POLICY PAPERS

>ONLINE
Forte de
Copacabana
2021

AUSÊNCIA DE GUERRAS SIGNIFICA PAZ?

Estratégias de Segurança Internacional em uma Nova Ordem Geopolítica Mundial

DOES NO WAR MEAN PEACE?

International Security Strategies in a New Geopolitical World Order

XVIIIFORTE

KONRAD ADENAUER STIFTUNG

CEBRI
BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS

XVIIIFORTE

AUSÊNCIA DE GUERRAS SIGNIFICA PAZ?

Estratégias de Segurança Internacional
em uma Nova Ordem Geopolítica Mundial

DOES NO WAR MEAN PEACE?

International Security Strategies in
a New Geopolitical World Order

POLICY PAPERS

Rio de Janeiro, 2021

Editor Editor
Anja Czymmeck

Coordenação editorial Project Coordination
Aline Soares
Reinaldo Themoteo

Banca avaliadora dos Policy Papers Policy Papers Evaluation Board
Coordenação *Coordination* **Monique Sochaczewski Goldfeld**
Kai Michael Kenkel e Eduardo Uziel

Tradução e revisão Translation and Revision
Christiano Sanches do Valle Silva, Clarisse Campelo, Franzi Becskehazy, Mônica Freitas de Hollanda Cavalcanti, Natalia Taddei, Rafael Reif de Paula, Verônica Pires

Revisão *Revision* **Heloisa Gonçalves Barbosa**

Coordenação *Coordination*
Jutta Gruetzmacher – Wordstation Traduções

Projeto Gráfico Design
Daniela Knorr

Fotografias Photos

Capa *Cover* **metamorworks/iStock.com**
Página *Page* 6 **Bildarchiv der Konrad-Adenauer-Stiftung**
Página Page 10 **CEBRI**
Página Page 16 **Erich Westendarp/Pixabay.com**

Impressão Print
Gráfica Cruzado

ISSN 2176-297X

"Ausência de Guerras Significa Paz? Estratégias de Segurança Internacional em uma Nova Ordem Geopolítica Mundial"

"Does No War Mean Peace? International Security Strategies in a New Geopolitical World Order"

Rio de Janeiro: Konrad-Adenauer-Stiftung, 2021.

www.kas.de/brasil

Fundação Konrad Adenauer
Rua Guilhermina Guinle, 163
Botafogo CEP: 22270-060
Rio de Janeiro, RJ – Brasil
Tel: (+55/21) 2220-5441
Fax: (+55/21) 2220-5448

www.kas.de/brasil
kas.brasil
kasbrasil

ISSN 2176-297X

SUMÁRIO SUMMARY

SUMÁRIO SUMMARY

KONRAD ADENAUER STIFTUNG

A Conferência de Segurança Internacional do Forte de Copacabana é promovida anualmente pela Fundação Konrad Adenauer no Brasil em parceria com o Centro Brasileiro de Relações Internacionais (CEBRI) e a Delegação da União Europeia no Brasil. Desde sua primeira edição, em 2003, o principal objetivo da Conferência do Forte é reunir especialistas dos setores governamental, acadêmico, privado e das forças armadas para discutir assuntos atuais no âmbito da segurança internacional que sejam de interesse comum aos parceiros dos dois lados do Atlântico. O que era um encontro relativamente pequeno entre políticos, especialistas e militares no Forte de Copacabana, na cidade do Rio de Janeiro, tornou-se a maior conferência de segurança internacional da América Latina!

Ao longo dos anos, o evento contou com o engajamento e as participações especiais de convidados e palestrantes renomados. As contribuições de vários ministros de defesa, membros das forças armadas, corpo diplomático, parlamentares, pesquisadores, empresários da área de segurança internacional e acadêmicos de inúmeras regiões, ao compartilharem seu conhecimento e experiência em ambiente acolhedor e propício para trocas e debates, comprovam o verdadeiro sucesso do evento. Certamente todos os convidados se mostraram animados em influenciar positivamente a agenda política do Brasil, dos demais países latino-americanos e da União Europeia.

Em 2021, o tema da Conferência de Segurança Internacional do Forte de Copacabana é "Ausência de guerras

The Forte de Copacabana International Security Conference is organised every year by the Konrad Adenauer Foundation in Brazil, in partnership with the Brazilian Centre for International Relations (CEBRI) and the Delegation of the European Union to Brazil. Since its first edition, in 2003, the main goal of the Forte de Copacabana Conference has been to gather experts from the government and private sectors, the academic community and the armed forces, to discuss current trends on international security of common interest to partners from both sides of the Atlantic. What started as a relatively small meeting of politicians, experts and the military at the Forte de Copacabana, in the city of Rio de Janeiro, has become the largest international security conference in Latin America!

Through the years, renowned guests and speakers have participated in the Forte de Copacabana Conference. The contributions of many ministers of Defence, members of the armed forces, congressmen, diplomats, researchers, international security entrepreneurs and academia from various regions vouch for the true success of the event. Participants share their knowledge and experience in a welcoming environment that fosters debate and the exchange of information and opinions. All guests have certainly felt moved to positively influence the political agenda of Brazil, of the other Latin American countries, and of the European Union.

In 2021, the theme of the 18th edition of the Forte de Copacabana International Security Conference is "Does no war

“O bom político precisa não somente saber muito, pensar de uma maneira realista e refletir, mas precisa também ter a coragem de fazer aquilo que ele considera correto.”

“*A good politician not only needs to know a lot, but he must be able to think realistically and to reflect, and most importantly, have the courage to do what he thinks is right.*”

KONRAD ADENAUER, 1965

significa paz?". Em sua 18°edição, o evento será realizado em formato virtual para proteger todos os envolvidos — convidados, audiência e organizadores. A virtualidade permitirá que este fórum ganhe uma proporção sem fronteiras, como comprovado na edição de 2020, quando tivemos um público originário de 45 países. Entre as novidades que apresentaremos este ano, além da oferta de tradução simultânea para variados idiomas, contaremos com intérprete da Língua Brasileira de Sinais (Libras), para uma atividade mais inclusiva, e ofereceremos maior interatividade com o público, através das redes sociais, a fim de tornar este momento uma oportunidade de fazer chegar esta discussão sobre segurança internacional a pessoas de variados perfis e oriundas de inúmeras regiões do globo.

Acompanhando a trajetória bem-sucedida da Conferência de Segurança Internacional do Forte de Copacabana está a publicação *Policy Papers - International Security Conference* que, além de ser bilíngue, é constituída por especialistas ou practioners da área de segurança internacional. Os *Policy Papers* visam identificar desafios e apresentar recomendações políticas para o futuro. Nesta publicação, temos um total de 14 artigos que abordam alguns dos principais tópicos relacionados à temática das estratégias de segurança internacional no âmbito da nova ordem geopolítica mundial. São discutidos temas como a proteção de infraestruturas críticas e o papel do setor privado na cooperação civil-militar, ameaças transnacionais e a promoção da cooperação civil-militar e seu papel na construção da paz, a gestão de incidentes cibernéticos e oportunidades para o Brasil e a União Europeia, a forma como os domínios espacial e cibernético interagem e as implicações para o Poder Aeroespacial brasileiro e também a segurança energética através de uma Transição Inclusiva considerada enquanto dimensão crucial em qualquer Estratégia de Segurança Internacional, entre diversos outros assuntos fundamentais no contexto da temática central.

mean peace?". In order to protect all participants — guests, the audience and organisers, this will be a virtual edition. The virtual environment will allow the Forte de Copacabana Conference to have unprecedented reach, beyond physical borders. In the 2020 edition, attendees from 45 different countries joined the Conference. Among the new elements introduced this year, in addition to simultaneous translation into different languages, we will provide interpreting into Brazilian Sign Language (Libras) to promote greater inclusion. We will also offer greater interactivity with the audience via social networks in order to make the best of this opportunity to convey the discussion on international security to people of various backgrounds and from many regions around the globe.

The publication of the book *Policy Papers - International Security Conference* follows the successful trajectory of the Forte de Copacabana International Security Conference. It is a bilingual edition, with contributions from experts or practitioners in the field of international security. The *Policy Papers* aim at identifying challenges and presenting policy recommendations for the future. This edition includes 14 papers addressing some of the main topics related to international security strategies in the new geopolitical world order. Topics discussed include the protection of critical infrastructure and the role of the private sector in civil-military cooperation, transnational threats, and the promotion of civil-military cooperation and its role in building peace, the management of cyber incidents and opportunities for Brazil and the European Union, the way spatial and cyber domains interact and the implications for the Brazilian Aerospace Power, and energy security via an Inclusive Transition considered as a crucial dimension for any International Security Strategy, among many other relevant topics related to the main theme.

Like in the Forte de Copacabana Conference, matters addressed in the *Policy Papers* are highly relevant in practical

terms, and are also an instrument for the maintenance of democracy. Since the sanitary emergency caused by Covid-19 and its countless economic implications and impacts, the global scenario has been one of great severity. The need for urgent action to be taken has been magnified by political and sociological issues that we expected to have been left in the past, such as populism and exacerbated nationalism, in addition to anti-vaccine, -science and -human rights movements. They have risen in various locations around the world and, although they seem to have lost momentum to some extent, they are far from being harmless elements in the new geopolitical world order scenario. These elements reinforce the importance of strengthening and protecting democratic institutions and practices. The dialogue that takes place at the various instances of multilateral fora is an essential part of this protection mechanism.

In 2021, in particular, with a view to presenting new analysts and fostering the network of specialists in the area of international security, we made a public call for unpublished papers to be selected by a highly qualified expert panel for publication in the book.The panel was chaired by Monique Sochaczewski, PhD in History, Politics and Cultural Assets from CPDOC/Fundação Getúlio Vargas, collaborating professor at the Politics and Maritime Strategies Course at the Brazilian Naval War College, and IDP's professor for the Masters programme in Law, Justice and Citizenship. Another renowned member of the panel was Dr. Kai Michael Kenkel, professor and coordinator of the Democracy and Armed Forces Nucleus at PUC-Rio, associate researcher at the German Institute of Global and Area Studies in Hamburg, working in the field of international security, focusing on intervention and peace operations issues. The final member of the panel was Eduardo Uziel, a diplomat since 2000, approved in the High Studies Course at the Rio Branco Institute in 2009, PhD candidate at the Université libre de Bruxelles, researching themes related to the United Nations, peace maintenance operations, the Security Council and the history of Brazilian foreign affairs. The Forte de Copacabana Conference organizing institutions thank the panel members for their remarkable dedication, which contributed to the excellence of the Policy Papers 2021 book.

We hope the *Policy Papers 2021* texts are an enjoyable read that contribute to your understanding of international security. Good reading!

Assim como na Conferência do Forte, as discussões promovidas pela publicação *Policy Papers* apresentam grande relevância não só em termos práticos, mas também como instrumento de manutenção da democracia. Desde a emergência sanitária da Covid-19 e as inúmeras implicações econômicas trazidas diretamente pela pandemia, temos atravessado um cenário global de especial gravidade. Ações urgentes precisaram ser tomadas, agravadas pelas questões políticas e de cunho sociológico que esperávamos pertencer ao passado, como o populismo e o nacionalismo exacerbado, além de movimentos contrários às vacinas, à ciência e aos direitos humanos. Ambos têm se manifestado em diversas partes do globo e, embora pareçam ter perdido força em certa medida, estão longe de serem componentes inofensivos do cenário da nova ordem geopolítica mundial. Tais elementos servem para ressaltar o quão importante é fortalecer e zelar pelas instituições e práticas democráticas. Parte essencial deste mecanismo de proteção é o diálogo presente nos fóruns multilaterais em suas diversificadas instâncias.

Especialmente em 2021, com vistas a apresentar novos nomes de analistas e fomentar a rede de especialistas na área de segurança internacional, foi realizada uma chamada pública de artigos inéditos para compor o livro, selecionados por uma banca altamente qualificada. A banca de seleção foi presidida pela Doutora em História, Política e Bens Culturais pelo CPDOC/Fundação Getúlio Vargas, Monique Sochaczewski, que também é professora colaboradora do Curso de Política e Estratégias Marítimas da Escola de Guerra Naval e professora permanente do Mestrado em Direito, Justiça e Cidadania do IDP. Outro membro ilustre da banca é professor e coordenador do Núcleo Democracia e Forças Armadas da PUC-Rio, Doutor Kai Michael Kenkel, que também é pesquisador associado do German Institute of Global and Area Studies em Hamburgo e atua na área da segurança internacional, com ênfase em questões de intervenção e operações de paz. Completa a equipe o diplomata de carreira desde 2000, aprovado no Curso de Altos Estudos do Instituto Rio Branco em 2009, Eduardo Uziel, que também é doutorando pela Universidade Livre de Bruxelas e pesquisa temas relacionados às Nações Unidas, operações de manutenção da paz, Conselho de Segurança e história da política externa brasileira. As instituições organizadoras da Conferência do Forte de Copacabana agradecem imensamente a todos os membros da banca por sua dedicação e excepcional colaboração, que enriqueceu a excelência da publicação do Policy Papers 2021.

