programas nucleares.

Neste esforço, uma segunda reunião será realizada no Vietnã, nos dias 27 e 28 de fevereiro de 2019. Será o segundo encontro entre um presidente americano e um líder supremo norte-coreano. Espera-se que os dois líderes avancem nos objetivos estabelecidos na declaração de Cingapura, que comprometeu ambos os lados a forjarem uma nova relação diplomática e construir um regime de paz, assentado na desnuclearização da península. Preliminarmente, *Kim Jong-Un*, segue nos encontros com o presidente chinês, *Xi Jinping*, enquanto o presidente sul-coreano, *Moon Jae-in* destaca a importância do segundo encontro e de uma futura visita do presidente norte-coreano à *Seul*, como sendo pontos decisivos para solidificação da paz.

Neste diapasão, observa-se que desde os anos 1970, o equilíbrio de poder na península mudou drasticamente. Atualmente, *Seul* conta com mais do que o dobro da população do norte, sua economia é, pelo menos, 25 vezes maior do que a de *Pyongyang* e, além disso, é capaz de financiar maiores aumentos anuais em seu

orçamento de defesa do que o norte pode reunir. Tal cenário foi reforçado pela contração na economia da Coreia do Norte na última década.

Em especial, no tange ao dilema da segurança na península, as relações no Leste da Ásia são divididas em dois polos: uma parceria sino russa em apoio à Coreia do Norte, e um bloco liderado pelos Estados Unidos da América, incluindo o Japão e a República da Coreia.

Contudo, a possibilidade de uma fratura na parceria sino russa para com a Coreia do Norte tem sido pouco analisada. Embora a Rússia nunca tenha desfrutado de uma posição forte no leste da Ásia, ela tem interesses de longa data e de raízes geográficas na península coreana. Além disso, a geopolítica de *Moscou* tem enfatizado a recuperação do seu papel na região do Pacífico, atenta a uma mudança no equilíbrio de poder no leste asiático. Por outro lado, embora pareça improvável que a China desloque totalmente a força americana no leste asiático em um futuro próximo, há pouca dúvida de que o equilíbrio de poder, na região, pende mais a favor de *Pequim*.

Finalmente, quaisquer que sejam as diferenças entre as grandes potências do leste da Ásia, no que diz respeito à questão coreana, Pequim, Moscou e Tóquio compartilham com *Washington* um interesse em evitar a ressurgência de conflitos ou a proliferação de armas nucleares. Portanto, a premissa é a coexistência pacífica entre o norte e o sul, fato que demanda dos Estados Unidos da América uma ação de contrapeso no pêndulo de poder que habilita o equilíbrio geopolítico na região.

O DESENVOLVIMENTO ECONÔMICO DA COREIA DO SUL - DO DILEMA DA SEGURANÇA À PROSPERIDADE*

***Alex Alexandre Mesquita*[1]**

I. Introdução

A República da Coreia é um dos países mais desenvolvidos do mundo, no que diz respeito aos aspectos econômico, social e tecnológico, embora a sua história recente pudesse ter inviabilizado tudo isso.

Ao longo do último século, a Coreia do Sul passou, por um período colonial traumático; uma guerra fratricida, que ainda não terminou; a divisão de um povo em dois países antagônicos; e um governo militar que impôs diversas restrições à liberdade individual e coletiva. Apesar de todos esses obstáculos, atingiu um momento de prosperidade que desperta estudos e conclusões diversas.

Analisando sob a ótica das teorias das relações internacionais e de segurança nacional, é possível encontrar nos conceitos realistas[2] as orientações para o fabuloso desenvolvimento experimentado pelos coreanos. O conceito de Interesse Nacional[3] e o Dilema da Segurança[4], aplicados nas relações com a antagonista República Democrática da Coreia foram elementos importantes para um planejamento econômico detalhado, de longo prazo e, até o momento, exitoso.

Com base nessas perspectivas, este texto buscará analisar o desenvolvimento econômico da República da Coreia, desde a sua independência até os dias atuais, considerando o Dilema da Segurança como um dos principais propulsores do seu atual estado de prosperidade.

---

* Artigo originalmente publicado no dia 29 de maio de 2019 no site do OMPV.

[1] Coronel do Exército Brasileiro.

[2] Os Realistas, em geral, assumem uma visão pessimista de mundo, o que significa que um Estado não deve confiar em outro Estado e, por isso, deve perseguir o objetivo de aumentar o seu poder, de modo a garantir a sua segurança.

[3] Os Realistas foram os responsáveis por traduzir o conceito de Interesse Nacional. Na busca por alcançar e manter os Interesses Nacionais, os realistas consideram que a ética não é fator primordial nas relações entre os Estados, sendo assim, os mesmos podem quebrar qualquer acordo e desobedecer a qualquer regra moral, em nome desses interesses. Até os dias de hoje, diversos países utilizam as bases do pensamento Realista, como elemento orientador da sua política de Relações Internacionais.

[4] Para a corrente realista, o estado de segurança é conseguido por meio da maximização do poder do Estado e esta maximização será alcançada às expensas da segurança de outros Estados, criando o paradigma do Dilema da Segurança. Isto é, o Estado somente estará seguro, se estiver mais forte do que os seus antagonistas (NYE, 2004).

II. Desenvolvimento

a. A reconstrução a partir das ruínas

A Coreia é uma nação com centenas de anos. Durante o século XIX, a península coreana foi palco da rivalidade japonesa com a Rússia e com a China, sendo anexada ao Império do Japão em 1910, permanecendo uma colônia até o final da II Guerra Mundial (II GM), em 1945.

O período colonial foi responsável por impactar negativamente a educação, com a proibição do uso do idioma coreano, que foi substituído pelo japonês, repercutindo em um altíssimo nível de analfabetismo. Embora tenha cooperado com desenvolvimento industrial da porção norte do país, o Japão manteve o sul predominantemente agrário e pobre, com 70% da população vivendo da agricultura.

Durante o período colonial, a Coreia fornecia alimentos e funcionava como um complexo industrial japonês. Com o fim dessa relação imperialista, a Coreia permaneceu com instalações modernas em termos de transporte e de eletricidade, uma indústria relativamente importante, do têxtil à produção de armamentos, passando pela química e pela mecânica. Havia, também, um sistema bancário completo, mas toda essa modernidade estava ao norte. Nessa época, a classe dominante era pouco desenvolvida, pois a presença japonesa não lhe proporcionou muito espaço. Além disso, havia grande incidência de corrupção.

Com o final da II GM, a península foi dividida sob a administração dos Estados Unidos da América, ao sul, e da ex-União das Repúblicas Socialistas Soviéticas, ao norte. Em agosto de 1948, foi fundada a República da Coreia, ao Sul, e um mês depois a República Democrática Popular da Coreia, ao norte (HOUGH, 2008).

Com a fundação da Coreia do Sul, foi promulgada a sua Constituição, que trazia um forte impulso ao desenvolvimento individual. Os seus artigos 15, 16, 17 e 18, respectivamente, asseguravam o direito à propriedade, igual oportunidade de educação, direito e dever de trabalhar e liberdade de associação coletiva, para todos os trabalhadores. Assim, garantiu-se o desenvolvimento com base na qualificação da mão de obra.

Ao final da guerra, o Japão pagou indenizações aos países ocupados e a Coreia foi beneficiada durante um período de 10 anos. Dentre os países asiáticos que receberam os recursos, a Coreia do Sul foi o país que melhor utilizou o dinheiro, graças a um estrito controle do seu uso, diminuindo o desperdício e o desvio de finalidade do seu emprego.

Uma medida prática para alcançar esse objetivo foi a edição da Lei de Operação e

gerenciamento das repatriações japonesas, que proibiram o uso dos recursos para fins políticos e estabeleceu pena de cinco a dez anos de prisão para os casos de descumprimento e casos de corrupção e até mesmo pena de morte caso os valores desviados excedessem os US$ 50.000,00.

As tensões internas, já existentes após a libertação do colonialismo japonês, se agravaram por conta da forte presença soviética no norte. Essas mesmas ideias comunistas começaram a contaminar também o sul. Para conter essa influência e dentro da concepção realista de interesse nacional, foi realizada uma profunda reforma agrária para reduzir a onda bolchevique e combater as oligarquias rurais herdadas do período colonial.

Em sequência à conturbada libertação do jugo japonês, os antagonismos e planos de reunificação hegemônicos de cada uma das partes levaram à Guerra da Coreia, em 1950, primeiro conflito da Guerra Fria, empurrando uma Coreia do Sul pobre, iletrada e agrária para uma situação ainda pior. Cumpre sublinhar que a Coreia do Norte herdou o parque industrial do período colonial e, economicamente, estava em situação bem mais favorável (BREEN, 2017).

Em 1953, após a Guerra da Coreia, o antagonismo norte-sul acirrou-se materializando, de vez, o Dilema da Segurança. Os Estados Unidos da América iniciaram o apoio à reconstrução do país, por meio de donativos. Este apoio estrangeiro perdurou até meados da década de 1970 e os recursos foram utilizados com o mesmo critério e controle dos fundos japoneses, garantindo um emprego extremamente exitoso, que continuou impulsionando a economia.

O governo civil instituído em 1946, tendo à frente o Presidente *Syngman Rhee*, utilizou os fundos recebidos para incentivar o início da industrialização e aumentou o controle econômico, mas não esteve imune ao fantasma da corrupção, que acabou levando à sua deposição, por um movimento popular, que permitiu um golpe e o estabelecimento de um governo militar comandado pelo general *Park Chung Hee*.

O presidente *Park Chung Hee* exerceu forte liderança e reforçou ainda mais a intervenção do Estado na economia. Investiu forte na criação de uma indústria metalomecânica[5] e petroquímica, base do desenvolvimento econômico, que poderia ser mobilizada para a produção de material bélico, em caso de uma nova guerra com a

[5] A construção do complexo de ferro e aço, em *Pohang*, é o maior símbolo do uso das reparações japonesas pelo governo coreano. O investimento estimado foi de 119 milhões de dólares de um total de 500 milhões.