Esperamos que você aprecie a leitura e amplie sua compreensão sobre segurança internacional com os textos deste *Policy Papers* 2021. Boa leitura!

Fundado em 1998, o Centro Brasileiro de Relações Internacionais (CEBRI) é o 2º think tank mais relevante da América Latina e Caribe, sendo o 1º mais relevante na categoria de defesa e segurança internacional, e o principal think tank brasileiro dedicado exclusivamente às relações internacionais e à política externa brasileira. Independente, apartidário e multidisciplinar, o CEBRI é uma instituição sem fins lucrativos que tem por objetivo engajar os setores público e privado, a academia e a sociedade civil em um debate plural sobre as mais relevantes questões internacionais e temas estratégicos para o Brasil. Através dos seus 12 núcleos temáticos, o CEBRI busca contribuir não apenas com a construção de políticas públicas focadas na agenda internacional do país, mas também com a formulação e disseminação de conteúdo de alta qualidade sobre o cenário internacional, temas globais e o papel do Estado brasileiro.

Conectado a uma ampla rede global de think tanks, instituições, fundações e organizações da sociedade civil ao redor do mundo, o CEBRI tem na cooperação internacional um dos pilares de seus projetos e iniciativas. Neste particular, gostaríamos de destacar a nossa parceria de longa data com a Fundação Konrad Adenauer (KAS) para a organização da Conferência de Segurança Internacional do Forte de Copacabana, que tem por objetivo a promoção do diálogo em temas de segurança internacional e de defesa entre a América do Sul e a Europa, incentivando uma reflexão conjunta diante dos desafios comuns e das oportunidades de cooperação. Desde 2004, o CEBRI e a KAS organizam, com o apoio da Delegação

Founded in 1998, the Brazilian Centre for International Relations (CEBRI) is the 2nd most relevant think tank in the Latin America and Caribbean region, being the most relevant think tank in the defence and international security category, and the leading Brazilian think tank exclusively dedicated to international relations and Brazilian foreign affairs. CEBRI is an independent, non-partisan and multidisciplinary non-profit institution aiming at engaging the public and private sectors, academia and civil society in a plural discussion on the most relevant international issues and strategic themes for Brazil. With 12 regional and thematic programmes, CEBRI aims to contribute to the development of public policies focused on the country's international agenda, and to create and disseminate high-quality material about the international scenario, global themes and the role of the Brazilian State.

CEBRI is connected to a vast global network of think tanks, institutions, foundations and civil society organisations from around the world, and international cooperation is at the core of its projects and initiatives. In this regard, we would like to acknowledge our long-standing partnership with the Konrad Adenauer Foundation (KAS) to organise the Forte de Copacabana International Security Conference. The Conference aims at promoting dialogue on international security and defence themes between South America and Europe, encouraging a joint reflection in the face of common challenges and cooperation opportunities. Since 2004, with support from the Delegation of the European Union to Brazil, CEBRI and KAS

have organised the main international security forum in Latin America, traditionally with the participation of senior government officials, politicians, academia, businessmen, civil society representatives and members of the armed forces of South American and European countries.

CEBRI prioritises the international defence and security agenda, dedicating one of its 12 Programmes exclusively to addressing this topic. The programme's knowledge and content production are coordinated by Senior Fellow Paulo Sérgio Melo de Carvalho, Lieutenant General of the Brazilian Army Reserve, and by Senior Fellow Ronaldo Carmona, a Professor at the Brazilian War College. The coordination between CEBRI's Board of Trustees and the International Defence and Security Programme is conducted by Trustee André Clark, General Manager of Siemens Energy Brasil.

CEBRI's International Defence and Security Programme aims at expanding reflection and critical analysis on the main challenges of international security and national defence, especially after the intensification and diversification of transborder security issues. Themes such as terrorism, drug trafficking, chemical, biological and radiological warfare, and cybersecurity are addressed from a perspective that aims at integrating global collective security and the need to adapt national policies.

Regarding cybersecurity, CEBRI has a Cybersecurity Analysis Group (Cyber Group) working within the International Defence and Security Programme. Aiming at promoting greater awareness of the urgency of a broad public discussion on cybersecurity, and at promoting strategic reflections on indispensable initiatives so that the public and the private sectors, academia and civil society may face, in the safest possible way, the challenges posed by this new digital revolution, the Cyber Group directs its agenda towards the following topics: cybersecurity management for the energy sector, information security and data protection governance, the Brazilian cybersecurity strategy, and cybersecurity during elections.

CEBRI is convinced that the 18th edition of the Forte de Copacabana International Security Conference "Does no war mean peace? *International security strategies in a new geopolitical world order*" is very timely and appropriate. During 2020, the world's population became rapidly aware of the main challenges, vulnerabilities and risks to international security and to the defence of their home States, even in the absence of war or armed conflicts.

In the first place, the last year has made it as clear as never before that there is an urgent need for a global response to the planetary climate and environmental crisis, and that the response must be based on respecting the principle of national sovereignty. Neither the world economy deceleration resulting from lockdown policies for fighting the new Coronavirus pandemic, nor the cooling effect of La Niña were enough to halt rising global temperatures, that reached their highest average in the historical series used to compare temperature changes to pre-industrial levels.

Moreover, two important summits on the environment were postponed to 2021 due to the new Coronavirus pandemic: the Glasgow (United Kingdom) Climate Change Conference and the Kunming Biodiversity Conference (China). The great apprehension of experts regarding the results of these two climate negotiation summits for the future of humanity highlights both the perception of a threat to international security brought about by climate change, and also the decisive role of the year 2021 for the future of the global fight against the planetary climate and environmental crises.

Likewise, the year 2020 represented an inflection point for the way contemporary society relates to information and communication technologies. Pressed by an unexpected health crisis, the immersion of contemporary society in this new era of indispensable coexistence with digital technologies has created countless

da União Europeia no Brasil, o principal fórum sobre segurança internacional da América Latina, que tem a tradição de contar com as contribuições de altos funcionários de governos, políticos, acadêmicos, empresários, representantes da sociedade civil e membros das forças armadas de países sul-americanos e europeus.

A agenda de defesa e segurança internacional e defesa é prioritária para o CEBRI, que tem um dos seus 12 núcleos temáticos voltados exclusivamente para este tópico. A produção de conhecimento e conteúdo das atividades do Núcleo é feita pelo Senior Fellow Paulo Sérgio Melo de Carvalho, General de Divisão da Reserva do Exército Brasileiro, e pelo Senior Fellow Ronaldo Carmona, Professor da Escola Superior de Guerra. A coordenação entre o Conselho Curador do CEBRI e o Núcleo Defesa e Segurança Internacional é conduzida pelo Conselheiro André Clark, General Manager da Siemens Energy no Brasil.

O Núcleo Defesa e Segurança Internacional do CEBRI tem por objetivo ampliar a reflexão e análise crítica sobre os principais desafios da segurança internacional e defesa nacional, sobretudo com o aumento e diversificação das questões securitárias transfronteiriças. Temas como terrorismo, narcotráfico, guerras químicas, biológicas e radiológicas e segurança cibernética são abordados desde uma perspectiva que busca integrar segurança coletiva global e necessidade de adaptação de políticas nacionais.

No que se refere ao tema da segurança cibernética, o CEBRI conta com um Grupo de Análise de Segurança Cibernética (Grupo Cyber) desenvolvido no âmbito do Núcleo Defesa e Segurança Internacional. Com os objetivos de promover uma maior conscientização sobre a urgência de um amplo debate público sobre a temática de segurança cibernética e de gerar uma reflexão estratégica acerca das iniciativas indispensáveis para que os setores público e privado, a academia e a sociedade civil possam enfrentar da forma mais segura possível os desafios criados por essa nova revolução digital, o Grupo Cyber orienta sua agenda de trabalho para os temas de gerenciamento da segurança cibernética no setor energético, governança da segurança da informação e proteção de dados, estratégia brasileira de segurança cibernética e cibersegurança nas eleições.

O CEBRI está convencido de que a XVIII edição da Conferência de Segurança Internacional do Forte de Copacabana "*Ausência de guerras significa paz? Estratégias de segurança internacional em uma nova ordem geopolítica mundial*" não poderia ocorrer em um momento mais adequado e oportuno. O ano de 2020 promoveu de forma bastante acelerada uma maior conscientização da população mundial acerca dos principais desafios, vulnerabilidades e riscos à segurança internacional e à defesa nacional dos Estados, mesmo na ausência de guerras ou conflitos armados.

Em primeiro lugar, o último ano expôs de uma forma nunca antes vista a urgência de uma resposta global para a crise climática e ambiental planetária que esteja baseada no respeito ao princípio da soberania nacional. Nem a desaceleração da economia mundial resultante das políticas de lockdown para o combate à pandemia do novo coronavírus, nem o efeito de resfriamento do La Niña, foram suficientes para conter o aumento na temperatura global, registrando sua média mais elevada na série histórica que mede a diferença de temperatura em relação aos níveis pré-industriais.

Além disso, a pandemia do novo coronavírus fez com que duas importantes cúpulas sobre o meio ambiente fossem adiadas para este ano de 2021: a cúpula do clima que aconteceria em Glasgow (Reino Unido) e a reunião sobre biodiversidade de Kunming (China). A grande apreensão dos especialistas quanto aos resultados dessas duas cúpulas de negociações climáticas para o futuro da humanidade não apenas evidencia a percepção de ameaça à segurança internacional trazida pelo tema, mas também o caráter decisivo do ano de 2021 para o futuro da luta global contra a crise climática e ambiental planetária.

opportunities, but also great challenges for international security.

In this context, there is great effort to keep cyberspace open, free and safe. Open to enable the promotion of universal, affordable and egalitarian internet access, in particular to enable economic growth and innovation and to generate political, social and economic development worldwide. Free to enable the promotion and protection of human rights and fundamental freedoms, including freedom of expression, access to information, right of assembly and association, privacy and fair trial. Safe to enable better cooperation and fight against cybercrimes, especially through the use of diplomatic and legal tools and in building cyber resilience against cyberattacks.

Finally, the year 2020 revealed the gradual erosion of existing multilateral organisms and transnational alliances as instruments capable of managing the international cooperation for fighting risks and threats to international security other than traditional wars or armed conflicts. The absence of a global strategy for fighting the pandemic and the low cooperation level among nation States, even in Europe, for fighting the virus are in sharp contrast with the increase in national and unilateral governmental measures for defending countries and their populations.

The latest developments make it essential to resume multilateral and transnational cooperation to keep international peace and security. We believe that the 18th edition of the Forte de Copacabana International Security Conference will strongly contribute to this resumption insofar as it will offer a space for plural dialogue and for building and valuing consensus on international security and defence issues among senior government officials, politicians, academia, businessmen, civil society representatives and members of the armed forces of South American and European countries.

Igualmente, o ano de 2020 representou um ponto de inflexão na forma como a sociedade contemporânea se relaciona com as tecnologias da informação e das comunicações. Pressionada por uma situação sanitária inesperada, a imersão da sociedade contemporânea nessa nova era de convivência indispensável com as tecnologias digitais tem gerado inúmeras oportunidades, mas também grandes desafios para a segurança internacional.

Neste âmbito, há um largo esforço para que o espaço cibernético se mantenha aberto, livre e seguro. Aberto para que permita a promoção de acesso à internet universal, acessível e igual, em particular para que permita crescimento econômico e inovação e gere desenvolvimento político, social e econômico no mundo todo. Livre para que seja possível a promoção e proteção dos direitos humanos e liberdades fundamentais, incluindo a liberdade de expressão, acesso à informação, direito de reunião e associação, privacidade e julgamento justo. Seguro para que permita melhor cooperação e luta contra crimes cibernéticos, especialmente através do uso de instrumentos diplomáticos e legais e na construção de resiliência cibernética contra ataques cibernéticos.

Por fim, o ano de 2020 expôs a erosão gradual dos organismos multilaterais e alianças transnacionais existentes como instrumentos capazes de gerir a cooperação internacional de enfrentamento a riscos e ameaças à segurança internacional de origem outra, que não guerras ou conflitos armados tradicionais. A ausência de uma estratégia global de enfrentamento à pandemia e o baixo nível de cooperação entre os Estados nacionais, inclusive na Europa, no combate ao vírus, contrastam com o crescimento de medidas governamentais de caráter nacional e unilateral para a defesa dos países e de suas populações.

Os últimos acontecimentos tornam imprescindível a retomada da cooperação multilateral e transnacional para a manutenção da paz e da segurança internacionais. Acreditamos que a XVIII edição da Conferência de Segurança Internacional do Forte de Copacabana contribuirá fortemente para essa retomada na medida em que oferecerá um espaço de diálogo plural e de construção e valorização de consensos em temas de segurança internacional e de defesa entre altos funcionários de governos, políticos, acadêmicos, empresários, representantes da sociedade civil e membros das forças armadas de países sul-americanos e europeus.