Coreia do Norte. O Dilema da Segurança passava orientar, cada vez de forma mais objetiva, os rumos econômicos do país.

Ainda, com foco no Dilema da Segurança a infraestrutura de transporte e comunicações já existente começou a ser ampliada, favorecendo as ligações em todo o país por meio de autoestradas e ferrovias modernas, que, além de transportar a produção, permitiram a mobilidade da população.

A partir de 1962, o financiamento externo evolui progressivamente, porém os donativos continuam a ser a fonte principal, até 1966. Os Estados Unidos da América incentivaram a Coreia a reatar relações econômicas com o Japão que, em seguida, assinou um acordo de dez anos (1965-1975), que previa uma ajuda econômica de 500 milhões de dólares, sendo 300 milhões sob a forma de donativos.

No período da administração do presidente *Park Chung Hee*, o combate à corrupção se tornou mais acirrado, com o estabelecimento de uma nova cultura no funcionalismo público, **que valorizava a integridade pessoal**. Um lema foi criado, com base na ideia de que o funcionário do governo deveria ver o "ouro" como uma simples pedra, alertando todos a não serem vítimas da ganância[6]. A corrupção, expandida no período colonial, ainda era uma grande sombra no governo coreano.

No campo da educação, este espaço de tempo recuperou o analfabetismo e iniciou o investimento no ensino técnico e das ciências exatas[7]. Ao dar instrução ao trabalhador da indústria, houve uma crescente melhora nos processos de produção, aumentando a eficiência e a qualidade dos produtos. Os coreanos dedicavam-se além dos demais países, buscando altos níveis de performance em todas as atividades. Graças à prioridade dada à formação profissional e à educação de base, havia quadros cada vez mais qualificados na força de trabalho.

A respeito desse período da história do desenvolvimento coreano, é possível entender que, após a época colonial e a destruição causada pela guerra fratricida interrompida em 1953, o Dilema da Segurança, paradigma do pensamento realista, foi principal impulso para a criação das bases econômicas. Por meio do planejamento, implementação e avaliação constante de resultados, combatendo a corrupção e o desperdício de recursos, foi possível implantar um parque metalomecânico e petroquímico; além de expandir as infraestruturas de transporte, comunicação e

[6] Segundo o presidente, "Se os funcionários públicos forem incorruptíveis, o povo viverá feliz por eles mesmos." (Discurso de Ano Novo em 1964).

[7] Ao final da II GM, 78% da população da Coreia do Sul não sabia ler ou escrever. Ao final de 1959, esse índice havia sido reduzido para 22%.

melhorar os índices de educação.

b. Da democratização à prosperidade

A partir da década de 1980, apesar do crescimento econômico, o governo militar começou a perder a confiança popular e, em junho de 1987, mais de um milhão de estudantes e cidadãos participaram de ações contra a administração central em escala nacional, que ficaram conhecidas como o "Movimento Democrático de Junho". Em **outubro de 1987**, depois de constituição revisada, eleições diretas do novo presidente foram realizadas em dezembro, o que marcou o **início da democratização coreana**.

Um dos legados pouco auspiciosos do período anterior, no campo do desenvolvimento, foi a desaceleração da economia. Com sindicatos fortes e salários mais altos, houve uma sensível redução da competitividade dos produtos coreanos no mercado internacional, resultando em exportações estagnadas, enquanto os preços das commodities continuavam a subir.

Com a democratização, a população começou a experimentar a liberdade e um crescente nível de prosperidade, distanciando-se cada vez mais da Coreia do Norte econômica e socialmente. O povo passou a perceber que o desenvolvimento econômico trazia consigo o progresso individual, o êxito material e a um elevado padrão de qualidade de vida. Em suma, os coreanos entenderam que **trabalho, aliado à liberdade gera prosperidade em grande escala**. Este passou a ser um grande diferencial em relação ao norte, e a prosperidade começou a se tornar um ativo de Segurança Nacional, ao reduzir a ameaça das ideias vindas da Coreia do Norte.

Contudo, no âmbito militar da Segurança Nacional, a ameaça norte-coreana mantinha-se cada vez mais crescente, com vários incidentes na zona desmilitarizada e confrontos de diversos tipos. Esta situação ainda contribuía para que a visão realista e o Dilema da Segurança continuassem a orientar a política e a economia da República da Coreia.

O bem-estar da população, como condição para a Segurança Nacional é uma construção da corrente idealista. Entretanto, como esclarecido anteriormente, o Dilema da Segurança continuava presente. Dentro desse conceito, para garantir a força do Sul, o norte precisava ser enfraquecido. Aliando os dois conceitos, percebe-se que, fortalecendo o bem-estar na Coreia do Sul, de maneira exponencial, o norte, em função das prioridades belicistas, não conseguiria acompanhar da mesma forma.

O sul da península coreana não foi presenteado com fartos recursos naturais e, até

hoje, as pessoas são consideradas maior riqueza do país. Nesse sentido, o incentivo à educação, iniciado no período da reconstrução, foi recebendo cada vez mais importância, em particular no **ensino universitário, com destaque para os cursos relacionados às Engenharias**. Segundo a concepção do período, o estudo das ciências exatas seria o grande responsável pelo desenvolvimento econômico e natural prosperidade.

Em consequência, a economia coreana passou de exportadora de commodities nas décadas de 1960, para produtora e exportadora de eletrônicos, navios, automóveis, máquinas em geral, produtos plásticos e têxteis na década de 1990 e chegou ao século XXI, como líder em semicondutores, computadores, produtos petroquímicos, telecomunicações, smartphones de última geração, tecnologia wireless e produtos de bem-estar para residências. Essa evolução já indicava o caminho promissor rumo a prosperidade, lastreada na educação.

O Dilema da Segurança, que impulsionou a indústria de base, passou a incentivar o desenvolvimento tecnológico. A independência em relação à produção de sistemas de comunicação, modernização da *internet*, melhoria da conectividade, dentre outros repercutiu novamente na melhoria do bem-estar da população[8], que estava cada vez mais convencida de que o modelo econômico de desenvolvimento estava no caminho certo. Dessa forma, independente das mudanças de governo, os rumos mantinham-se os mesmos.

Uma característica muito importante e que também está relacionada ao desenvolvimento é o nacionalismo e o sentimento de comunidade, construído ao longo de séculos. Estas condições fizeram com que o povo, após a democratização, mesmo discordando da orientação política do período militar, continuasse a apoiar as iniciativas desenvolvimentistas estruturadas na administração do presidente *Park Chung Hee* (DE MENTE, 2017) **Não houve, por parte do povo coreano, um sentimento de revanche ou de negação ao que foi construído no passado, mas sim um ímpeto de continuidade, em prol do desenvolvimento**.

Com o tempo, o distanciamento econômico entre norte e sul tornou-se um abismo e a população sul-coreana atingiu um nível de bem-estar que era inimaginável ao final

[8] Em palestra realizada em 2019, durante o *Capacity Bulding Workshop for Korea National Defense University Program*, o professor *Siwook Lee*, do *Korean Development Institute* declarou que a continuidade das políticas de desenvolvimento é constantemente cobrada ao governo por uma classe média cada vez mais esclarecida e participativa. Desta forma, segundo ele, mesmo com as mudanças sucessivas de governos, a prosperidade continua e não há desconstrução do legado anterior (GKEDC, 2019).

da década de 1953, quando a educação era precária e não havia um horizonte favorável. A prosperidade nacional trouxe a segurança social e se tornou um real elemento da segurança nacional, prevenindo tensões internas e externas, em particular a oriundas da Coreia do Norte (BO-KYUK, 2016).

O desenvolvimento da Coréia do Sul dos dias atuais revela um total contraste com a antagonista do norte, que hoje é um país governado com base em uma ideologia autoritária e obsoleta, que não alterou a sua percepção a respeito da segurança nacional, empregando os seus recursos econômicos no desenvolvimento de armas nucleares, empurrando o povo para mais uma crise alimentar.

O estudo do período pós-democratização, realizado de forma resumida, permite visualizar que o Dilema da Segurança, continua presente e é um paradigma para o desenvolvimento econômico coreano, transformando o país em referência tecnológica mundial, após organizar de forma robusta a sua indústria de base no período seguinte à Guerra da Coreia. O resultado é um país cada vez mais próspero. Hoje, essa prosperidade é o principal elemento de segurança social, que impacta diretamente na segurança nacional (BO-KYUK, 2016).

III. Conclusão

O desenvolvimento econômico da República da Coreia sempre esteve diretamente relacionado com a necessidade de garantir a segurança do país contra a ameaça da República Popular Democrática da Coréia.

Após a independência e fim da Guerra da Coreia, buscou-se a organização da indústria metalomecânica e petroquímica, para apoiar um possível esforço de guerra contra a Coreia do Norte, dentro de uma lógica de pensamento realista de segurança nacional, que foi responsável por estabelecer as bases da economia coreana. Com a democratização, por meio do crescente desenvolvimento baseado no campo tecnológico, foi criado um ciclo virtuoso de prosperidade e de bem-estar, que tem mantido a segurança do país contra ameaças mais difusas.

Em resumo, o desenvolvimento econômico teve o grande objetivo de dotar a República da Coreia de condições para combater e derrotar a Coreia do Norte, inicialmente atendendo a uma lógica realista e, em seguida, evitar a influência comunista, dentro de uma lógica Idealista, mas sempre com a influência do Dilema da Segurança.

A Coreia sempre foi um paradigma de desenvolvimento para países emergentes e

a comparação com a trajetória brasileira é inevitável. O Brasil e a Coreia foram contemporâneos em muitos desafios, dentre eles as mudanças políticas e o desenvolvimento econômico das décadas de 1950, 1960, 1970 e 1980 do século passado. Contudo, observando o atual estado de prosperidade coreana, pode-se dizer que o Brasil perdeu o seu caminho em algum momento da história. Cabe a esta geração identificar como isso ocorreu e orientar a retomada do progresso.