A Delegação da União Europeia (UE) no Brasil é uma dentre as mais de 140 representações da UE no mundo. Nosso foco é a promoção de relações políticas, econômicas e de cooperação entre a UE e o Brasil, como parte de nossa Parceria Estratégica instituída em 2007. O estabelecimento de relações diplomáticas se deu em 1960, reforçando intensos laços históricos, culturais, econômicos, políticos e de cooperação. Os principais temas desta Parceria Estratégica, com mais de 30 diálogos formais sobre políticas setoriais e com mais de uma centena de projetos em andamento, incluem questões econômicas, cooperação em questões-chave de política externa e ações conjuntas em desafios globais, em áreas como direitos humanos, mudança climática, segurança e defesa, e também no combate à pobreza e ao crime organizado.

Nas relações diplomáticas com nossos parceiros, diferentes países e regiões ao redor do mundo, bem como fóruns multilaterais, devido à pandemia de covid-19, já tínhamos, e reforçamos, o compromisso de incrementar nossa cooperação, buscando soluções que nos levarão a uma reconstrução mais verde e mais resiliente e à recuperação de nossas sociedades. A UE criou uma operação humanitária e de assistência de larga escala para auxiliar nossos parceiros em países emergentes e em desenvolvimento. Implementamos com sucesso uma cooperação entre Estados membros e instituições europeias com uma nova abordagem denominada "Equipe Europa". Como "Equipe Europa", a Delegação da UE no Brasil, as Embaixadas de Estados membros da UE e instituições europeias

The European Union (EU) Delegation to Brazil is one of over 140 EU representations around the world. We are focused on promoting political, economic and cooperation relations between the EU and Brazil, within our Strategic Partnership instituted in 2007. Diplomatic relations were established in 1960, building on close historical, cultural, economic, cooperation and political ties. Central topics of this Strategic Partnership, with more than 30 formal sector-policy dialogues and a hundred ongoing projects, include economic issues, cooperation on key foreign policy issues, and jointly addresses global challenges in areas such as human rights, climate change, security and defence, as well as the fight against poverty and organized crime.

In our external relations with different partner countries and regions around the world, as well as in multilateral fora, owing to the COVID-19 pandemic, we were and are even more committed to enhance our cooperation, looking for solutions that will lead us to an even greener and resilient reconstruction and recuperation of our societies. The EU has set up a large-scale humanitarian and assistance operation to help our partners in emerging and developing countries. We successfully implemented a close cooperation between Member States and European institutions with a new "Team Europe" approach. As "Team Europe", the EU Delegation to Brazil and the Embassies of the Member States of the European Union and European institutions such as the European Investment Bank have

joined efforts with Brazilian institutions to accommodate the raising demands of the pandemic. The support actions have had two strands: physical emergency aid provided mainly through existing projects financed by the EU and its Member States, and adjustment of work plans in order to include actions to prevent and combat the pandemic.

The EU and Brazil are also important trading partners. We are the largest foreign investors in Brazil. The EU is Brazil's second-biggest trading partner, accounting for 15% of its total trade, and Brazil is the EU's twelfth biggest trading partner, accounting for 1.5% of total EU trade (2020).

The theme of international security and defence is of utmost importance to the EU as we face many challenges, namely: growing geopolitical competition and pressure on the multilateral system; destabilisation of our regional environment; as well as increasingly sophisticated hybrid and transnational threats targeting the EU directly. Our key objectives are to preserve peace, prevent conflicts and strengthen international security, in accordance with the purposes and principles of the United Nations Charter.

To counter these challenges, protect our citizens, and enhance our strategic autonomy to become a stronger global partner, the EU needs to define what kind of security and defence actor it wants to be.

The common security and defence policy (CSDP) is an integral part of the Union's common foreign and security policy (CFSP) and it is framed by the Treaty on European Union (TEU). It is a rapidly evolving policy. In June 2016, an EU Global Strategy on Foreign and Security Policy (EUGS) was adopted and identified five main priorities for EU foreign policy: 1 - the security of the Union; 2 - state and societal resilience to the East and South of the EU; 3 - the development of an integrated approach to conflicts; 4 - cooperative regional orders; and 5 - global governance for the 21st century. This strategy was the outcome of a truly collective work, with all the Member States, providing a unique opportunity to focus on values and interests that we all shared, as Europeans.

As underlined by the EU High Representative and Vice President of the European Commission, Josep Borrell, the world is changing very quickly and the EU security and defence policy must be led in consonance with the big changes in the world. That is why the EU needs to do more and to do more together. As the demand for EU engagement is rising, its supply must keep pace.

In this context, the EU is working on a Strategic Compass that should be adopted in March 2022 and will help not only strengthen a common European security and defence culture but also define the right objectives and concrete goals for its policies. Its main missions are to: enhance our resilience to prevent and respond to changing security threats and challenges; have the necessary civilian and military capabilities and step up cooperation with partners bilaterally and with international organisations.

A unified EU, in the spirit of "Team Europe", is the best way to make our external action more effective. It is also in this context that our partnership with Latin America, and with Brazil, is gaining a new relevance and urgency. Our global agendas are very much aligned, and we face the same challenges – from migration and the pandemic to cyber or climate security. A new Strategy for Latin America and the Caribbean is due precisely to mark this new phase in our partnership. The joint communication, called "***European Union, Latin America and the Caribbean: joining forces for a common future***", adopted in April 2019, focuses on four sectors to develop our partnership: prosperity, democracy, resilience, and effective global governance, with practical steps for each of these fields.

como o Banco Europeu de Investimentos uniram esforços com instituições brasileiras para responder às crescentes demandas da pandemia. As ações de apoio possuem dois eixos: ajuda emergencial física, fornecida principalmente através de projetos já existentes financiados pela UE e seus Estados membros, e o ajuste de planos de trabalho, com a finalidade de incluir ações de prevenção e combate à pandemia.

A UE e o Brasil também são importantes parceiros comerciais. Somos os maiores investidores estrangeiros no Brasil. A UE é o segundo maior parceiro comercial do Brasil, destino de 15% das exportações brasileiras, e o Brasil é o décimo segundo maior parceiro comercial da UE, destino de 1,5% das exportações totais da UE (2020).

Um tema da maior importância para a UE é segurança internacional e defesa, pois nos deparamos com muitos desafios, a saber: o aumento da competição geopolítica e da pressão sobre o sistema multilateral; a desestabilização de nosso ambiente regional; bem como um aumento na sofisticação de ameaças híbridas e transnacionais que têm a UE diretamente como alvo. Nossos principais objetivos são preservar a paz, evitar conflitos e fortalecer a segurança internacional, segundo os propósitos e princípios da Carta das Nações Unidas.

A UE precisa definir o tipo de atuação que deseja ter no âmbito de segurança e defesa para enfrentar tais desafios, proteger nossos cidadãos e aprimorar nossa autonomia estratégica para nos tornarmos um parceiro global mais forte.

A Política Comum de Segurança e Defesa (PCSD) é parte integral da Política Externa e de Segurança Comum (PESC) da UE, respaldada pelo Tratado da União Europeia (TUE). Trata-se de uma política em rápida evolução. Em junho de 2016, foi adotada uma Estratégia Global da UE para a Política Externa e de Segurança (EGUE), que identificou cinco prioridades para a política externa da UE: 1 - a segurança da UE; 2 – a resiliência do Estado e da sociedade ao Leste e ao Sul da UE; 3 - o desenvolvimento de uma abordagem integrada a conflitos; 4 - cooperação entre ordens regionais; e 5 – governança global para o século XXI. Esta estratégia resultou de um trabalho verdadeiramente coletivo, envolvendo todos os Estados membros, apresentando uma oportunidade única para focar nos valores e interesses que todos compartilhamos como europeus.

Conforme enfatizado pelo Alto Representante da UE e Vice-presidente da Comissão Europeia, Josep Borrell, o mundo está mudando muito rapidamente, e a política de segurança e defesa da UE deve ser conduzida em consonância com as grandes transformações mundiais. Portanto, a UE precisa realizar mais, e realizar mais em conjunto. Há uma crescente demanda pelo envolvimento da UE, e suas ações devem acompanhar tal crescimento.

Neste contexto, a UE está desenvolvendo uma Bússola Estratégica que deve ser adotada em março de 2022. Esta ajudará não somente a fortalecer a cultura comum de segurança e defesa europeia, como também ajudará a definir objetivos adequados e metas concretas para suas políticas. Suas principais missões são: aprimorar nossa resiliência na prevenção e resposta às transformações nas ameaças e desafios de segurança; ter as capacidades civis e militares necessárias e reforçar as cooperações com parceiros bilaterais e com organizações internacionais.

Uma UE unificada, no espírito da “Equipe Europa”, é a melhor forma de tornar mais eficiente nossa ação externa. É também neste contexto que nossa parceria com a América Latina e com o Brasil ganha nova relevância e urgência. Nossas agendas globais estão muito alinhadas e enfrentamos os mesmos desafios — de migrações e pandemia à segurança cibernética ou climática. Uma nova Estratégia para a América Latina e Caribe é aguardada justamente para marcar esta nova fase em nossa parceria. A comunicação conjunta, intitulada "União Europeia, América Latina e Caribe: unir esforços em prol de um futuro comum", adotada em abril de 2019,

The coronavirus pandemic has disrupted our ways of living and working, as well as the way we conduct foreign policy. It has enormous consequences for international stability and, as our Commission President Ursula von der Leyen stated: "Alone, none of us can face up to today's global challenges. Only together do we have the strength to fight poverty, corruption or terror. Only together can we fight climate change and invest in progress. And only together can we stand for peace and prosperity." It remains a priority in the coming months to broaden this approach beyond the emergency situations we have experienced, in order to further strengthen international security and overcome this crisis together.

concentra-se em quatro setores para o desenvolvimento de nossa parceria: prosperidade, democracia, resiliência e governança global efetiva, com passos práticos para cada um destes campos.

A pandemia do coronavírus impôs uma ruptura nas nossas formas de viver e trabalhar, assim como na nossa condução da política externa. Traz imensas consequências para a estabilidade internacional e, segundo declaração de Ursula von der Leyen, Presidente de nossa Comissão: "Isoladamente, nenhum de nós consegue enfrentar os desafios globais atuais. Somente juntos temos força para combater a pobreza, a corrupção ou o terrorismo. Apenas juntos podemos combater a mudança climática e investir no progresso. E somente juntos podemos defender a paz e a prosperidade." É prioritário, nos próximos meses, ampliar esta abordagem para além das situações de emergência pelas quais passamos, para reforçar ainda mais a segurança internacional e superarmos juntos esta crise.

ARTIGOS
ARTICLES

Margarita Cuervo Iglesias

Mestre em Estudos de Desenvolvimento, doutoranda, Universität der Bundeswehr München. Além de ter trabalhado como gerente de projetos no escritório da Konrad-Adenauer-Stiftung em Bogotá e como assistente de pesquisa em Berlim, atualmente é bolsista da KAS e membro de sua escola de doutorado em segurança e desenvolvimento.

MA in Development Studies, PhD candidate, Universität der Bundeswehr München. Besides having worked as project manager at the Konrad-Adenauer-Stiftung office in Bogota and research assistant in Berlin, she is currently a KAS scholar and member of its security and development doctoral college.

Proteção de infraestruturas críticas: O papel central do setor privado na cooperação civil-militar

Protection of Critical Infrastructures: The Private Sector as Pivotal Actor of Civil-Military Cooperation

Margarita Cuervo Iglesias

Resumo

O aumento dos riscos emergentes que afetam o fornecimento transnacional e doméstico de bens públicos tornou ainda mais evidente a ligação entre segurança e estabilidade econômica. Nesse contexto, a proteção de infraestruturas críticas ganhou destaque entre líderes de segurança e defesa do mundo todo. Embora a partir de perspectivas diferentes, estados europeus e latino-americanos desenvolveram respostas institucionais para prevenir e mitigar riscos a instalações, redes e serviços cruciais para o funcionamento de seus governos, assim como para o fornecimento de bens essenciais para sua população. Neste artigo, argumenta-se que, embora alguns passos cruciais tenham sido dados nessa direção, é necessário aumentar a cooperação civil-militar a esse respeito e facilitar esforços conjuntos que incluam o setor privado. Devido a seus recursos e papel fundamental em infraestruturas críticas, as empresas não estatais também têm interesse e potencial para contribuir para a construção de resiliência. Por fim, o documento destaca recomendações importantes a serem consideradas na interface civil-militar com vistas a construir resiliência e gerenciar riscos que afetem infraestruturas críticas.

Summary

With cumulative, emerging risks that affect the transnational and domestic supply of public goods, the intertwining between security and economic stability has become more evident. In this context, the protection of critical infrastructures has gained considerable momentum amongst security and defence leaders worldwide. Although from different perspectives, European and Latin American states have developed institutional responses to prevent and mitigate risks to facilities, networks, and services crucial for the functioning of governments and providing fundamental goods to their population. This paper argues that, although some crucial steps have been taken in this direction, it is necessary to enhance civil-military cooperation in this respect and facilitate joint efforts with the private sector. Because of their resources and pivotal role in critical infrastructures, non-state enterprises also have an interest in and a potential to contribute to building resilience. Finally, the paper highlights important recommendations to consider in the civil-military interface to build resilience and manage risks that affect critical infrastructures.

Context and relevance

The first two decades of the twenty-first century have witnessed increasing uncertainty with emerging risks that require comprehensive and transnational approaches to tackle them. Over the past years, the vulnerability of crucial sectors for social and economic stability has become more evident as hybrid threats and unexpected events jeopardise global security and business continuity. While each country and multilateral organisation has its definition and sometimes even differing terms to refer to this matter, a consensus has grown around the importance of protecting critical infrastructures.

Critical infrastructures are facilities, networks and assets that ensure public goods and services and therefore, in case of failure or destruction, could affect national security. These sectors are increasingly exposed to a broad spectrum of phenomena that can interrupt or disrupt their services: terrorism, cyberattacks, industrial espionage, natural hazards, pandemics, and other events that directly or indirectly compromise physical security. In this sense, they are systemically relevant sectors that go from the energy, water and food supply, waste disposal and nuclear industry, to information and communication technology, finance, health, and chemical industries.

One of the reasons why protecting critical infrastructures has become more relevant is that the interconnectedness and transnational character of many of these sectors increases their susceptibility. This, in turn, fosters the interaction between multiple destabilising factors and hazards. For instance, a global health event such as a pandemic or a climate-related catastrophe can compromise the continuity of global supply chains; in such a context, decision-making may increasingly depend on virtual communication and hostile actors and geopolitical adversaries can profit from growing vulnerability to carry out cyberattacks, which, ultimately, also have physical consequences for security.

Another example of why military and civilian organisations are concerned with how to better safeguard critical infrastructures is related to the use of social media by state and non-state actors interested in instability. The diffusion of disinformation throughout such wide-reaching channels can create, profit from and exacerbate an atmosphere of social discontent, polarisation and ambiguity, thus having cognitive and behavioural consequences. This has been recently witnessed in cases of electoral interference. Indeed, the practice of using information networks to polarise, misinform and fuel political instability is likely to increment. This poses the additional challenge of countering attacks that certainly have consequences for security without being able to trace the adversaries or even know which military or non-military means can counter these threats.

Current security threats are less straightforward and the volatility of the geopolitical, environmental, and social context is rather the rule. Consequently, there is a consensus that the best way of tackling this ambiguity is through risk management and building resilience, for which a whole-of-society approach is needed. Indeed, besides identifying possible risks and preparing for them, organisations and governments are

Contexto e relevância

As primeiras duas décadas do século XXI testemunharam o aumento da incerteza, com riscos emergentes que exigem abordagens de enfrentamento abrangentes e transnacionais. Nos últimos anos, a vulnerabilidade de setores cruciais para a estabilidade social e econômica tornou-se mais evidente, à medida que ameaças híbridas e eventos inesperados colocam em risco a segurança global e a continuidade dos negócios. Apesar de cada país e organização multilateral ter sua própria definição e, às vezes, até mesmo termos diferentes para se referir ao tema, existe um consenso quanto à importância de proteger infraestruturas críticas.

Infraestruturas críticas são instalações, redes e ativos que garantem o fornecimento de bens e serviços públicos e que, por este motivo, em caso de falha ou destruição, podem afetar a segurança nacional. Estes setores estão cada vez mais expostos a uma ampla gama de fenômenos que podem perturbar ou interromper seus serviços: terrorismo, ciberataques, espionagem industrial, desastres naturais e pandemias são alguns dos muitos eventos que, direta ou indiretamente, comprometem a segurança física. Trata-se de setores sistemicamente relevantes que incluem energia, água, abastecimento de alimentos, disposição de resíduos, indústria nuclear, tecnologia da informação, comunicação, finanças, saúde e indústrias químicas.

Uma das razões pelas quais a proteção de infraestruturas críticas tornou-se mais relevante é que o caráter interconectado e transnacional de muitos desses setores aumenta sua suscetibilidade. Isso, por sua vez, promove a interação entre vários fatores e acarreta riscos desestabilizadores. Um evento de saúde global, como uma pandemia ou catástrofe relacionada ao clima, pode comprometer a continuidade das cadeias de abastecimento globais, por exemplo. Nesse contexto, com a tomada de decisões dependendo cada vez mais da comunicação virtual, atores hostis e adversários geopolíticos podem se aproveitar da crescente vulnerabilidade para realizar ataques cibernéticos que, em última análise, também têm consequências físicas para a segurança.

Outro motivo pelo qual organizações militares e civis estão buscando formas de melhorar a proteção das infraestruturas críticas está relacionado ao uso das mídias sociais por atores estatais e não estatais interessados na instabilidade. A disseminação da desinformação por meio de canais de grande alcance pode gerar e exacerbar um clima de insatisfação, polarização e ambiguidade social, com consequências cognitivas e comportamentais. Isso foi demonstrado recentemente em casos de interferência eleitoral. Na verdade, o uso das redes de informação para polarizar, desinformar e alimentar a instabilidade política tende a aumentar. Como resultado, haverá o desafio adicional de conter ataques que certamente terão impactos na segurança, sem a possibilidade de rastrear os adversários ou mesmo de saber quais meios, militares ou não militares, podem ser usados no combate a tais ameaças.

As ameaças atuais à segurança são complexas, e a regra é justamente a volatilidade do contexto geopolítico, ambiental e social. À vista disso, é consenso dizer que a melhor forma de lidar com essa ambiguidade é por meio da gestão de riscos e da construção de resiliência, utilizando uma abordagem que envolva toda a sociedade. De fato, além

oriented to enhance their ability to resist, absorb, recover from, or successfully adapt to adversity. Against this backdrop, civil-military cooperation is needed to counter risks to critical infrastructures.

Among the civilian organisations that governments and their security forces can engage in building resilience, private corporations play a pivotal role. For one thing, due to the increasing globalisation and privatisation since the last decades of the twentieth century, a significantly major part of critical infrastructures is currently owned and managed by private companies. Moreover, in the technology, information and communication global supply chains, non-state enterprises are the leading force, which makes them a growing target of and means to perpetrate cyberattacks. Among other worrisome examples, the recent hack to SolarWinds in the United States raised awareness on these vulnerabilities, which in this case impacted several sensitive stakeholders, including the inland energy infrastructure, federal and foreign governmental agencies.

The resources available to the business sector are an additional reason to coordinate actions with this actor in building resilience. Since they are also interested in promoting business continuity, private corporations can join their knowledge and capabilities with those of military and non-military state entities. Additionally, given the high sensitivity that this issue represents for security, both military and private organisations are at the front-line of defending critical infrastructures: they are a likely direct target of attacks, can experience the indirect impact of hazards, but also have a high potential to prevent, mitigate and restore afterwards. Just like corporations are interested in security for their operations, military capabilities must be built to counter this sort of threats and, for this purpose, companies that own or operate critical infrastructures are of paramount importance.

Consequently, coordinated efforts between military and private sector organisations can have the ability to increase societal and economic resilience in the view of such threats. Both the experiences of Europe and Latin America can bring important insights and lessons, although there is still much more to do in terms of joint and transnational efforts. A comprehensive, civil-military approach that engages not only public entities but also the private sector is therefore necessary.

Steps in the right direction, with some remaining gaps in civil-military cooperation

In this scenario, states around the Western hemisphere are developing legislative and policy frameworks to tackle potential threats to sectors identified as crucial for stability. Moreover, armed forces have included the protection of critical infrastructures among their missions, either with this or other terminology. While security forces are adapting to the rising uncertainty and volatility in their operational environment, interaction and close cooperation with civilian entities, including the private sector, still needs to be enhanced for a whole-of-society response.

Although facing different operational challenges, military and civilian organisations

de identificar os possíveis riscos e se preparar para eles, as organizações e os governos são orientados a aumentar sua capacidade de resistir, absorver, se recuperar ou se adaptar com sucesso às adversidades. Nesse contexto, a cooperação civil-militar torna-se essencial como forma de lidar com os riscos às infraestruturas críticas.

Dentre as organizações civis com as quais os governos e as forças de segurança podem se engajar para aumentar sua resiliência, as empresas privadas desempenham um papel fundamental. Em primeiro lugar porque, com a crescente globalização e privatização das últimas décadas do século XX, muitas infraestruturas críticas passaram a ser controladas e gerenciadas por empresas privadas. Além disso, as empresas não estatais são líderes das cadeias globais de fornecimento de tecnologia, informação e comunicação, o que as torna um alvo crescente de ataques cibernéticos. Dentre outros exemplos preocupantes, a recente invasão por hackers do sistema da SolarWinds, nos Estados Unidos, veio comprovar tal vulnerabilidade. De fato, o ataque afetou diversas áreas sensíveis, que incluíram a infraestrutura nacional de energia, além de agências governamentais federais e estrangeiras.

Os recursos à disposição do setor empresarial são mais um motivo para articular ações com esse ator na busca de resiliência. As empresas privadas também estão interessadas em promover a continuidade dos negócios e podem agregar seus conhecimentos e competências aos de entidades militares e não militares do governo. Além disso, dada a alta sensibilidade deste problema para a segurança, as organizações militares e privadas estão na linha de frente da defesa de infraestruturas críticas: são um provável alvo direto de ataques, podem sofrer o impacto indireto dos perigos, mas também têm um alto potencial para prevenção, mitigação e posterior restauração. Assim como as grandes empresas estão interessadas na segurança de suas operações, as forças militares precisam se preparar para enfrentar esse tipo de ameaças. Por esse motivo, as empresas que possuem ou operam infraestruturas críticas são de suma importância.

Consequentemente, a coordenação de esforços entre organizações do setor militar e privado pode aumentar a resiliência social e econômica diante de tais ameaças. As experiências da Europa e da América Latina podem contribuir com pontos de vista e lições importantes, embora ainda haja muito a ser feito em termos de esforços conjuntos e transnacionais. Portanto, é necessária uma abordagem civil-militar abrangente que envolva não apenas entidades públicas, mas também o setor privado.

Passos na direção certa e algumas lacunas na cooperação civil-militar

Nesse cenário, os governos do hemisfério ocidental estão desenvolvendo estruturas legislativas e políticas para enfrentar as ameaças potenciais aos setores identificados como cruciais para a estabilidade. Além disso, as forças armadas incluíram a proteção de infraestruturas críticas como uma de suas missões, seja com esta ou outra terminologia. Enquanto as forças de segurança estão se adaptando à crescente incerteza e volatilidade em seu ambiente operacional, a interação e a estreita cooperação com entidades civis, incluindo o setor privado, ainda precisam ser aprimoradas para uma resposta que inclua toda a sociedade.

both in Europe and Latin America can learn from the experience of one another in terms of protection of critical infrastructure and countering emerging risks. Due to a long history of exposure to natural disasters and crises due to the effects of climate change, some Latin American countries have integrated the response and coordination between multiple public and private actors, including the military and corporate.

For instance, in the past decade, the Chilean army has strengthened its capabilities to respond to natural disasters, humanitarian crises and possible security risks that emerge in such contexts. In the aftermath of both the 2010 earthquake and the 2017 wildfires, the armed forces responded to mitigate the damage caused by these natural disasters. Among others, an integrated emergency information system enabled both civilian and military authorities to identify and manage risks to the population. The armies of Argentina, Brazil, Colombia, and Peru also have similar units and approaches to climate-related and other emergencies. A regional leader in security and defence, since the first decade of the twenty-first century, Brazil has developed its cybersecurity architecture and incorporated issues such as the protection of key energy security installations into its national defence policy and strategy. This includes preparedness for possible natural events and cyberattacks.

More recently, the Chilean government has presented a bill to deploy the armed forces in the protection of critical infrastructure. The draft law has been criticised insofar as it allows the use of public force to deal with possible security breaches in critical sectors without declaring a constitutional state of emergency. In this case, in the context of the social protests and unrest in Chile at the end of 2019, the government used the armed forces to unblock roads and re-establish public order in the face of excesses that occurred on the backdrop of the demonstrations. Something similar happened in Colombia in 2021 as the spiral of social discontent and roadblocks have jeopardised food, health and fuel supply, and cases of violent manifestations amid peaceful protests have destroyed public transport infrastructure. Both are highly sensitive cases, since deploying the armed forces in response to legitimate social protests, whether in a state of emergency or not, must be proportional and, without careful democratic civilian control and oversight, can lead to abuses and violent escalations.

While governments in the Latin American region have mostly developed national, unilateral plans and frameworks to protect critical infrastructure, the European Union (EU) and its member states have advanced on multilateral and bilateral mechanisms in addition to national efforts to counter threats in this area. Already in 2004, upon request of the European Council, the European Commission began to outline a comprehensive strategy to protect critical infrastructure in view of potential terrorist attacks. Although the communication mentions that private companies are also to be integrated into ensuring operational continuity in the sectors potentially affected by terrorism, it does not delve into this matter or the possible cooperation of companies with the military. Also in that year, the EU created its Agency for Network and Information Security (ENISA) to protect critical infrastructure in this sector.