Referências:

BO-KYUK, Suh. **Resolving the Korean Conflict through a Combination of Human Rights and Human Security.** The Korean Journal of International Studies, Vol. 14, nº 1, p. 53-75, 2016.

BREEN, Michael. **The New Koreans.** Nova Iorque: Thomas Dunne Books, 2017.

DE MENTE, Boyé Lafayette. **The Korean Mind-Understanding Contemporary Korean Culture**. Vermont: Tuttle, 2017.

GLOBAL KNOWLEDGE EXCHANGE & DEVELOPMENT CENTER. **Capacity Bulding Workshop for Korea National Defense University Program.** Seoul, 2019.

HOUGH, Peter. **Understanding Global Security**. London: Routledge, 2008.

NYE, Joseph S. **Soft Power-The Means to Success in World Politics, Public Affairs.** Nova Iorque: Perseus Book Groups, 2004.

PAN AMAZÔNIA E OS SISTEMAS DE MONITORAMENTO*

***Ana Carolina da R. Monteiro Teixeira*[1]**

O monitoramento ambiental por satélites é de grande utilidade para o combater o desmatamento, queimadas e a degradação ambiental, gerando dados que servem como subsídio para a implementação de políticas públicas de combate ao desmatamento e propiciam maior participação e controle social.

Figura 1- Reprodução/Ipea/Exército Brasileiro

Fonte: SATRIFO, 2019.

Dos países que constituem a Pan Amazônia, a Bolívia possui um sistema de monitoramento remoto próprio, o SATRIFO, que fornece informações para a prevenção e controle de incêndios florestais no país.

Esse sistema trabalha com o próprio FAN (Fundación Amigos de la Naturaleza) e conta também com o INPE e o país também trabalha com o Sistema de Alerta Pilcomayo (contam também com esse sistema o Paraguai e a Argentina).

Os outros países que constituem a Pan Amazônia não possuem sistemas de monitoramento próprios, e contam com sistemas via satélite da NASA e Copernicus (Programa Europeu de Monitoramento Global do Meio Ambiente e Segurança) por exemplo. Isso faz com que o INPE (Brasil) e o CENSIPAM se destaquem no que toca

* Artigo originalmente publicado no dia 10 de setembro de 2019 no site do OMPV.

[1] Graduanda em Relações Internacionais.

ao monitoramento remoto da Pan Amazônia, subsídios com dados e imagens as políticas e estratégias de defesa.

Referências:

SATRIFO. **Focos de Calor**. Satrifo, 2019. Disponível em: https://incendios.fan-bo.org/Satrifo/mapa-interactivo/. Acesso em: 04 de setembro de 2019.

A GEOPOLÍTICA DE MEIRA MATTOS E A AMAZÔNIA*

***Gregor de Rooy*[1]**

O General Carlos de Meira Mattos (1913 - 2007) chegou à patente de General de Divisão e, além de notória carreira militar, destacou-se pelos seus estudos de geopolítica. Para os estudiosos do assunto como Miyamoto, Kelly, Freitas e Costa, Meira Mattos é um dos mais importantes geopolíticos brasileiros.

Além da vasta produção (foram nove livros que trataram de geopolítica publicados ao longo de 42 anos, 1960 - 2002), seus estudos evidenciam uma característica do pensamento geopolítico nacional em que a cada autor/publicação adiciona-se um novo aspecto complementar à literatura anterior. Assim, numa geopolítica marcada pela continuidade na defesa de teses centrais sendo a principal a importância da integração nacional para a manutenção do território, Meira Mattos acrescenta novos aspectos ou fortalece outros aspectos já mencionados, porém não desenvolvidos pelos geopolíticos anteriores a ele. A dizer, a necessidade de formação de uma elite nacional consciente das realidades geopolíticas do Brasil, a constante consulta à história em sua análise geopolítica, o diálogo entre esta e a ciência política, relações internacionais e estratégia.

Ao tema da integração nacional, anteriormente pensado a partir da importância da expansão da infraestrutura dos meios de transportes, é acrescentada a importância da infraestrutura de telecomunicações e infraestrutura energética. Todos estes aspectos deveriam estar a serviço do desenvolvimento do território nacional que garantiria a segurança, o progresso do país e sua ascensão ao status de potência. Para isso, Meira Mattos sugere um novo manejo das elites dirigentes. Assim, recorre repetidas vezes a uma das máximas do historiador inglês *Arnold Toynbee*, que diz:

> "Após uma etapa de crescimento, algumas sociedades humanas entraram em colapso pela perda do poder criador das minorias dirigentes, que, à míngua de vitalidade, perderam a força mágica de influir sobre as massas não criadoras e de atraí-las" (TOYNBEE apud MATTOS, 2011a, p. 54).

---

* Artigo originalmente publicado no dia 04 de outubro de 2019 no site do OMPV.

[1] Doutorando em Ciências Militares na ECEME.

Logo, a geopolítica, definida pelo autor como um ramo da política que trata da sua aplicação aos ***espaços geográficos*** (MATTOS, 2011b), certamente seria melhor aplicada no território nacional se as elites dirigentes dela tivessem consciência.

É neste e deste arcabouço teórico e conceitual que o autor se debruça, principalmente, sobre as fronteiras, a região amazônica e a posição do Brasil no mundo. O tema das fronteiras, especialmente as terrestres, é analisado por Meira Mattos com riqueza de detalhes históricos, geográficos e densidade teórica. Em claro exercício de práxis geopolítica, Meira Mattos sugere uma solução mais econômica do que militar para a segurança das fronteiras. Isto se daria por meio da criação de áreas de intercâmbio fronteiriço e do povoamento da faixa de fronteira.

A questão da posição e da realidade geográfica do Brasil no mundo é estudada em sintonia com as possibilidades de o país tornar-se uma potência. Para isso são analisados diferentes números (população, dimensão territorial, recursos naturais e etc...), autores e cálculos de mensuração do Poder Nacional em que o autor sugere uma fórmula própria.

Já o território nacional per se é analisado em convergência com a estratégia em ***Estratégias Militares Dominantes*** (MATTOS, 2011c) onde é feito notório levantamento das contribuições de autores clássicos de estratégia. Para Meira Mattos, o território brasileiro deveria ser palco de uma política militar, a princípio, defensiva. Esta política implicaria essencialmente na vigilância das fronteiras terrestres, marítimas, aéreas e na preservação das rotas sem as quais não haveria a necessária liberdade de movimentação de pessoas, mercadorias e tropas (MATTOS, 2011d).

Além do tema das fronteiras, da posição do Brasil no mundo e de uma estratégia militar defensiva em congruência com a realidade geográfica brasileira, Meira Mattos analisa desafios geopolíticos domésticos e aí se concentra a maior parte de sua produção. Sobre estes desafios, a questão do desenvolvimento nacional é indissociável da questão do desenvolvimento territorial e, consequentemente, a Defesa Nacional seria mais bem garantida se os dois primeiros aspectos fossem pensados juntos e geridos com maior eficácia. É por isso que sua geopolítica, antes de falar em Forças Armadas e projeção de poder (não olvidados pelo autor) fala mais em desenvolvimento, especialmente o de infraestruturas, que permitisse a integração nacional ou até mesmo o povoamento de áreas ermas como partes da região amazônica. Para isso, além de elites mais bem preparadas, o estado deveria também ter ou criar o adequado aparato legal e burocrático.

É com esta visão que o autor desenvolve densa análise sobre a região Amazônica principalmente na obra: Uma Geopolítica da Pan-Amazônia (MATTOS, 2011e). Observa Meira Mattos, com riqueza em detalhes históricos, que a região sempre foi objeto da cobiça por parte de outros estados tais como a França, os Estados Unidos da América; institutos como o Instituto *Hudson* e organizações internacionais como a UNESCO. Neste contexto, a sua geopolítica ganha contornos interessantes e pouco comuns em demais autores. Meira Mattos a desenvolve também em diplomático diálogo com os escritos de autoridades de estados vizinhos tais quais os ex-presidentes venezuelanos *Rafael Caldera* e *Andrés Peres*, o ex-chanceler venezuelano *Alberto Zambrano* e o General peruano *Edgardo Mercado Jarrí*n de modo que expõe a convergência de pensamentos geopolíticos sobre a região e pensa em uma geopolítica autenticamente Pan-Amazônia que representasse ou convergisse os objetivos de todos os estados formadores da bacia Amazônica.

Este diálogo e esta geopolítica foram pensados em conjunto com as expectativas do autor para o Tratado de Cooperação Amazônica assinado entre Bolívia, Brasil, Colômbia, Equador, Guiana, Peru, Suriname e Venezuela em 1978. Em poucas linhas o tratado previa criar um mecanismo de desenvolvimento da região amazônica sem que nenhum dos países renunciasse às respectivas soberanias territoriais (CPDOC, 2009).

A região amazônica, para o autor, é entendida como desafio e "Às" geopolítico. Desafio devido a sua imensidão geográfica, fronteiras diversas e densa floresta equatorial. Às por causa das riquezas naturais e do fato do país, entre as 10 economias do mundo, ainda ter uma imensa "reserva" territorial para a qual poderia se desenvolver. Assim, a estratégia descrita por Meira Mattos e realizada por diferentes governos (sendo o Militar o mais enérgico até então) é uma estratégia mais focada no desenvolvimento econômico da região do que na expansão da malha operacional militar. Sobre este desenvolvimento, o autor cita uma série de projetos de infraestrutura, indústria, habitação, pecuária, agricultura e atividades extrativistas; também cita instituições/organizações (SUDAM, SUFRAMA, INCRA, BASA) ligadas ao Estado que deveriam gerir os projetos. Ademais, o autor sugere a criação ou fortalecimento de cidades polos de desenvolvimento que poderiam ressoar/reverberar para o restante da região.