Additionally, in 2006, the Commission created the European Programme for Critical Infrastructure Protection (EPCIP), which envisioned a methodology, action plan,

Embora enfrentando diferentes desafios operacionais, as organizações militares e civis na Europa e na América Latina podem aprender com a experiência umas das outras em termos de proteção de infraestrutura crítica e combate aos riscos emergentes. Devido a uma longa história de exposição a desastres naturais e crises causados pelas mudanças climáticas, alguns países latino-americanos articularam sua resposta e coordenação entre múltiplos atores públicos e privados, inclusive do setor militar e corporativo.

Por exemplo, na última década, o exército chileno fortaleceu sua capacidade de resposta a desastres naturais, crises humanitárias e possíveis riscos à segurança que surgem em tais contextos. Após o terremoto de 2010 e os incêndios florestais de 2017, as forças armadas atuaram na mitigação dos danos causados por esses desastres naturais. Além disso, foi criado um sistema integrado de informação de emergência que permitiu às autoridades civis e militares identificar e gerenciar os riscos para a população. Os exércitos da Argentina, Brasil, Colômbia e Peru também possuem unidades e abordagens semelhantes para emergências, como as relacionadas ao clima, dentre outras. Líder regional em segurança e defesa, desde a primeira década do século XXI, o Brasil desenvolveu sua arquitetura de segurança cibernética e incorporou questões como a proteção das principais instalações de segurança energética em sua política e estratégia de defesa nacional. Isso inclui prontidão para possíveis eventos naturais e ataques cibernéticos.

Mais recentemente, o governo chileno apresentou um projeto de lei para mobilização das forças armadas na proteção de infraestruturas críticas. O projeto de lei foi criticado por permitir o uso da força pública para lidar com possíveis violações de segurança em setores críticos sem antes declarar o estado de emergência constitucional. No final de 2019, com a onda de protestos e o clima de inquietação social no Chile, o governo utilizou as forças armadas para desbloquear estradas e restabelecer a ordem pública em face dos excessos que haviam ocorrido com as manifestações. Algo semelhante aconteceu na Colômbia, em 2021, quando a crescente insatisfação social e os bloqueios nas estradas prejudicaram o abastecimento de alimentos, medicamentos e combustíveis. Houve casos de manifestações violentas, durante protestos pacíficos, que acabaram destruindo a infraestrutura de transporte público. Ambos são casos altamente sensíveis, uma vez que o emprego das forças armadas na resposta a protestos sociais legítimos, quer em estado de emergência ou não, deve ser proporcional e, quando usado sem cuidadoso controle e supervisão civil democráticos, pode levar a abusos e escalada da violência.

Enquanto os governos da região da América Latina desenvolveram principalmente planos e estruturas nacionais unilaterais para a proteção de suas infraestruturas críticas, a União Europeia (EU) e seus Estados Membros avançaram nos mecanismos multilaterais e bilaterais que se somam aos esforços nacionais de combate às ameaças nesta área. Já em 2004, a pedido do Conselho Europeu, a Comissão Europeia começou a delinear uma estratégia abrangente para a proteção de infraestruturas críticas contra potenciais ataques terroristas. Embora a comunicação mencione que as empresas privadas também devem ser contempladas, de modo a garantir a continuidade operacional nos setores potencialmente afetados pelo terrorismo, não se aprofunda sobre o tema ou sobre a possível cooperação entre empresas e forças armadas. Naquele mesmo ano, a UE criou a Agência da União Europeia para a Cibersegurança (ENISA) com o objetivo de proteger as infraestruturas críticas do setor.

response to contingency and cooperation measures with third countries. Two years later, the EU issued the Directive for European Critical Infrastructure, with specific criteria to identify European critical infrastructure and demanding that member states engage in this task. Among the most relevant mechanisms for the European protection of critical infrastructure, an early-warning system serves for rapid information exchange and monitoring of risks to this type of facilities and assets: the Critical Infrastructure Warning Information Network (CIWIN). Although the focus of these instruments was initially to build resilience against terrorist attacks, the development of the geopolitical and security environment in the past decade has leaned emphasis towards hybrid warfare and, with increasing attention, cyberthreats.

Besides the potential of incidents that directly compromise physical infrastructure, European states have mostly, although not exclusively, focused on hybrid threats and the influx of destabilising state and non-state actors. In this respect, the North Atlantic Treaty Organization (NATO) has also developed a major focus on hybrid threats. Here too, the military organisation strives for the engagement of the private sector in countering and preparing for emerging risks that compromise critical infrastructures. Indeed, already from its wording, Article 2 of the North Atlantic Treaty assumes economic cooperation between the member states as a basis of the defence alliance.

However, the rapid advance in technological developments and digitalisation has, in turn, increased state and private infrastructure exposure to hybrid threats. For instance, NATO has advanced in dialogues with companies of the energy sector to envision cooperation to protect this type of infrastructure. Moreover, during the last decade, the Alliance has also worked with the private industry developing collaborative networks and expertise exchange with representatives of information technology companies to develop capabilities against cyberthreats.

Another private-sector development with geopolitical consequences further stresses the importance of awareness-raising and cooperation with companies in protecting those infrastructures crucial for security and stability. Just like in other regions of the world, Beijing's increasing participation in building and buying road and railway projects, electronic infrastructure, sea and airports is noticeable in Europe and Latin America. It has long been evident that China's investments in private and public critical infrastructure represent a strategic advantage, but little is being done to stop its scaling presence and influence. This, too, is an area where public and private actors concerned with security must cooperate.

All of the above points underline the importance of a whole-of-society perspective to address emerging security risks. Against this backdrop, coordinated efforts between military and civilian organisations, including in particular the private sector, can enhance the ability to build societal resilience and safeguard critical infrastructure. The next and final section proposes some courses of action that can be considered when fostering more civil-military action for this purpose.

Além disso, em 2006, a Comissão criou também o Programa Europeu de Proteção de Infraestruturas Críticas (EPCIP), que previa metodologia, plano de ação, resposta a medidas de contingência e cooperação com países fora da UE. Dois anos depois, a UE propôs a diretiva Europeia de Infraestruturas Críticas, descrevendo os critérios para identificação das Infraestruturas Críticas Europeias (ICE) e exigindo que os Estados Membros se engajassem nesta tarefa. Um dos mecanismos mais relevantes para a proteção de infraestruturas críticas europeias é a Rede de Alerta para Infraestruturas Críticas (CIWIN), um sistema de alerta precoce que serve para a troca rápida de informações e monitorização de riscos para este tipo de instalações e ativos. Apesar do foco inicial desses instrumentos ter sido a criação de resiliência contra ataques terroristas, o desenvolvimento do ambiente geopolítico e de segurança da última década passou a enfatizar a guerra híbrida, com atenção crescente para as ameaças cibernéticas.

Além de focar no potencial de incidentes que comprometem diretamente a infraestrutura física, os estados europeus têm se concentrado, principalmente, embora não exclusivamente, em ameaças híbridas e no influxo de elementos desestabilizadores estatais e não estatais. Nessa mesma linha, a Organização do Tratado do Atlântico Norte (OTAN) desenvolveu um foco significativo nas ameaças híbridas. Aqui, a organização militar também se esforça para envolver o setor privado no combate e preparação para os riscos emergentes que comprometem as infraestruturas críticas. Na realidade, já em sua redação, o Artigo 2 do Tratado do Atlântico Norte pressupõe a cooperação econômica entre os Estados Membros como base da aliança de defesa.

No entanto, o rápido avanço nos desenvolvimentos tecnológicos e na digitalização, por sua vez, aumentou a exposição da infraestrutura pública e privada a ameaças híbridas. Por exemplo, a OTAN tem avançado nos diálogos com empresas do setor de energia, visando a cooperação para proteger esse tipo de infraestrutura. Além disso, durante a última década, a Aliança também trabalhou com a indústria privada, desenvolvendo redes colaborativas e trocas de experiência com representantes de empresas de tecnologia da informação para a capacitação contra ameaças cibernéticas.

Outro desenvolvimento no setor privado com consequências geopolíticas destaca ainda mais a importância da sensibilização e da cooperação com as empresas na proteção de infraestruturas cruciais para a segurança e a estabilidade. Assim como em outras regiões do mundo, a crescente participação de Pequim na construção e compra de projetos rodoviários e ferroviários, infraestrutura eletrônica, marítima e aeroportuária é evidente na Europa e na América Latina. Há muito ficou claro que os investimentos da China em infraestrutura crítica privada e pública representam uma vantagem estratégica, mas pouco vem sendo feito para impedir sua presença e influência crescentes. Esta também é uma área em que os atores públicos e privados preocupados com a segurança devem cooperar.

Todos os pontos levantados acima enfatizam a importância de uma perspectiva que englobe toda a sociedade para lidar com os riscos de segurança emergentes. Nesse contexto, os esforços coordenados entre organizações militares e civis, incluindo em particular o setor privado, podem aumentar a capacidade de geração de resiliência social e salvaguardar infraestruturas críticas. A próxima seção propõe caminhos que podem ser considerados para o fomento da ação civil-militar com este propósito.

Recommendations for decision-makers

In general terms, in the case of Latin American countries, although there has been recent progress in developing frameworks to protect critical infrastructure, it is still necessary to promote more multilateral and bi-national cooperation. Undoubtedly, strengthening domestic regulations and capabilities is an important foundation but, given the increasingly transnational character of the threats, collaborative efforts among partners in the region are essential.

While the operational landscape of the two regions differs in many respects, given the growing global potential for hybrid threats and catastrophes related to climate change, information and expertise sharing from military and civilian organisations on both sides of the Atlantic would serve to enhance preparedness. While Latin American countries can still learn much from the European experience against hybrid threats to their critical infrastructures, EU civilian and military organisations can benefit from exchanges with their peers that have been dealing with natural disasters for many decades.

As for the EU, there is a positive balance in the development of national capabilities, as well as bilateral and multilateral cooperation mechanisms. However, as Brussels has already indicated, cooperation with NATO needs to be strengthened, both because of the need to align responses to and share information on emerging risks, and because of the value of the United States experience and role in dealing with threats to critical infrastructures. In this respect, the European Centre of Excellence for Countering Hybrid Threats, which has existed since 2016, is an important initiative to foster EU-NATO cooperation.

The following lines overview additional ways in which civilian and military organisations in both regions can and should continue to build resilience to threats that affect highly sensitive sectors. Firstly, *public-private partnerships* can help enhance cooperation between armed forces and civilian counterparts interested in protecting critical infrastructures. These have the potential of generating synergy effects by profiting from the different capabilities that the public and private actors bring in. Applying this approach to the protection of critical infrastructures also fosters adaptability and responsiveness in a comprehensive manner.

Additionally, public-private partnerships aiming to build resilience with the participation of military and private sector organisations should *not only prioritise great private corporations and contractors, but also engage small and middle-sized enterprises* (SMEs). This can improve resilience along transnational and cross-sectorial value chains that ultimately ensure operational continuity. Moreover, through this type of partnerships, governments can promote shared responsibility with private corporations and the latter can benefit, among others, through participation in relevant regulation in topics like energy security, information and technology management.

Secondly, civilian and military leaders in the security sector must activate, test and improve existing *information exchange mechanisms and platforms for risk monitoring*

Recomendações para os tomadores de decisão

Em termos gerais, observaram-se avanços recentes no desenvolvimento de sistemas de proteção de infraestruturas críticas nos países latino-americanos. Entretanto, continuam sendo necessárias ações de cooperação multilateral e binacional. Sem dúvida, o fortalecimento das regulamentações e competências nacionais constitui uma base importante, porém, dado o caráter cada vez mais transnacional das ameaças, os esforços de colaboração entre os parceiros da região tornaram-se essenciais.

Apesar de seus panoramas operacionais sejam diferentes sob vários aspectos, dado o crescente potencial global para ameaças híbridas e catástrofes relacionadas às mudanças climáticas, organizações civis e militares dos dois lados do Atlântico podem aumentar seu nível de prontidão, compartilhando informações e conhecimentos especializados. Enquanto os países latino-americanos têm muito a aprender com a experiência europeia contra ameaças híbridas a suas infraestruturas críticas, as organizações civis e militares da UE podem se beneficiar do intercâmbio com seus pares, habituados a lidar com desastres naturais há várias décadas.

Quanto à UE, existe um equilíbrio positivo no desenvolvimento das capacidades nacionais, bem como nos mecanismos de cooperação bilateral e multilateral. No entanto, como Bruxelas já indicou, a cooperação com a OTAN precisa ser reforçada, tanto pela necessidade de alinhar as respostas e compartilhar informações sobre riscos emergentes, quanto pelo valor da experiência e do papel dos Estados Unidos no tratamento de ameaças às infraestruturas críticas. Neste sentido, o Centro Europeu de Excelência para Combate às Ameaças Híbridas, que existe desde 2016, é uma iniciativa importante para fomentar a cooperação UE-OTAN.