Em poucas linhas, esta foi a sua geopolítica. Um trabalho de densa consulta a diferentes teóricos, intelectuais, fatos históricos e contumaz defesa da ideia de que o desenvolvimento e integração territorial dependeriam de uma elite mais preparada. À

tradição geopolítica brasileira, Meira Mattos acrescentou a relevância da infraestrutura de energia e telecomunicações e, com menor ênfase, a importância de uma indústria e tecnologia nacionais e coesão social que pudessem viabilizar projetos de integração, povoamento das regiões ermas e defesa do território. Todas estas políticas viabilizariam uma estratégia de defesa mais robusta.

Frente aos desafios desta década e das que se avizinham cabe-nos dar continuidade ao pensamento geopolítico nacional que há muito tem contribuído em políticas públicas. Novos elementos foram introduzidos por Meira Mattos e ainda podem e devem ser mais estudados e aplicados tendo em vista o desenvolvimento e a soberania da Nação.

Referências:

BECKER, Bertha. K. **Geopolítica da Amazônia.** Estudos avançados, Vol. 19, nº 53, p.71-86, 2005.

FGV - CPDOC. **Tratado de Cooperação Amazônica**. CPDOC, 2009. Disponível em: http://www.fgv.br/cpdoc/acervo/dicionarios/verbete-tematico/tratado-de-cooperacao-amazonica-1978. Acesso em: 14 de setembro de 2019.

MATTOS, Carlos de Meira. **Geopolítica e modernidade**. Rio de Janeiro: Editora FGV, 2011a.

MATTOS, Carlos de Meira. **Brasil: geopolítica e destino**. Rio de Janeiro: Editora FGV, 2011b.

MATTOS, Carlos de Meira. **Estratégias militares dominantes**. Rio de Janeiro: Editora FGV, 2011c.

MATTOS, Carlos de Meira. **Geopolítica e teoria de fronteiras**. Rio de Janeiro: Editora FGV, 2011d.

MATTOS, Carlos de Meira. **Uma geopolítica pan-amazonica**. Rio de Janeiro: Editora FGV, 2011e.

SOBERANIA E PAN AMAZÔNIA[*]

Erick Andrade Santos Couto[1]

Quando observamos o campo de conhecimento habitado pela geopolítica, percebemos que se trata de uma área que detém como fim analisar as relações entre poder e espaço geográfico. Ou como afirma o General Meira Mattos definindo a geopolítica como sendo a política aplicada aos espaços geográficos (MATTOS, 1980). As dinâmicas da disputa geopolítica, ao longo do tempo, vêm se transfigurando. No início, os contenciosos geopolíticos detinham como propósito final o Estado, pois os conflitos eram realizados somente entre Estados. Além disso, o Estado era percebido como a única fonte de poder e representação política.

Tratando da geopolítica em tempos mais recentes, a mesma procura por intermédio do poder influenciar na tomada de decisão dos Estados acerca do usufruto do território, pois os modelos mais clássicos da dinâmica geopolítica, tais como a conquista de colônias e a conquista de territórios passaram a ser bastante onerosas. Com isso, notamos a propagação da chamada ***coerção velada***. Em outras palavras, pressões de maneiras variadas e distintas que tem por fim influenciar a administração dos Estados sobre o uso de seus territórios.

Como aponta *Bertha Becker*, nos dias de hoje o mundo passa por uma inclinação ao internacionalismo dos movimentos sociais. Tais movimentos detém suas próprias territorialidades, suas próprias geopolíticas e tendem a articularem-se, se transformando em um fenômeno global deveras complexo (BECKER, 2005).

Mas onde o Brasil e, sobretudo, a Amazônia se enquadra nessa dinâmica?

Ao longo do tempo, não é muito difícil notar a cobiça por parte das potências estrangeiras na região visando obter as riquezas da Pan Amazônia (FELLET, 2019). Como nas décadas de 1850 e 1860, na qual os Estados Unidos, a França e o Reino Unido buscavam o acesso ao rio Amazonas. Para isso, se utilizaram da bandeira do espírito do livre comércio e do liberalismo para terem direito de navegar pelo rio. Ou em uma declaração da então premiê britânica *Margareth Thatcher*, em 1983, na qual compactou com os rumores de internacionalização da Amazônia e foi a favor da

[*] Artigo originalmente publicado no dia 11 de Dezembro de 2019 no site do OMPV.
[1] Doutorando em Ciências Militares na ECEME.

tentativa de atrelar a dívida externa de países emergentes à venda de recursos naturais. Reduzindo dessa forma, o poder dos Estados em gerir suas próprias riquezas na Amazônia. Como na fala do então presidente da França *François Mitterrand*, anos depois, que afirmou a necessidade de aceitação por parte do Brasil uma soberania relativa da Amazônia. Na declaração do democrata americano *Al Gore*, que durante sua campanha eleitoral rumo a presidência nos anos 2000 afirmou que os brasileiros achavam que a região amazônica era somente deles.

Logo em seguida afirmou que não era, a Amazônia era de todos. Posterior a isso, o então senador *Robert Kasten* reafirmou essa linha de pensamento ao dizer: "Assim como o ozônio, as chuvas, o oxigênio etc., a Amazônia deve pertencer a todos".

Por vezes, os anseios por parte das potências estrangeiras se escondem por detrás de bandeiras ou discursos humanistas, como o livre mercado, o liberalismo, a ciência ou o meio ambiente por exemplo. Essa ação acaba por mascarar as verdadeiras intenções desses Estados. Em tempos recente, vemos a tentativa de ingerência por parte dos Estados europeus, em especial a França, no que diz respeito a administração e proteção da Amazônia, na qual é utilizado o discurso da proteção ambiental visando a internacionalização da Amazônia. Como exposto acima, podemos observar que esse tipo de discurso não é atual e nem sempre está ligado diretamente ao meio ambiente. Os temas nos discursos variam ao longo do tempo, mas a ambição continua sendo a mesma, o controle do maior ativo estratégico brasileiro.

E qual é a reação do Brasil e dos outros países que pertencem a Pan Amazônia?

No dia 06 de setembro, na cidade de Letícia, na Colômbia, ocorreu uma reunião entre os chefes de estado dos países amazônicos. O encontro para o chamado "Pacto de Letícia pela Amazônia" procurou discutir a ação dos países em uma política única no que diz respeito a preservação do meio ambiente e normas para a exploração das riquezas amazônicas. O Pacto possui 16 pontos que transparecem o compromisso dos Estados em se unirem e agirem no combate ao desmatamento, a principal causa dos incêndios (MANETTO, 2019). Os países acordaram criar mecanismos de cooperação regional e de intercâmbio de informações, dando base para não só o combate as queimadas, mas também a outras atividades ilícitas (TRT, 2019). Outro ponto abordado pelos países signatários do Pacto é a reinvindicação "[d]os direitos soberanos dos países da região sobre seus territórios e recursos naturais, incluindo o desenvolvimento e o uso sustentável desses recursos". Dentre os integrantes do Pacto, o Brasil foi o mais incisivo no que tange a relativização da soberania, tendo o presidente brasileiro Jair Bolsonaro

destacado a necessidade de união dos Estados "sem nenhum ceder a qualquer tentação externa de deixar sob administração de terceiros nossa área (Amazônia)".

A Amazônia e a soberania na região sempre foram um tema muito sensível para o Brasil, em especial para os militares brasileiros e como afirmou o chanceler colombiano *Carlos Holmes Trujillo*, "as ações deverão compreender não só os países amazônicos, mas também os países da América do Sul". A falta de um mecanismo ou instituição fixa que seja um fórum de diálogo e formação de coalizões políticas na região, aos moldes do CDS[2], dificulta uma resposta rápida e coesa frente as tentativas de ingerência de nações estrangeiras (FUCILLE; REZENDE, 2013). É possível notar também que, desde o governo Dilma, há a falta de uma liderança brasileira na América do Sul e na representatividade dos países sul-americanos no sistema internacional. Um fato que ilustra esse cenário é a não participação do Brasil nas reuniões do G7, lugar que ocupou entre os anos de 2003 e 2011[3]. Não exercer a liderança regional acarreta um vácuo de poder no subcontinente sul-americano, dando assim a possibilidade para que outros Estados busquem ocupar esse lugar. Pois não existe espaços vazios de poder nas relações internacionais.

Referências:

BECKER, Bertha. K. **Geopolítica da Amazônia.** Estudos avançados, Vol. 19, nº 53, p.71-86, 2005. Disponível em: http://www.scielo.br/pdf/ea/v19n53/24081.pdf. Acesso em: 15 de setembro de 2019

FELLET, João. **De Fordlândia a 'bem comum': as contradições na história do interesse estrangeiro na Amazônia.** BBC, 2019. Disponível em: https://www.bbc.com/portuguese/brasil-49363394. Acesso em: 15 de setembro de 2019.

FUCCILLE, Alexandre; REZENDE, Lucas Pereira. **Complexo regional de segurança da América do Sul: uma nova perspectiva.** Contexto Internacional, Rio de Janeiro, Vol. 35, nº 1, p. 77-104, 2013.

MANETTO, Francesco. **Sete países amazônicos acertam uma agenda contra a crise ambiental.** El País, 2019. Disponível em: https://brasil.elpais.com/brasil/2019/09/06/internacional/1567786813_480794.html. Acesso em: 15 de setembro de 2019.

MEIRA MATTOS, Carlos de. **Uma geopolítica Pan-Amazônia.** Rio de Janeiro: Biblioteca do Exército, 1980.

[2] Conselho de Defesa Sul-Americano. O CDS é um órgão de concertação e interlocução entre os Estados que o compõe, detendo da capacidade de incentivar o intercâmbio no que tange aos temas sobre segurança e defesa, cujas decisões só podem ocorrer se forem acordadas por consenso e com previsão de pelo menos um encontro anual (FUCCILLE; REZENDE, 2013).

[3] Com exceção de 2004.

TRT. **Em que consiste o Pacto de Letícia pela Amazônia assinado na Colômbia?** TRT, 2019. Disponível em: https://www.trt.net.tr/portuguese/ciencia-e-tecnologia/2019/09/08/em-que-comsiste-o-pacto-de-leticia-pela-amazonia-assinado-na-colombia-1265451. Acesso em: 15 de setembro de 2019.

MOVIMENTOS MIGRATÓRIOS

OPERAÇÃO ACOLHIDA: UMA AÇÃO ESSENCIAL EM RORAIMA*

***Tássio Franchi*[1]**

Pouco conhecida da maioria dos brasileiros, a Operação Acolhida é uma ação fundamental para o estado de Roraima, para o Brasil e para dezenas de milhares de pessoas desassistidas que chegam às nossas fronteiras, e que já somam mais de 200 mil nos últimos anos. A mais notória onda migratória que o Brasil recebe advém da Venezuela, dado o contexto político-social daquele país. Recordemos que, ao final do século XX, *Hugo Chaves* chegou ao poder na Venezuela. Falecendo em 2013, deixou o poder para seu indicado ao cargo, *Nicolás Maduro*, atual presidente. Devido a uma série de questões conjunturais, o país vem passando por dificuldades que têm levado milhões de venezuelanos a deixar o país em busca de novas oportunidades.

A Venezuela possui aproximadamente 2.199 Km de fronteira com o Brasil (12,2% das fronteiras terrestres brasileiras), além de limites com a Colômbia e a Guiana. O Estado venezuelano de Bolívar faz fronteira com os estados do Amazonas e Roraima. Roraima é o estado mais setentrional do Brasil e tem características peculiares: está isolado da rede elétrica nacional, o que limita a instalação de indústrias; possui grandes áreas demarcadas como Terras Indígenas; dispõe de uma oferta limitada de postos de trabalho; e tem uma baixa densidade demográfica, que se converte em um planejamento estatal de infraestrutura de saúde, segurança e educação dimensionada para a população existente, cerca de meio milhão de pessoas.

Em todo o Amazonas e parte de Roraima, a fronteira é dominada pela floresta amazônica, criando uma região de difícil acesso. Todavia, foi no estado de Roraima, mais especificamente na cidade de Pacaraima (distante 200 km da capital Boa Vista), que se estabeleceu a porta de entrada da maioria dos venezuelanos que chega ao Brasil. Isso ocorre pois parte da fronteira entre os países é no lavrado roraimense, uma região com vegetação e relevo semelhantes ao cerrado, que possibilita o trânsito mais fácil de pessoas. Além disso, é nesta região que se encontram as rodovias que ligam os dois países, a BR-174 e a Ruta 10.

Desde 2016, o volume de venezuelanos que cruzaram a fronteira aumentou

---

* Artigo originalmente publicado no dia 03 julho de 2019 no site do OMPV.

[1] Doutor em Desenvolvimento Sustentável e Professor da ECEME.

gradativamente. As limitações da capacidade do estado de Roraima ficaram evidentes em 2017. Desta forma, em fevereiro de 2018, o governo federal editou a Medida Provisória (MP) 820, dando início a uma operação interministerial voltada ao ordenamento da fronteira e ao acolhimento aos deslocados, a Operação Acolhida. A MP 820 foi transformada na Lei nº 13.648, de 21 de junho de 2018, ganhando, assim, um caráter mais permanente. Além do governo federal, o poder estadual, municípios de Roraima, grupos da sociedade civil organizada, a Igreja, organizações não-governamentais (ONG's) e entidades internacionais têm cooperado no acolhimento aos venezuelanos. As Forças Armadas (FFAA), em especial o Exército Brasileiro e a Força Aérea Brasileira, têm sido peças fundamentais neste processo.

As ações estão estruturadas sobre três pilares: ordenamento da fronteira, abrigamento e interiorização. Nessas ações, a 1ª Brigada de Infantaria de Selva, sediada em Boa Vista, intensificou as atividades na Faixa de Fronteira (150 km) e nas principais vias de acesso, garantindo o ordenamento territorial e encaminhando os deslocados para as estruturas da Operação Acolhida.

Com relação aos deslocados que adentram o território nacional, foram visualizadas soluções duráveis que garantissem amplas opções, em conformidade com a legislação nacional e internacional, para os venezuelanos. Destacam-se entre essas ações o repatriamento voluntário ao seu país de origem; a passagem segura pelo território nacional em busca de outro destino, algo que tem se mostrado a opção de um grande número de venezuelanos; a integração no local de chegada com o acolhimento jurídico, social e econômico do migrante pela sociedade local; e, por fim, a interiorização ou reinstalação, que garanta melhores chances de inserção social dos deslocados.

Mais da metade dos venezuelanos que chegaram ao Brasil desde 2018 já deixou o país. Parte retornando à Venezuela, em um movimento pendular típico das regiões de fronteira, e outros rumo a outros países da América do Sul. Atualmente, a Colômbia é o país que mais recebe os deslocados venezuelanos, com mais de um milhão de solicitações de entrada no país.

Neste ínterim, a Operação Acolhida tem gerenciado uma série de infraestruturas críticas ao sucesso da missão. Pode-se mencionar os postos de recepção, triagem, atendimento médico e abrigos para indígenas e não indígenas, que estão montados em Pacaraima, na linha de fronteira. Em Boa Vista, são mais 11 abrigos que atendem a mais de 6 mil pessoas simultaneamente. Por ali já passaram centenas de venezuelanos que deixaram os abrigos, porque já conseguiram empregos, porque retornaram à Venezuela,

ou ainda porque parte deles foi deslocada para outros estados da federação no processo de interiorização voluntária.

A interiorização já atendeu mais de 11 mil venezuelanos, levando-os para outros estados em parcerias com ONG's e com a sociedade civil. Existe uma dupla importância neste processo. Primeiro, aliviar a pressão sobre as infraestruturas do estado de Roraima e dos municípios diretamente afetados pelo fluxo migratório. Segundo, propiciar melhores chances de integração para os deslocados venezuelanos em regiões onde possam ser aproveitados no mercado de trabalho. A interiorização é uma parte essencial da Operação Acolhida e tem conseguido redistribuir cerca de 500 venezuelanos por mês com o apoio da Força Aérea Brasileira, de companhias de aviação que doam assentos em voos comerciais e de entidades da sociedade civil que custeiam passagens por meio de suas redes de solidariedade.

A história nos mostra que crises migratórias em algum momento se estabilizam e depois retrocedem. Observou-se esse movimento com os refugiados haitianos, que após um período de intensa chegada, reduziram o fluxo de entrada no Brasil nos anos recentes. Entretanto, se a situação econômica e social na Venezuela não melhorar, o fluxo de pessoas buscando melhores condições deve se manter. Mesmo que aconteçam oscilações nos números totais de entradas de venezuelanos em determinados períodos, será preciso manter uma estrutura com flexibilidade e capacidade de atender às demandas futuras. Isto implica a necessária manutenção da assistência aos deslocados, ainda que no curto e médio prazo.

Com certeza, o Exército Brasileiro estará presente, contribuindo na construção de soluções que o país postular. Entretanto, as Forças Armadas têm como atividade-fim a defesa da Pátria (art. 142 Cf. 1988) e será preciso pensar o que é melhor para o país. Continuar a empregar as FFAA neste tipo de ação ou estruturar e capacitar outras instituições públicas federais ou estaduais para gerirem a assistência aos deslocados? Será que não é o momento de o governo federal começar a planejar uma saída das Forças Armadas como protagonistas desta ação? Ou, caso a decisão seja pela continuidade delas na missão, como fazer para que isso não prejudique sua missão principal de vigilância de nossas fronteiras em todo o território nacional?

ALGUMAS REFLEXÕES SOBRE A SITUAÇÃO NA FRONTEIRA BRASIL-VENEZUELA E OS EPISÓDIOS DE SEU FECHAMENTO*

***George Alberto Garcia de Oliveira*[1]**

O presente texto tem por finalidade apresentar algumas reflexões sobre a fronteira BRASIL-VENEZUELA, com foco na região de Pacaraima, e dos episódios de fechamento dessa fronteira, ocorridos em 6 de agosto de 2018, por determinação de um juiz federal brasileiro, e no período de 21 de fevereiro a 10 de maio de 2019, por determinação do governo venezuelano.

Inicialmente, cabe ressaltar que importantes geopolíticos, ao longo da história, registraram a importância das fronteiras para os Estados. O alemão *Friedrich Ratzel* defendia que a fronteira seria o órgão periférico do Estado, cuja localização materializa o dinamismo, a força e as mudanças territoriais do Estado. *Karl Ernst Haushofer*, outro geopolítico e militar alemão, registrou que as fronteiras seriam motivo de permanente litígio entre os Estados. O sueco *Kjéllen* comparava as fronteiras do Estado à epiderme de um corpo vivo, que receberia e transmitiria, em primeira mão, todas as manifestações de poder emitidas ou dirigidas ao "cérebro" estatal, destinadas ou vindas do exterior. O brasileiro Everardo Backheuser, a seu turno, considerava que as fronteiras refletiam o poder de um Estado, devendo, portanto, serem protegidas.

Independentemente das diferentes abordagens dos geopolíticos acima mencionados, não resta dúvida que os fatos que acarretam mudanças na dinâmica da fronteira de um Estado devem ser acompanhados pelo governo. Trazendo para a nossa realidade, pode-se considerar que a resposta do governo brasileiro no enfrentamento da crise migratória venezuelana é um exemplo prático desse acompanhamento.

O mundo tem acompanhado, com preocupação, a crise social, econômica e política na qual a Venezuela mergulhou. Em virtude dessa crise, milhares de venezuelanos têm migrado para outros países, dentre eles o Brasil, com o intuito de buscar melhores condições de vida. A maioria desses venezuelanos ingressa no território brasileiro pelo município de Pacaraima e se desloca para Boa Vista, capital do estado de Roraima, ou para outras cidades da região amazônica brasileira, as quais não possuem a infraestrutura de serviços públicos e o mercado de trabalho adequados para a absorção

---

* Artigo originalmente publicado no dia 25 julho de 2019 no site do OMPV.