A seguir, apresentamos outras maneiras por meio das quais as organizações civis e militares das duas regiões não só podem, como devem continuar construindo resiliência a ameaças que afetem setores altamente sensíveis. Em primeiro lugar, as *parcerias público-privadas* podem ajudar a melhorar a cooperação entre as forças armadas e suas contrapartes civis interessadas em proteger infraestruturas críticas. Elas têm o potencial de gerar efeitos sinergísticos, beneficiando-se das diferentes competências trazidas pelos parceiros públicos e privados. A implementação dessa abordagem à proteção de infraestruturas críticas também promove a adaptabilidade e a capacidade de resposta de uma forma abrangente.

Ademais, as parcerias público-privadas que visam construir resiliência com a participação de organizações militares e do setor privado deveriam *não apenas priorizar grandes empresas e fornecedores privados*, como também *envolver pequenas e médias empresas* (PMEs). Isso melhora a resiliência das cadeias de valor transnacionais e intersetoriais e, em última análise, garante a continuidade operacional. Além do que, por meio desse tipo de parceria, os governos podem promover a responsabilidade compartilhada com as empresas privadas, e estas podem se beneficiar, dentre outras coisas, com a participação na regulamentação de temas relevantes como segurança energética, gestão da informação e da tecnologia.

Em segundo lugar, líderes civis e militares do setor de segurança devem ativar, testar e

and reporting. The high degree of uncertainty and volatility faced by civilian organisations and armed forces in protecting critical infrastructure makes the ability to monitor, access and share real-time information that accounts for developments and anomalies a decisive factor. This is why some of the areas with the greatest potential for collaboration between the military sector and private corporations in risk management are intelligence and capacity building.

In this regard, governments and organisations interested in improving the resilience of their critical sectors should invest, leverage resources, and foster information sharing tools and mechanisms. This includes *military and business intelligence and the training of security professionals* in the private sector, military personnel and analysts in the public sector. Indeed, to anticipate potential attacks or identify risks promptly, it is key to share information collaboratively through resource platforms that help access and exchange data among all stakeholders.

Such measures can, in turn, support strategic foresight and early warning systems, which are highly valuable in terms of risk management. Both military and private sector corporations can share their expertise and resources, protocols, and processes to anticipate, assess, and mitigate hazards that might affect systemically relevant sectors. For this purpose, *data management and analytics* can offer useful insights into atypical developments, enabling timely responses. This is all the more relevant because, even if governments and private companies invest in structural measures to enhance the resilience of critical infrastructures, there will always be highly unpredictable risks. Indeed, this implies a paradox: some risks may be so improbable that stakeholders do not invest resources in preparedness; but once the risk becomes imminent, it is too late to generate an adequate response.

A further identified priority is to increase the readiness and awareness of society for such risks. In this regard, *conducting crisis management and emergency preparedness exercises* with the participation of different stakeholders is a useful instrument. Beyond the importance of running such drills to build and enhance capabilities, this can also help to raise public understanding regarding different types of threats and how to respond to an eventual crisis. For this reason, involving media and civil society actors when conducting crisis management exercises is crucial.

Ideally, these practices should *involve multiple stakeholders at the national and transnational level*, testing coordination, communication, responsiveness, joint contingency plans, and how can private corporations, military and other stakeholders ensure levels of continuity under an emergency. As mentioned before, besides the cybersecurity dimension, other crises should receive attention, such as those that might result from natural disasters, extremist and terrorist attacks. The mutually reinforcing potential of these events and risks should also be highlighted during exercises.

Additionally, *private sector partners for governments and their armed forces can help to build networks and communication bridges* with key civil society organisations and multiplicators to advance on *education and awareness-raising* on the risks, how to

aprimorar *mecanismos de troca de informações e plataformas para monitoramento e relatórios de risco*. O alto grau de incerteza e volatilidade enfrentado por organizações civis e forças armadas na proteção de infraestrutura crítica torna um fator decisivo a capacidade de monitorar, acessar e compartilhar em tempo real informações sobre eventos e anomalias. É por esse motivo que algumas das áreas com maior potencial para colaboração entre o setor militar e as empresas privadas no gerenciamento de risco são inteligência e capacitação.

Por essa razão, governos e organizações interessadas em melhorar a resiliência de seus setores críticos devem investir, alavancar recursos e promover ferramentas e mecanismos de compartilhamento de informações. Isso inclui *inteligência militar e corporativa e treinamento de profissionais de segurança* no setor privado, militares e analistas do setor público. Com efeito, para prever ataques potenciais ou identificar riscos prontamente, é fundamental compartilhar informações de forma colaborativa por meio de plataformas de recursos que ajudem a acessar e trocar dados entre todas as partes interessadas.

Essas medidas podem, por sua vez, servir de base para sistemas de previsão estratégica e de alerta precoce, que são de enorme valor para a gestão de risco. As corporações militares e do setor privado podem compartilhar conhecimentos, recursos, protocolos e processos, com vistas a prever, avaliar e mitigar perigos que possam afetar setores sistemicamente relevantes. *Gerenciamento e análise de dados* podem oferecer perspectivas úteis sobre eventos atípicos, permitindo respostas oportunas. Isto é de grande relevância pois, mesmo que governos e empresas privadas invistam em medidas estruturais para aumentar a resiliência de infraestruturas críticas, sempre haverá riscos de elevada imprevisibilidade. Na verdade, isso implica um paradoxo: alguns riscos podem ser tão improváveis que as partes interessadas não invistam recursos para a prontidão de resposta; porém, caso o risco se torne iminente, será tarde demais para gerar uma resposta adequada.

Outra prioridade identificada é o aumento da prontidão e da consciência da sociedade frente a tais riscos. Consequentemente, será útil *implementar um sistema de gestão de crises e exercícios de preparação para emergências* com a participação de diferentes partes interessadas. Estes exercícios são importantes não só para gerar e aprimorar competências, mas também para ajudar a aumentar a compreensão do público sobre os diferentes tipos de ameaça e como responder a uma eventual crise. Por esse motivo, é fundamental envolver a mídia e a sociedade civil na condução dos exercícios de gerenciamento de crises.

Idealmente, essas práticas deveriam *envolver várias partes interessadas a nível nacional e transnacional* para testar coordenação, comunicação, capacidade de resposta, planos de contingência conjuntos e como as empresas privadas, militares e outras partes interessadas podem garantir níveis de continuidade em caso de emergência. Conforme mencionado anteriormente, além da dimensão da segurança cibernética, outras crises merecem atenção, como aquelas que podem resultar de desastres naturais, ataques extremistas e terroristas. O potencial de reforço mútuo desses eventos e riscos também deve ser destacado durante os exercícios.

Adicionalmente, *parcerias do setor privado com governos e suas forças armadas podem ajudar a construir redes e pontes de comunicação* com as principais organizações da

minimise vulnerability and ways to respond when a crisis emerges that jeopardises critical infrastructure.

Given the rising focus on cyber threats, companies from the information and technology sector receive most of the attention. However, the comprehensive approach and civil-military cooperation transcend this sector. The increasing digitalisation and employment of artificial intelligence to automatise industrial, commercial, and service-oriented processes entail a transversal impact for all sectors in terms of hybrid threats. At the same time, military organisations depend on private contractors. Therefore, it is also relevant to *develop protocols for data protection and security*, especially in times when those sectors are particularly vulnerable due to crises or attacks.

Finally, just like in any other mission, when involving armed forces in the protection of critical infrastructures, it is important to *ensure civilian control and oversight over military engagement and cooperation with the private sector.* Certainly, besides joining efforts in intelligence and risk assessment, the military can also use its capabilities to safeguard the physical integrity of infrastructure. However, depending on the context and types of destabilising factors and threats, this can potentially lead to abuses in the use of force if it is not regulated and subject to democratic control and management. Indeed, the recent experience in countries like Chile and Colombia has shown how governments have resorted to the military in response to demonstrators blocking roads. Even though the bottlenecks caused by such protests severely impact diverse critical sectors —including the supply of basic and public goods, access to health services—, the measures and state response must be proportionate and respectful of the legitimate right to protest.

In general, the protection of critical infrastructure is in the interest of homeland and global security, but also in the interest of business continuity. The increasing interconnectedness between sectors crucial to the functioning of nations and the transnational nature of many of the value chains of the companies behind them make it necessary to adopt holistic perspectives to contribute to social and economic resilience. In this effort, civil-military cooperation, involving the armed forces and the private sector, is of vital importance.

sociedade civil e multiplicadores, para aprimorar a *educação e conscientização* sobre os riscos, sobre como minimizar a vulnerabilidade e maneiras de responder quando surgir uma crise que coloque em risco a infraestrutura crítica.

Dado o foco crescente nas ameaças cibernéticas, as empresas do setor de informação e tecnologia são as que têm atraído mais atenção. No entanto, a abrangência da cooperação civil-militar transcende esse setor. A crescente digitalização e uso de inteligência artificial para automatizar processos industriais, comerciais e de serviços tem um impacto transversal com ameaças híbridas afetando todos os setores. Ao mesmo tempo, as organizações militares dependem de fornecedores privados. Portanto, é relevante *desenvolver protocolos para proteção e segurança de dados*, sobretudo num momento em que tais setores encontram-se particularmente vulneráveis a crises ou ataques.

Finalmente, como em qualquer outra missão, ao envolver as forças armadas na proteção de infraestruturas críticas, é importante *garantir o controle e supervisão civil sobre o envolvimento e a cooperação militar com o setor privado*. Certamente, além de agregar esforços de inteligência e avaliação de risco, os militares também podem usar suas capacidades para salvaguardar a integridade física da infraestrutura. Entretanto, dependendo do contexto e dos tipos de fatores desestabilizadores e ameaças, pode haver abusos no uso da força, caso esta não seja regulada ou sujeita a controle e gestão democráticos. De fato, a experiência recente em países como Chile e Colômbia demonstrou como os governos recorreram aos militares na resposta aos manifestantes que bloqueavam estradas. Ainda que os gargalos causados por tais protestos afetassem severamente diversos setores críticos — inclusive o fornecimento de bens públicos básicos e o acesso aos serviços de saúde —, as medidas e a resposta do Estado devem ser proporcionais, respeitando o direito legítimo de manifestação.

Em geral, a proteção de infraestruturas críticas é de interesse para a segurança interna e global, mas também para a continuidade dos negócios. A crescente interconexão entre setores cruciais para o funcionamento das nações e a natureza transnacional de muitas das cadeias de valor das empresas por trás delas exigem a adoção de perspectivas holísticas que contribuam para a resiliência social e econômica. Nesse esforço, a cooperação civil-militar, envolvendo as Forças Armadas e o setor privado, é de vital importância.

Sources consulted and recommended

BAUBION, C. OECD risk management: strategic crisis management. **OECD Working Papers on Public Governance 23**. 2013. Retrieved from: https://www.oecd-ilibrary.org/docserver/ 5k41rbd1lzr7-en. pdf?expires=1622824656&id=id&accname=guest&checksum=FEF49E39C7B65ECB26392CD3CA2AD9FA Accessed 2 June 2021.

BORCHERT, H.; FORSTER, K. Homeland Security and the Protection of Critical Energy Infrastructures: A European Perspective. In: BRIMMER, E. (Ed.). **Five Dimensions of Homeland and International Security**. Washington D.C., US, Center for Transatlantic Relations, 2008. p. 133–148. ISBN 0-9801871-0-9.

CARR, M. Public–private partnerships in national cyber-security strategies. **International Affairs**, v. 92, n. 1, p. 43–62, 2016.

COMMISSION OF THE EUROPEAN COMMUNITIES. Critical Infrastructure Protection in the fight against terrorism. Brussels. 2004. Retrieved from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF Accessed 2 June 2021.

KAPLAN, R.S.; LEONARD, H.B.; MIKES, A. The risks you can't foresee. **Harvard Business Review**. 2020. Retrieved from: https://hbr.org/2020/11/the-risks-you-cant-foresee Accessed 12 May 2021.

LIMNÉLL, J. Countering hybrid threats: role of private sector increasingly important. Shared responsibility needed. **Hybrid CoE Strategic Analysis 6**. 2018. Retrieved from: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis-6-Limnell.pdf Accessed 31 May 2021.

PAIVA, I. National defense policy and the protection of the critical energy infrastructure in Brazil. **Austral. Brazilian Journal of Strategy & International Relations**, v. 5, n. 10, p. 173-198. 2016.

RÜHLE, M.; ROBERTS, C. Enlarging NATO's toolbox to counter hybrid threats. 2021. Retrieved from: https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html Accessed 2 June 2021.

WIGELL, M.; MIKKOLA, H.; JUNTUNEN, T. Best practices in the whole-of-society approach in countering hybrid threat. European Parliament. 2001. Retrieved from: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf Accessed 2 June 2021.