[1] Tenente-Coronel do Exército Brasileiro.

desse contingente populacional. Consequentemente, essas cidades passaram a enfrentar diversos problemas, como o inchaço nos serviços públicos (principalmente na área da saúde), o aumento dos índices de violência, a prostituição, a mendicância e a ocupação desordenada de espaços públicos.

Em 15 de fevereiro de 2018, o governo do Brasil reconheceu a situação de vulnerabilidade decorrente do aumento do fluxo migratório para o Estado de Roraima, provocado pela crise na Venezuela, e criou um Comitê Federal de Assistência Emergencial. O Ministério da Defesa assumiu a secretaria-executiva desse comitê e um General de Divisão do Exército Brasileiro foi nomeado coordenador operacional das ações de assistência emergencial.

Como resultado, foi desencadeada a Operação Acolhida, na qual tropas das Forças Armadas do Brasil, em coordenação com a Organização das Nações Unidas (ONU), com órgãos de segurança pública, com agências governamentais, com organizações não governamentais e com entidades religiosas e filantrópicas, têm realizado ações de cunho humanitário, acolhendo os venezuelanos que ingressam no território brasileiro, fugindo da crise da república bolivariana. Essa operação possui como pilares básicos o ordenamento da fronteira, o abrigamento e a interiorização.

Não se sabe ao certo quanto tempo a Operação Acolhida durará, haja vista que não se vislumbra uma solução a curto ou a médio prazo para a crise venezuelana. Mesmo que ocorram reformas na Venezuela, sob as perspectivas econômica, política e social, a recuperação integral desse país não se dará da noite para o dia. Dessa forma, é lícito supor que os venezuelanos continuarão deixando sua terra natal nos próximos anos. Muito se fala e se escreve sobre as atuais condições da fronteira BRASIL-VENEZUELA.

Mas, como era a dinâmica dessa fronteira antes da crise, principalmente na região de Pacaraima?

A verdade é que essa pequena cidade, com cerca de 12.000 habitantes, sempre funcionou como entreposto comercial, atraindo venezuelanos em busca de bens de consumo básico e de atendimento médico. Além disso, muitos venezuelanos, de forma costumeira, matriculam seus filhos nas escolas públicas de Pacaraima, que oferecem um ensino de melhor qualidade que as escolas venezuelanas próximas da fronteira. Em relação aos brasileiros, havia um movimento bastante peculiar de compras nas lojas venezuelanas de *Santa Elena do Uairén*, as quais, antes da crise, vendiam produtos de

limpeza, roupas e perfumes com preços mais baixos do que os praticados no Brasil. Além disso, venezuelanos cruzavam a fronteira diariamente para trabalhar no Brasil e vice-versa. Em linhas gerais, o que se observava era um efetivo fluxo de fronteiriços ingressando em ambos os países para ter acesso a bens, serviços e oportunidades que fossem mais bem ofertados em um ou em outro local.

Com a crise, os brasileiros deixaram de comprar em *Santa Elena do Uairén*, haja vista que ela, assim como as demais cidades venezuelanas, ficou desabastecida. No entanto, a coluna vertebral do trânsito de fronteiriços se manteve e se mantém: os venezuelanos compram comida e outros bens em Pacaraima, utilizam o sistema público de saúde dessa cidade e suas crianças continuam estudando nas escolas brasileiras mais próximas. No tocante ao trabalho, brasileiros e venezuelanos continuam cruzando a fronteira, todos os dias, para trabalhar no país vizinho.

A partir dessa fotografia, não é difícil imaginar que o fechamento dessa fronteira possa causar (e efetivamente causa) problemas para a população de ambos os países, principalmente para os fronteiriços, que circulam em Pacaraima e *Santa Elena* todos os dias.

Em 5 de agosto de 2018, em decisão liminar, o juiz federal Helder Girão Barreto, da 1ª Vara da Federal, determinou a suspensão do ingresso e a admissão de imigrantes venezuelanos no Brasil, pelo estado de Roraima. Após serem notificadas, no dia 6 de agosto, por volta das 17 horas, a Polícia Federal e a Força Nacional posicionaram algumas viaturas nas proximidades do marco BV-8, na BR-174, e passaram a impedir a entrada de venezuelanos no Brasil:

Figura 1 - Polícia Federal e Força Nacional fecham a fronteira BRASIL-VENEZUELA

Fonte: OLIVEIRA, 2018.

No tocante ao ponto de vista do fluxo migratório, não se observou grandes mudanças, principalmente por dois aspectos: o primeiro é que a Venezuela fecha seu próprio posto de controle de fronteira, todos os dias, por volta das 18 horas, interrompendo o fluxo de venezuelanos em direção ao Brasil; e o segundo aspecto é que a liminar que suspendia o ingresso de venezuelanos foi indeferida pela Ministra Rosa Weber, do Supremo Tribunal Federal, no mesmo dia do fechamento.

No entanto, mesmo esse pequeno lapso temporal gerou transtornos para a população local. O horário do fechamento - por volta das 17 horas - coincidia com a saída das crianças venezuelanas que estudavam em Pacaraima. Pais e mães, que moravam em *Santa Elena* e que tinham o costume de buscar os filhos em Pacaraima, foram impedidos de passar, o que gerou certo desconforto na região do BV-8.

Entre 21 de fevereiro e 10 de maio de 2019, por determinação de *Nicolas Maduro*, a Guarda Nacional Bolivariana manteve a fronteira BRASIL-VENEZUELA fechada. O objetivo alegado foi o de barrar a ajuda humanitária oferecida pelos Estados Unidos da América e por países vizinhos, incluindo o Brasil, após pedido do autoproclamado presidente interino *Juan Guaidó*. Após o anúncio do fechamento, venezuelanos correram para Pacaraima, para comprar comida e outros itens básicos.

Ao longo do período no qual a fronteira foi mantida fechada, os venezuelanos utilizaram trilhas que davam acesso à Pacaraima, seja para migrar para o Brasil, seja para comprar comida. Além disso, esse movimento era seguido pelas crianças venezuelanas, que frequentam as escolas de Pacaraima, e até mesmo por moradores de *Santa Elena* que trabalham no Brasil.

Figura 2 - Após fechamento da fronteira, venezuelanos usam rotas alternativas para entrar no Brasil

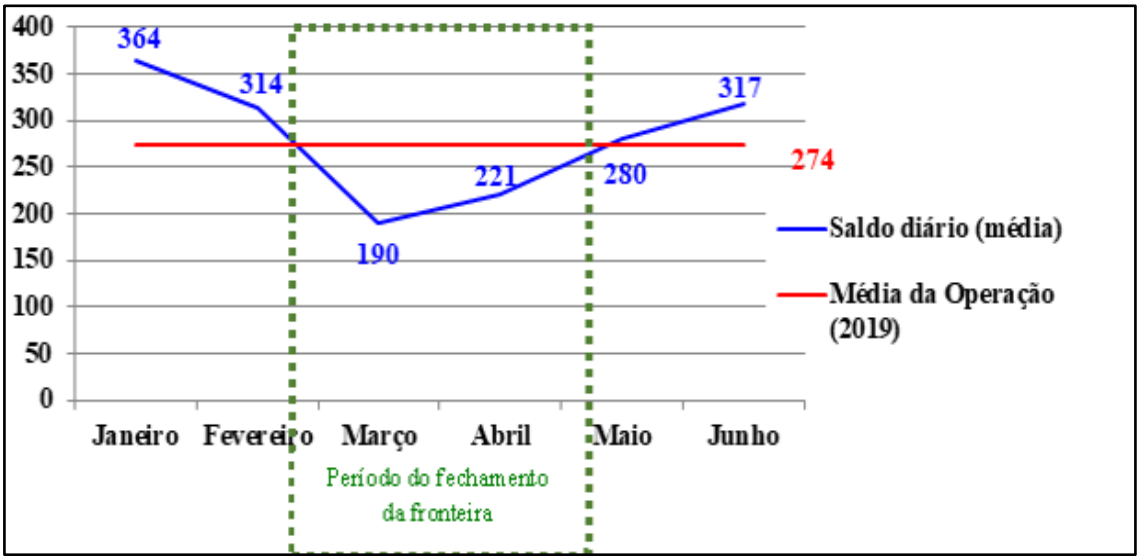
Fonte: SCHUCH, 2019.

Outra forma reportada para alcançar o Brasil, mesmo com a proibição venezuelana, era o pagamento de suborno aos militares venezuelanos. Rafael Levy, chefe do escritório da ONU em Pacaraima, afirmou:

> "O que mudou com o fechamento da fronteira é que as pessoas têm de se submeter a riscos muito maiores. Todos passam por vias não oficiais para chegar ao Brasil. O fato de terem de pagar algum tipo de suborno aumenta o nível de precariedade em que eles chegam. Muitas vezes têm de deixar todo o dinheiro que têm com os guardas" (ARAÚJO, 2019, p. 1).

Observa-se, assim, que os próprios venezuelanos encontraram formas de superar essa proibição do governo da Venezuela. Isso fica visível ao se verificar as estatísticas de passagem de venezuelanos pelo Posto de Bloqueio e Controle de Estradas (PBCE)[2], mobiliado por tropas do Exército Brasileiro, em Pacaraima. Verificando o gráfico abaixo, no qual constam os saldos diários de venezuelanos que passaram pelo PBCE de Pacaraima, em direção à cidade de Boa Vista, percebe-se uma queda no quantitativo, principalmente nos meses de março (190 venezuelanos por dia) e abril (221 venezuelanos por dia), mas não a interrupção do fluxo migratório. Em maio e junho, os números subiram, o que é um fato natural, dada a reabertura da fronteira.

Gráfico 1 - Saldo diário de venezuelanos contabilizados no PBCE de Pacaraima



Fonte: O AUTROR, 2019.