OECD - Organisation for Economic Co-operation and Development. Recommendation of the Council on the Governance of Critical Risks. 2014. Retrieved from: https://www.oecd.org/gov/risk/Critical-Risks-Recommendation.pdf Accessed 2 June 2021.

Fontes consultadas e recomendadas

BAUBION, C. OECD risk management: strategic crisis management. **OECD Working Papers on Public Governance 23**. 2013. Obtido de: https://www.oecd-ilibrary.org/docserver/5k41rbd1lzr7-en.pdf?expires=1622824656&id = id&accname = convidado&checksum = FEF49E39C7B65ECB26392CD3CA2AD9FA Acesso em: 2 de junho de 2021.

BORCHERT, H.; FORSTER, K. Homeland Security and the Protection of Critical Energy Infrastructures: A European Perspective. *Em*: BRIMMER, E. (Ed.). **Five Dimensions of Homeland and International Security**. Washington DC, EUA, Center for Transatlantic Relations, 2008. p. 133–148. ISBN 0-9801871-0-9.

CARR, M. Public–private partnerships in national cyber-security strategies. **International Affairs**, v. 92, n. 1, p. 43–62, 2016.

COMMISSION OF THE EUROPEAN COMMUNITIES. Critical Infrastructure Protection in the fight against terrorism. Bruxelas. 2004. Obtido de: https://eur concepts/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF Acesso em: 2 de junho de 2021.

KAPLAN, RS; LEONARD, HB; MIKES, A. Os riscos que você não pode prever. **Harvard Business Review**. 2020. Obtido de: https://hbr.org/2020/11/the-risks-you-cant-foresee Acesso em: 12 de maio de 2021.

LIMNÉLL, J. Countering hybrid threats: role of private sector increasingly important. Shared responsibility needed. **Hybrid CoE Strategic Analysis 6**. 2018. Obtido de: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis-6-Limnell.pdf Acesso em: 31 de maio de 2021.

PAIVA, I. National defense policy and the protection of the critical energy infrastructure in Brazil. **Austral. Revista Brasileira de Estratégia & Relações Internacionais**, v. 5, n. 10, pág. 173–198. 2016.

RÜHLE, M.; ROBERTS, C. Enlarging NATO's toolbox to counter hybrid threats. 2021. Obtido de: https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html Acesso em: 2 de junho de 2021.

WIGELL, M.; MIKKOLA, H.; JUNTUNEN, T. Best practices in the whole-of-society approach in countering hybrid threat. European Parliament. 2001. Obtido de: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf Acesso em: 2 de junho de 2021.

OECD - Organisation for Economic Co-operation and Development. Recommendation of the Council on the Governance of Critical Risks. 2014. Obtido de: https://www.oecd.org/gov/risk/Critical-Risks-Recommendation.pdf Acesso em: 2 de junho de 2021.

Jorge M. Lasmar

Jorge M. Lasmar (PhD, London School of Economics) É docente de Relações Internacionais na PUC Minas, Brasil. É Codiretor da Rede Colaborativa de Pesquisa em Terrorismo, Radicalização e Crime Transnacional (TRAC) e Diretor de Assuntos Jurídicos da Associação Internacional de Estudos de Segurança e Inteligência, INASIS.

Jorge M. Lasmar (PhD, London School of Economics) is a professor of International Relations at PUC Minas, Brazil. He is the co-director of the Collaborative Network on Terrorism, Radicalization and Transnational Crime (TRAC) and the Legal Director of the International Association for the Studies of Security and Intelligence, INASIS.

O novo ambiente global de risco e o constante aumento da complexidade do nexo civil-militar: Novas regras, vulnerabilidades e papéis

The New Global Risk Environment and the Increasingly Complex Civil-Military Nexus: New Rules, Vulnerabilities and Roles

Jorge M. Lasmar

Resumo

Mudanças estruturais pós guerra fria aumentaram o risco no sistema internacional. A isto, acrescentou-se a recente crise da Covid-19, com a expansão da percepção do risco global, incluindo ameaças múltiplas, difusas e inéditas, cada uma criando um número maior de elementos desconhecidos e rupturas no sistema. Ademais, o ambiente de risco destas novas crises globais também revela vulnerabilidades que podem ser discretamente exploradas em mobilizações de guerra híbrida para afetar nocivamente inimigos/rivais e causar rupturas sistêmicas capazes de solapar a confiança em instituições sociais e governamentais — tudo sem o emprego de força militar convencional. Este novo risco deixa menos claro o nexo civil-militar e tem impacto sobre o processo global de gestão de risco. Portanto, faz-se necessária uma reavaliação do(s) papel(papéis) das forças armadas na gestão de crises globais, uma vez que requisitos, práticas e normas funcionais essenciais de guerra também começam a sofrer o impacto destas mesmas mudanças.

Executive summary

Post-Cold War structural changes have augmented risk in the international system. This has been further compounded by the recent Covid-19 crisis with the perception of global risk expanding to include multiple, diffused and unprecedented threats, each generating a greater number of unknowns and disruptions in the system. Furthermore, the risk environment of these new global crises also reveals vulnerabilities that can be discreetly exploited in hybrid warfare engagements to adversely affect enemies/rivals and cause systemic disruptions capable of undermining trust in social and governmental institutions — all without the employment of conventional military force. This new risk environment blurs the civil-military nexus and impacts the global risk management process. Thus, a re-assessment of the role(s) of the armed forces in global crisis management is required as key functional requisites, practices, and norms of warfare also begin to be impacted by these changes.

In this context, this paper first introduces the OECD's innovative model of risk crisis management before exploring the varied impact on and of the military in this process. New global crises are unprecedented and/or have discreet effects thus lacking a clear operational picture. The OECD risk assessment model recommends re-designing existent tools for risk identification, crisis preparedness and crisis management. As crises become global, responses need to be networked and focussed on capacity building rather than scenario planning. Traditional early warning techniques require re-shaping to develop strategic foresight capabilities and a multidisciplinary intelligence network capable of engaging in sense-making processes. However, the necessity of a networked response also blurs the civil/military divide as the requirement to mobilise different stakeholders and use new communication strategies arise. Thus, it is critical to understand, operate in and respond to this new crisis environment because it augments the risk of new forms and spaces of 'societal warfare', which operates in the Gray zone between war and peace.

Context and Importance of the Problem

Post-Cold War structural changes have augmented risk in the international system. This has been further compounded by the recent Covid-19 crisis and the perception of global risk expanding to include multiple, diffused, and unprecedented threats, each generating a greater number of unknowns and disruptions in the system. As the COVID-19 pandemic demonstrated, the increase in the quantity and intensity of both licit and illicit transnational flows, the interdependent growth, the more complex informational and cyber environment as well as the increasingly intricate global supply chain have all enhanced global vulnerabilities and provided ideal conditions for the emergence of massively disruptive global crises.

Thus, the current risk environment also provides new fertile ground for both ill-intentioned state and non-state actors who maliciously exploit these structural vulnerabilities when forwarding their agenda. On the one hand, this impacts global order as states sway away from open direct competition on common domains and move towards advancing their own systems, supply chains, networks, investments, etc. This means that both great powers and states traditionally seen as weaker states — and thus outside great power competition — are increasingly developing selective offensive capabilities outside the conventional use of force. On the other hand, this environment also nurtures the capacity of non-state actors to disrupt and destabilise states. These changes demand a new adaptive geopolitics and crisis management response.

This is relevant because not only are we witnessing an increasing use of greatly disruptive Gray zone tactics by an expanding number of malicious actors, but also due to the fact that many of these actions are stealthy in nature. As these tactics do not openly employ conventional military forces, they usually either stay below the threshold of conventional response or are just simply not detected in a timely manner. Additionally, within a crisis management scenario, these tactics no longer allow for a

Neste contexto, o presente trabalho apresenta o modelo inovador de gestão de risco de crises da OCDE antes de explorar os variados impactos sobre os militares e dos militares neste processo. As novas crises globais não têm precedentes e/ou têm efeitos discretos e, portanto, não apresentam um quadro operacional claro. O modelo de gestão de risco da OCDE recomenda reprojetar as ferramentas existentes para a identificação de risco, prontidão para crises e gestão de crises. À medida que as crises se tornam globais, as respostas devem ser articuladas e devem focar na construção de capacidades em vez de focar no planejamento por cenários. As técnicas tradicionais de alerta precoce devem ser reformuladas para desenvolver capacidades de previsão estratégica e uma rede de inteligência multidisciplinar capaz de se engajar em processos de construção de sentido. No entanto, a necessidade de uma resposta articulada em conjunto também deixa menos clara a divisão civil/militar à medida que surge a necessidade de mobilizar diferentes partes interessadas e utilizar novas estratégias de comunicação. Assim, são essenciais a compreensão e saber navegar e responder ao novo ambiente de crise, pois este aumenta o risco de novas formas e espaços de "guerra social" que operam na zona cinzenta entre guerra e paz.

Contexto e importância do problema

Mudanças estruturais pós guerra fria aumentaram o risco no sistema internacional. A isto, acrescentou-se a recente crise da Covid-19, com a expansão da percepção do risco global, incluindo ameaças múltiplas, difusas e sem precedentes, cada uma criando um número maior de elementos desconhecidos e rupturas no sistema. Como a pandemia de Covid-19 demonstrou, o aumento na quantidade e intensidade de fluxos transnacionais lícitos e ilícitos, o crescimento interdependente, o ambiente mais complexo de informações e cibernético, bem como uma cadeia de suprimentos global cada vez mais intrincada, contribuíram para aumentar as vulnerabilidades globais e apresentaram condições ideais para o surgimento de crises globais extremamente disruptivas.

Desta forma, o atual ambiente de risco também apresenta novo solo fértil para atores estatais e não estatais mal-intencionados que exploram maliciosamente tais vulnerabilidades estruturais ao avançar com sua agenda. Por um lado, há um impacto na ordem global, pois os estados afastam-se da competição aberta e direta em domínios comuns, indo em direção ao avanço de seus próprios sistemas, cadeias de suprimentos, redes, investimentos etc. Isto significa que tanto grandes potências quanto Estados tradicionalmente vistos como Estados mais fracos — e, portanto, fora da grande competição por poder — estão, cada vez mais, desenvolvendo capacidades ofensivas seletivas fora do uso convencional da força. Por outro lado, este ambiente também reforça a capacidade de atores não estatais de promover perturbações e desestabilizar os Estados. Estas mudanças demandam uma nova geopolítica adaptativa e respostas de gestão de crises.

A relevância disto se deve a estarmos testemunhando o uso cada vez mais intenso de táticas disruptivas na zona cinzenta por um número crescente de atores maliciosos e também devido ao fato de que muitas destas ações têm natureza furtiva. Por estas táticas não empregarem forças militares convencionais, geralmente ficam abaixo do limiar de resposta convencional, ou simplesmente não são detectadas de maneira oportuna.

civil/military division of work based on the "kinetic/non-kinetic" distinction. Although these tactics are not a novelty in themselves, the changes in the environment have favoured not only known tactics of discreet offensive actions such as cyber access and disruption operations, but also silent hybrid warfare engagements designed to adversely affect enemies/rivals by causing systemic disruptions capable of undermining the trust in the target's social and governmental institutions, i.e., "efforts to manipulate or disrupt the information foundations of the effective functioning of economic and social systems" (Mazarr et al, 2019, xii). Thus, these actors are increasingly gaining the ability to silently trigger global crises and undermine states.

Thus, it is critical that the European and South American armed forces develop their capacity to understand, operate and respond in this new crisis environment. This goes beyond the existing models of multidimensional crisis management as the new environment augments the risk of new forms and spaces of "societal and cognitive warfare" that blurs, even further, the increasingly Gray zone between war/peace. As this new risk environment dims the civil-military nexus and impacts the global risk management process, the armed forces should re-assess their role(s) in global crisis management as key functional requisites, practices, and norms of warfare also begin to be impacted by these same changes.

Critique of policy option(s)

As the European and South American crisis-management experience in bodies such as the United Nations, NATO, European Union, and OECD makes it clear, dealing with a systemic crisis requires a complex risk management structure. This structure includes tools for risk identification and crisis preparedness, response teams and policies for crises management as well as mechanisms to evaluate the crisis afterwards (feedback and lessons learned).

In this model, effective crisis management begins even before the crisis. Identifying threats and adequately preparing for them is essential to mitigate the potential consequences of a crisis. Hence, the first step to prepare for a large-scale disruptive crisis is to do a risk assessment (OECD, 2013). Traditional risk assessment approaches are built using "sectoral analysis based on historical events" (OECD, 2013). This means that the entire crisis preparation and identification framework must first be divided into specific sectors (industrial, economic, sanitary, military, etc.) and be based on other historical events of the same type (OECD, 2013). In other words, to predict, identify and prepare for crisis, states build preparedness structures dedicated exclusively to dealing with specific crisis based on the experience of past events. This preparedness can be found across all levels — from the strategic to the operational — in both European and South American armed forces. Specifically, in the case of Brazil, its National Defence Policy, its Military Strategic Planning, the Ministry of Defence's Defence Scenario 2020-2030, as well as the Army's Technical Methodological Manual of Risk Management are all examples of strategic and operational documents that follow such logic.