O futuro da Venezuela é incerto. Se é certo que a crise tem se aprofundado cada vez mais nesse país vizinho, é certo também que o Governo do Brasil continuará acompanhando a evolução dos acontecimentos na fronteira Norte e apoiando os venezuelanos que ingressam no território brasileiro, em busca de melhores condições de

[2] Os militares presentes nesse posto checam a documentação de todos os venezuelanos que por lá passam, além de realizar a contagem desses estrangeiros.

vida. No mais, o que se espera é que a Venezuela empreenda, o mais rápido possível, as reformas necessárias, para que possa voltar a crescer e reencontrar o seu caminho.

Referências:

ARAÚJO, Pedro**. Fechamento da fronteira do Brasil com a Venezuela não reduziu migração.** PE Notícias, 2019. Disponível em: http://penoticias.com.br/blog/fechamento-da-fronteira-do-brasil-com-a-venezuela-nao-reduziu-migracao/. Acesso em: 15 de maio de 2019.

OLIVEIRA, Valéria. **Fronteira do Brasil com a Venezuela é fechada após decisão judicial, diz PRF.** G1, 2018. Disponível em: https://g1.globo.com/rr/roraima/noticia/2018/08/06/fronteira-do-brasil-com-a-venezuela-e-fechada-apos-decisao-judicial-diz-prf.g html. Acesso em: 15 de março de 2019.

SCHUCH, Matheus. **Com fronteira fechada, venezuelanos usam desvios para entrar no Brasil.** GZH Mundo, 2019. Disponível em: https://gauchazh.clicrbs.com.br/mundo/noticia/2019/02/com-fronteira-fechada-venezuelanos-usam-desvios-para-entrar-no-brasil-cjsg2ps5e009d01p8cz85jh0n.html. Acesso em: 15 de março de 2019.

TERRORISMO

TERRORISMO INTERNACIONAL - TENDÊNCIAS E PERSPECTIVAS*

***André César Guttoski Lemos*[1]**

1. Introdução

O terrorismo é um fenômeno social complexo que encontra diversidade de definições em todo o mundo. O Departamento de Defesa dos Estados Unidos da América define este fenômeno como violência premeditada e politicamente motivada contra não-combatentes, perpetrada por grupos subnacionais ou clandestinos, geralmente para influenciar um público (EUA, 2006). Outra definição que podemos encontrar é a de *Walter Laqueur*, que o trata como a contribuição para o ilegítimo uso da força, de modo a conseguir um objetivo político, quando pessoas inocentes são os alvos (WHITTAKER, 2005).

O terrorismo de caráter internacional tem sua tipificação por meio de seus incidentes, cujas consequências e ramificações transcendem nitidamente as fronteiras nacionais, ou seja, quando vítimas, executantes e o local de um atentado, ou ainda os meios utilizados envolvem mais de um país ou nacionalidade (WOLOSZYN, 2010).

Atualmente, o Departamento de Estado dos Estados Unidos da América reconhece 68 organizações terroristas de caráter internacional, adotando três critérios legais para tal:

a. Deve ser uma organização internacional;

b. A Organização deve engajar-se em atividade terrorista definida conforme seus regramentos ou deter a capacidade e intenção de engajar-se em atividade terrorista; e

c. A atividade terrorista da organização deve ameaçar a segurança dos nacionais norte-americanos ou a segurança nacional dos Estados Unidos da América (defesa nacional, relações internacionais ou interesses econômicos).

O Estado Islâmico do Iraque e da Síria (ISIS) é um grupo *jihadista* sunita, que propõe a criação do califado para impor autoridade religiosa sobre todos os muçulmanos (RAND, 2019). Este grupo foi fundado em 1999, teve participação na insurgência iraquiana que fez frente a invasão de 2003 e, em 2014, ganhou

---

* Artigo originalmente publicado no dia 05 de novembro de 2019 no site do OMPV.

[1] Major do Exército Brasileiro.

proeminência mundial devido à sua expansão territorial na Síria e no Iraque. Esta organização, também denominada *Daesh*, é integrada por uma diversidade de atores não-estatais, fazendo o uso sistemático da violência, principalmente pelo uso do ato terrorista e pela ação de milícia armada. Sua atuação é apoiada por mecanismos próprios de divulgação, assumindo para todo o Sistema Internacional sua matriz salafista-jihadista (MATOS, 2019).

O ISIS tem forte influência na *Al-Qaeda*, com uma estrutura híbrida e flexível, com sua atuação concebida em forte descentralização, celular e difusa. Assim sendo, essa organização concede ao grupo uma vantagem a se contrapor à monitoração, permitindo a replicação de grupos em caráter regional ou local, em todo o mundo (MATOS, 2019).

Esse "efeito espelho" entre a *Al-Qaeda* e o *Daesh* pode ser visto, também, nos seus objetivos estratégicos a médio e longo prazo. O plano gizado para unir num califado global já era preconizado pela *Al-Qaeda*, no tempo de *Bin Laden*. O "Plano Mestre" da *Al-Qaeda* contemplava já os sete estádios rumo à "Vitória Final" (MATOS, 2019).

O Estado Islâmico foi conhecido pela ação de conquista de territórios na região da Síria e do Iraque, entretanto, é pela perpetração de atos terroristas em diversos lugares no mundo, que deram notoriedade ao grupo. Feito este preâmbulo, este artigo tem por objetivo apresentar algumas tendências do terrorismo internacional, tomando-se como referência o recente artigo de *Erin Miller*, publicado pelo START (*National Consortium for the Study of Terrorism and Responses to Terrorism*).

2. Desenvolvimento

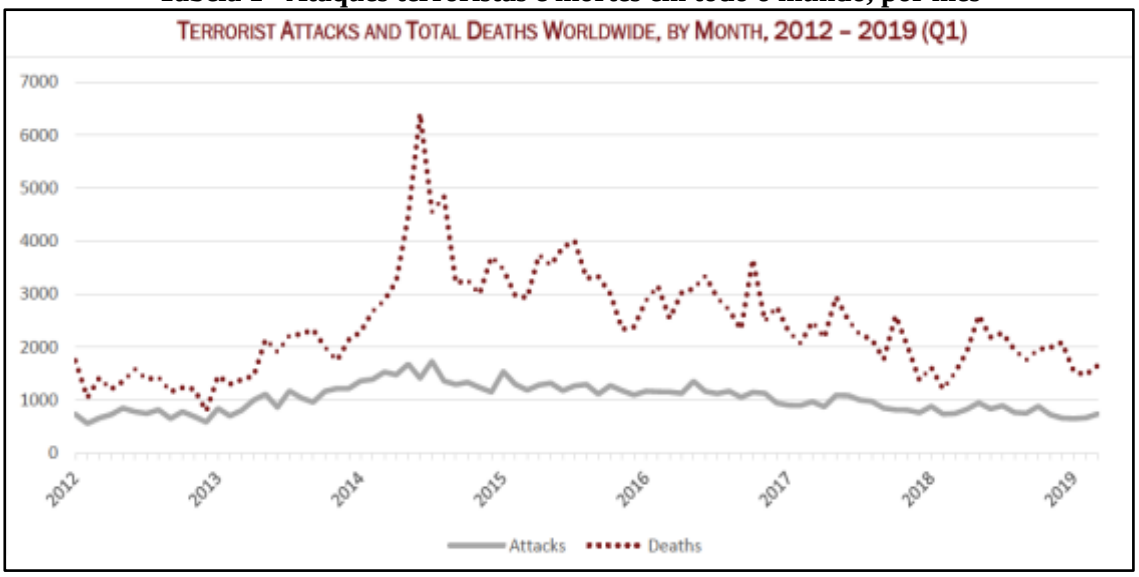
O ano de 2018 contabilizou-se mais de 9.600 ataques terroristas em todo o mundo, que causaram mais de 22.980 mortes (7.290 terroristas e 15.690 vítimas). Estes números, quando comparados à 2014 (aproximadamente 17.000 ataques com mais de 45.000 mortes) representa uma redução de 43% do número de ataques e uma redução de 48% do número de mortes (MILLER, 2019).

Percebe-se a importância do Iraque quanto ao fenômeno do terrorismo no mundo. Assim, a redução percentual de ataques e mortes neste país, entre os anos de 2017 e 2018, contribuíram para com as reduções destes aspectos mundialmente. Na Europa ocidental, as estatísticas também vão ao encontro da tendência de redução dos números de ataques terroristas e suas mortes. Entre 2017 e 2018, a redução de ataques foi da

ordem de 31%, enquanto o número de mortes reduziu 70%.

O fato apontado pelo relatório é o declínio do Estado Islâmico no Iraque que se contrasta com a sua capacidade de aumento de influência no mundo. Nos Estados Unidos da América, entre 2017 e 2018, o número de ataques terroristas mantiveram-se estáveis, entretanto observam-se a redução em 54% do número de mortes. Extraída no *Global Terrorism Database* em in 2018, observa-se na tabela 01 o ano de 2014, representando o ápice do número de mortes causadas por atentados terroristas, fato este interligado à ascensão da organização Estado Islâmico. Pode-se também comprovar a tendência de diminuição do número de ataques e mortes relacionados ao fenômeno terrorista.

Tabela 1 - Ataques terroristas e mortes em todo o mundo, por mês



Fonte: Global Terrorism Database, 2019.

Com relação ao aspecto geográfico da incidência do terrorismo, o artigo aponta os cinco países que concentram mais do que a metade de todos os ataques (Afeganistão - 18%; Iraque - 14%; Índia - 9%; Nigéria -7 % e Filipinas - 6%). Além disto, observa-se que mais da metade de todas as mortes estão concentradas em dois países, o Afeganistão, com 43%, e a Nigéria, com 11%.

Tabela 2 - Países com mais de 150 ataques terroristas em 2018

TERRORIST ATTACKS AND TOTAL DEATHS, COUNTRIES WITH MORE THAN 150 ATTACKS, 2018

Country	Total Attacks	% of Total	% Change from 2017	Total Killed*	% of Total	% Change from 2017
Afghanistan	1776	18%	26%	9812	43%	61%
Iraq	1362	14%	-46%	1432	6%	-78%
India	888	9%	-8%	412	2%	-11%
Nigeria	645	7%	33%	2574	11%	43%
Philippines	601	6%	-13%	440	2%	-11%
Somalia	527	5%	-14%	1144	5%	-40%
Pakistan	480	5%	-33%	697	3%	-35%
Yemen	325	3%	43%	829	4%	9%
Cameroon	235	2%	114%	296	1%	21%
Syria	232	2%	-6%	1547	7%	-24%
Colombia	205	2%	72%	132	1%	57%
Thailand	182	2%	2%	69	0%	-4%
Libya	166	2%	-13%	244	1%	-16%
Mali	164	2%	15%	584	3%	61%
Democratic Republic of the Congo	163	2%	14%	993	4%	67%
Worldwide Total	**9607**	**100%**	**-13%**	**22987**	**100%**	**-13%**

*Includes perpetrator deaths

Fonte: MILLER, 2019.

Ainda, entre 2017 e 2018 podem ser destacados os países com maiores reduções na violência de cunho terrorista:

- Egito: redução em 76% de ataques (54 em 2018) e 89% em mortes (98 em 2018);

- Nepal: redução em 60% de ataques (99 em 2018) e 100% em mortes (nenhuma em 2018); e

- Iraque: redução em 46% de ataques (1.362 em 2018) e 78% em mortes (1.432 em 2018).

Ao passo que, neste mesmo período, são elencados como países com maiores aumentos de taxas relacionadas ao terrorismo:

- Camarões: aumento em 114% de ataques (235 em 2018) e 21% em mortes (296 em 2018);

- Colômbia: aumento em 72% de ataques (205 em 2018) e 57% em mortes (132 em 2018); e

- Arábia Saudita: aumento em 70% de ataques (92 em 2018) embora a redução em 45% de mortes (17 em 2018).

Ao abordarmos as informações de atores perpetradores de ataques terroristas, o artigo mostra que de 2017 para 2018 houve um decréscimo do número de ataques executados por perpetradores não afiliados a organizações terroristas (redução de ataques de 102, em 2017, para 90, em 2018).

Ao mesmo tempo, em 2018 houve uma queda do número de organizações terroristas que executaram ataques em todo o mundo (372, em 2017, para 320, em

2018). A tabela 3 -Grupos responsáveis por mais de 100 ataques, aponta as 12 maiores organizações terroristas no mundo.

Tabela 3 - Grupos responsáveis por mais de 100 ataques

Perpetrator Group	Total Attacks	Change from 2017	Total Killed*	Change from 2017
Taliban	1266	40%	8508	73%
Islamic State of Iraq and the Levant (ISIL)	735	-45%	2221	-69%
Al-Shabaab	493	-14%	1149	-39%
Fulani extremists	304	285%	1188	245%
New People's Army (NPA)	283	-22%	188	-6%
Maoists/ Communist Party of India - Maoist (CPI-Maoist)	268	-15%	189	-15%
Houthi extremists (Ansar Allah)	267	68%	659	48%
Boko Haram	243	-29%	1327	-16%
Islamic State- Khorasan Province	155	-21%	1203	-8%
Kurdistan Workers' Party (PKK)	122	-23%	136	-28%
National Liberation Army of Colombia (ELN)	121	95%	106	126%
Separatists (Cameroon)	112	1767%	150	1150%

*Includes perpetrator deaths

Fonte: MILLER, 2019.

Por fim, o relatório aponta os principais alvos dos atentados terroristas, em todo o mundo, nos anos de 2017 e 2018. A tabela 4 - alvos de ataques terroristas no mundo, 2017-2018, apresenta como principal alvo os cidadãos e as propriedades privadas, seguidos da polícia, do governo, negócios, forças armadas e figuras/instituições religiosas.

Tabela 4 - alvos de ataques terroristas no mundo, 2017-2018

Target Type	Number of Targets 2018	2017
Private Citizens & Property	3147	3552
Police	1623	1604
Government (General)	977	932
Business	604	803
Military	385	456
Religious Figures/Institutions	251	231
Educational Institution	185	171
Terrorists/Non-State Militia	153	161
Transportation	140	151
Utilities	140	159
Journalists & Media	105	131
Government (Diplomatic)	89	96
Violent Political Party	83	149
NGO	47	56
Telecommunication	40	33
Airports & Aircraft	21	12
Maritime	21	15
Food or Water Supply	14	11
Other	14	7
Tourists	13	18
Abortion Related	1	1
Total	8053	8749

Fonte: MILLER, 2019.

3. Conclusão

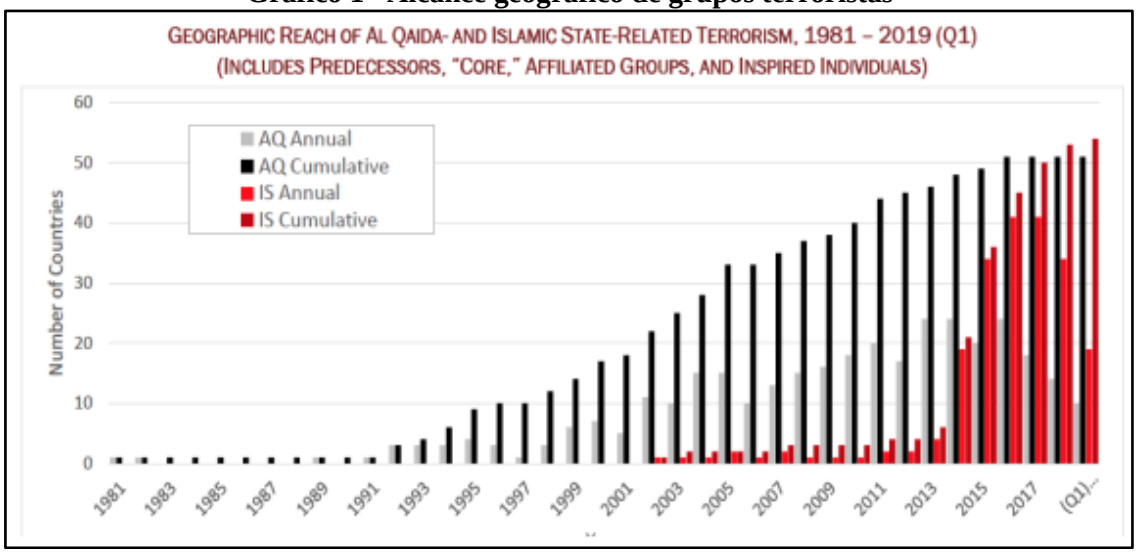
O terrorismo internacional é um importante fenômeno que impacta as relações internacionais e a política externa dos Estados, principalmente quando da formulação de

suas políticas de defesa.

Ademais, a política de combate ao terrorismo norte-americana, denominada ***Guerra ao Terror***, não pode ser apontada como ineficiente, visto seus resultados, principalmente no campo militar, quando do combate ao *Al-Qaeda* e, mais recentemente, ao Estado Islâmico.

Pesquisadores do *Global Terrorism Database*, mostraram que a rápida expansão do Estado Islâmico está ligada quando de sua associação ao *Al-Qaeda*, bem observado a partir de 2014. Ainda, eles apresentam a tendência de progressivo aumento de países impactados por atentados terroristas do Estado Islâmico (Gráfico 1), mesmo observando sua derrota no campo militar, empreendida pela Guerra ao Terror, nos territórios da Síria e do Iraque.

Gráfico 1 - Alcance geográfico de grupos terroristas



Fonte: MILLER, 2019.

O recente anúncio da morte do líder da organização Estado Islâmico, *Abu Bakr al-Baghdadi*, em operação com tropas de operações especiais dos Estados Unidos da América, no noroeste da Síria, retrata bem o sucesso desta política, no campo militar (BBC, 2019). O futuro dirá o quanto será desarticulada de comando e controle desta organização e ainda, se esta ação possibilitará novas operações, fruto da reunião de dados obtidos no local onde se encontrava o líder do Estado Islâmico, entretanto é um fato que a motivação ideológica da *jihad* não será obstaculizada por este tipo de medida.

Conforme apresentado em relatório de 2019, o número de Estados que sofreram ataques terroristas foi de 56 países. A tendência de aumento progressivo da expansão de ataques, em novos países, apresenta um desafio com o qual a política de combate ao terrorismo ainda não soube lidar.

4. Referências:

BBC. **Quem era Abu Bakr al-Baghdadi, líder do Estado Islâmico morto por forças americanas.** BBC, 2019. Disponível em: https://www.bbc.com/portuguese/internacional-50200967. Acesso em: 28 de outubro de 2019.

EUA. **22 U.S.C. 2656f - Annual country reports on terrorism.** Legal Information Institute, 2019. Disponível em: https://www.law.cornell.edu/uscode/text/22/2656f. Acesso em: 26 de outubro de 2019.

MATOS, Hermínio Joaquim de. **Requiem para o "Estado Islâmico"? Jihadismo na Europa - Infiltração, dissimulação e engano no planejamento de ataques terroristas.** In FAGUNDES, Carlos Frederico Felício; LASMAR, Jorge Mascarenhas; CHUY, José Fernando Moraes. Perspectivas do Terrorismo Transacional Contemporâneo, Cap. 2, p. 37-65, 2019. Belo Horizonte: Arraes, 2019.

MILLER, Erin. **Global Terrorism in 2018.** Maryland: Universidade de Maryland, 2019. Disponível em: https://www.start.umd.edu/sites/default/files/publications/local_attachments/START_GTD_TerrorismIn2018_Oct2018.pdf. Acesso em 10 de outubro de 2019.

RAND CORPORATION. **The Islamic State (Terrorist Organization).** Disponível em: https://www.rand.org/topics/the-islamic-state-terrorist-organization.html?page=14. Acesso em: 26 de outubro de 2019.

WHITTAKER, David J. **Terrorismo - um retrato.** Rio de Janeiro: Biblioteca do Exército, 2005.

WOLOSZYN, André Luís. T**errorismo global: aspectos gerais e criminais.** Rio de Janeiro: Biblioteca do Exército, 2010.

ISBN: 978-85-64844-10-0
CDD
9 788564 844100