Ademais, em um cenário de gestão de crise, estas táticas não permitem mais uma divisão de trabalho civil/militar baseada na distinção "cinética/não cinética". Apesar de tais táticas não serem novidade por si mesmas, as mudanças no ambiente favoreceram táticas conhecidas de ações ofensivas discretas como acesso cibernético e operações disruptivas, e também mobilizações silenciosas de guerra híbrida projetadas para afetar negativamente inimigos/rivais com rupturas sistêmicas capazes de solapar a confiança nas instituições sociais e governamentais, ou seja, "esforços para manipular ou perturbar as bases de informações do funcionamento efetivo de sistemas econômicos e sociais" (Mazarr et al, 2019, xii). Assim, estes atores estão, cada vez mais, adquirindo a capacidade de silenciosamente disparar crises globais e solapar Estados.

Portanto, é essencial que as forças armadas europeias e sul-americanas desenvolvam sua capacidade de compreensão, operação e resposta a este novo ambiente de crise. Isto se estende para além dos modelos existentes de gestão multidimensional de crise, pois o novo ambiente aumenta o risco de novas formas e espaços de "guerra social e cognitiva", que deixa ainda menos clara a zona cinzenta entre guerra/paz. Por este novo ambiente ofuscar o nexo civil-militar e ter impacto sobre o processo global de gestão de risco, as forças armadas devem reavaliar seu(s) papel (papéis) na gestão de crises globais, uma vez que requisitos, práticas e normas funcionais essenciais de guerra também começam a sofrer o impacto destas mesmas mudanças.

Crítica sobre opções de políticas

Conforme evidenciado pelas experiências europeia e sul-americana de gestão de crises em organismos como a ONU, a OTAN, a União Europeia e a OCDE, lidar com uma crise sistêmica requer uma estrutura complexa de gestão de riscos. Tal estrutura inclui ferramentas para identificação de riscos e prontidão para crise, equipes de resposta e políticas para gestão de crises, assim como mecanismos de avaliação pós-crise (*feedback* e lições aprendidas).

Neste modelo, uma gestão de crise eficiente principia antes mesmo da própria crise. A identificação de ameaças e a preparação adequada para elas são essenciais para mitigar as consequências potenciais de uma crise. Neste sentido, o primeiro passo preparatório para uma crise disruptiva de larga escala é a realização de uma avaliação de risco (OCDE, 2013). As abordagens tradicionais de avaliação de risco são elaboradas a partir de "análises setoriais baseadas em eventos históricos" (OCDE, 2013). Isto significa que todo o marco de preparação e identificação da crise deve ser primeiramente dividido em setores específicos (industrial, econômico, sanitário, militar etc.) e se basear em outros eventos históricos do mesmo tipo (OCDE, 2013). Em outras palavras, para a previsão, identificação e preparação para crises, os Estados constroem estruturas de prontidão dedicadas exclusivamente a lidar com crises específicas, baseados na experiência de eventos passados. Esta prontidão pode ser encontrada em todos os níveis — do estratégico ao operacional — nas forças armadas europeias e sul-americanas. Especificamente no caso do Brasil, a Política de Defesa Nacional, o Planejamento Estratégico Militar, o Cenário de Defesa 2020-2030 do Ministério da Defesa, e o Manual Técnico da Metodologia de Gestão de Riscos são todos exemplos de documentos estratégicos e operacionais que seguem esta lógica.

However, the actions of the South American and European armed forces in the fight against the COVID-19 pandemic demonstrate how global, transboundary, crises have systemic cascading effects rendering the sectorial approach inappropriate in some cases. Simultaneously, the new structural environment in which the crisis was embedded made it difficult to adopt measures based on past events. Thus, crises of this nature require a different risk assessment approach to be able to deal more effectively with both uncertainty and complexity (OECD, 2013). In these cases, it is necessary to develop and design a National Defence Policy and Military Strategic Planning with a broader view of risk. In other words, it is necessary to understand that there are multiple threats, a great number of unknowns and that any threat can trigger cascade effects in other areas (OECD, 2013). This broader view of risk assessment cannot be restricted to just one sector as it requires a systemic view. Thus, armed forces must also coordinate with other stakeholders such as private companies and NGOs — and not only during the crisis. This means moving beyond the concept of Civil-Military Cooperation (CIMIC) that tends to be restricted to the operational framework of crisis management or even further than the European Union's concept of Civil-Military Coordination (CMCO) as it would imply that civil military coordination should also happen both before and after any crisis starts.

Traditionally, once the risk has been identified, the next step is to develop an action plan. This is especially important when the risk identified has either a high probability of occurrence or a significant consequence. Based on their previous experience, armed forces generally plan for traditional crisis emergencies based on scenarios. In this technique, each armed force develops a series of response protocols that must be adopted if a certain situation arises. This scenario-based planning depends directly on a fixed chain of command and predetermined procedures designed to deliver the right response at the right time. For example, the protocols that Brazil developed during the 2016 Olympic Games and the 2014 Football World Cup in the event of a terrorist attack scenario; or, in the case of the European Union (EU), the multiple overseas operations undertaken across Europe, Africa, and Asia using available civilian and military instruments (for instance, EUCAP Sahel Niger, EU NAVFOR MED, EUBAM RAFAH, EUAM Ukraine, etc.). However, global crisis no longer allows for always planning based on fixed scenarios and protocols. The uncertainty of contemporary crises and the fact that they are unprecedented require approaches that are more flexible and capable of better adapting to the threat as it evolves. A practical example of this idea is NATO's concept of the Capability Development Process (CDP), which has been internalised by several European and South American countries, including by Brazil's Ministry of Defence. In the case of Brazil, this is becoming apparent in what is a clear shift from a threat-based planning approach to a method grounded in capabilities-based planning. There are various other initiatives to restructure the Defence System in South America in order to adopt the CDP. Argentina's Military Capabilities Project (PROCAMIL) is another example of a move towards a capabilities-based response that draws upon the CDP. This convergence amongst South American armed forces can be an instrumental first step towards the formation of an integrated system of the region's defence capabilities and can even foster a transatlantic interoperability. In this sense, the European experience with its Common Security and Defence Policy can be of invaluable assistance to Latin America, aiding it to further advance the on-going

No entanto, as ações das forças armadas europeias e sul-americanas no combate à pandemia de Covid-19 demonstram como crises globais, transfronteiriças, causam efeitos em cascata sistêmicos que, em alguns casos, tornam inadequada a abordagem setorial. Concomitantemente, o novo ambiente estrutural em que a crise se inseriu dificultou a adoção de medidas baseadas em eventos passados. Assim sendo, crises desta natureza demandam uma abordagem distinta de avaliação de risco para poder lidar mais efetivamente com incertezas e complexidades (OCDE, 2013). Nestes casos, faz-se necessário o desenvolvimento e a elaboração de uma Política Nacional de Defesa e de um Planejamento Estratégico Militar com uma visão mais abrangente do risco. Em outras palavras, é necessário compreender que há múltiplas ameaças, um número grande de elementos desconhecidos, e que qualquer ameaça pode disparar efeitos em cascata em outras áreas (OCDE, 2013). Esta visão mais abrangente da avaliação de risco não pode se restringir a apenas um setor, pois é necessária uma visão sistêmica. Portanto, as forças armadas devem agir em coordenação com outras partes interessadas, como empresas privadas e ONGs — e não apenas durante a crise. Isto significa ir além do conceito de Cooperação Civil-Militar (CIMIC), que tende a se restringir ao marco operacional da gestão de crise, ou ir além até mesmo do conceito de Coordenação Civil-Militar (CMCO) da União Europeia, pois implica que a coordenação civil-militar também deveria acontecer antes de e após o início de qualquer crise.

Tradicionalmente, uma vez identificado o risco, o passo seguinte é a elaboração do plano de ação, especialmente importante quando o risco identificado tem uma elevada probabilidade de ocorrer ou tem uma consequência relevante. Com base em experiências prévias, as forças armadas geralmente preparam planos para emergências em crises baseados em cenários. De acordo com esta técnica, cada força armada elabora uma série de protocolos de respostas que deverão ser adotados no caso da deflagração de determinada situação. Este planejamento baseado em cenários depende diretamente de uma cadeia de comando fixa e de procedimentos predeterminados elaborados para aplicar a resposta no momento oportuno. Por exemplo, os protocolos elaborados pelo Brasil durante os Jogos Olímpicos de 2016 e a Copa do Mundo de Futebol de 2014 para o caso de um cenário de atentado terrorista; ou, no caso da União Europeia (UE), as múltiplas operações internacionais realizadas na Europa, África e Ásia usando instrumentos civis e militares disponíveis (por exemplo, EUCAP Sahel Niger, EU NAVFOR MED, EUBAM RAFAH, EUAM Ucrânia etc.). No entanto, a crise global não comporta mais planejamentos sempre baseados em cenários e protocolos fixos. As incertezas das crises contemporâneas, e o fato de elas não terem precedentes, demandam abordagens mais flexíveis e capazes de melhor adaptação às ameaças à medida que estas evoluem. Um exemplo prático desta ideia é o conceito de Processo de Desenvolvimento de Capacidades (CDP) da OTAN, internalizado por muitos países europeus e sul-americanos, inclusive pelo Ministério da Defesa brasileiro. Isto está ficando aparente, no caso do Brasil, na evidente mudança de uma abordagem de planejamento baseada em ameaças para um método ancorado no planejamento baseado em capacidades. Há várias outras iniciativas de reestruturação do Sistema de Defesa na América do Sul para a adoção do CDP. O Projeto de Capacidades Militares da Argentina (PROCAMIL) é outro exemplo, inspirado no CDP, de direcionamento para respostas baseadas em capacidades. Esta convergência nas forças armadas sul-americanas pode ser um primeiro passo fundamental na direção da formação de um sistema integrado das capacidades de defesa da região, e pode até promover a interoperabilidade transatlântica. Neste sentido, a experiência europeia com sua Política Comum de Segurança e Defesa pode ser

re-design of individual defence and crisis management systems as well as contributing to the formation of a Latin American/Transatlantic integrated system of defence capabilities. Europe has a long experience harmonizing divergent European military cultures, institutional practices and views, as well as a long tradition of civil-military coordination as it is a specific requirement of the European Union (Lisbon Treaty, art. 43). These are experiences that can be leveraged by Latin American countries.

Hence, planning for current crises requires building a response network whose focus is on capacity building rather than scenario planning (OECD, 2013). Consequently, the armed forces must also focus on leadership, innovation capacity and systems that allow cooperation to prepare for new crises. Therefore, it is important to establish, within the formal chain of command and structure, a crisis-management system based on the coordination of scalable clusters of civilian and military specialists capable of: 1) timely identifying a threat and what is needed to face it; 2) evaluating existing and needed resources, capabilities and options vis-à-vis the threat; and 3) implementing the chosen options within an integrative framework (Leite, 2011).

Therefore, it is also necessary to establish activation mechanisms that can trigger the response to a novel crisis. The traditional policy is the development of early warning systems that detect the occurrence of a threat and quickly initiate the response protocols. These systems are able to identify threats through intense monitoring and information sharing, such as natural disaster monitoring systems, for example (OECD, 2013). New crises, however, due to their diffuse nature and the speed with which they arise, are often not necessarily detected by traditional means of early warning. These novel situations call for the development of strategic foresight capabilities in order to perceive and identify the weak signs present at the beginning of a crisis that often go unnoticed. To develop such capabilities, the armed forces should set up a multidisciplinary intelligence network and rapid alert systems, such as the European ARGUS, linked with the responsible strategic and operational body of each force and under the integrative command and control from the Ministry of Defence.

This predicament aggravates yet another problem of the initial response to new crises. Traditionally, at the beginning of the crisis, those involved in its management construct what is termed the "operational picture". In traditional crises, the operational picture is drawn through an accurate monitoring of the development of the crisis. In other words, the armed forces and agencies involved identify the dimension of the problem, estimate its reach and impact, predict how it can evolve and plan the authorities' responsibilities in the response process (OECD, 2013). Nonetheless, because new crises are unprecedented or have discreet effects, they may not present a clear operational picture. Their threats and effects are diffuse, fast and unprecedented. The armed forces, thus, need to be prepared to engage in a sense-making process to first understand what is actually happening and how big the problem is (OECD, 2015). For that, it is necessary to lay the normative, structural and procedural foundations of a sense-making culture in the armed forces. This could be done by explicitly including such a structure, awareness and principles in the respective national defence planning and national defence strategy as well as in

um auxílio valioso para a América Latina, ajudando a Região a avançar ainda mais na reestruturação de sistemas individuais de defesa e gestão de crises, e também contribuindo para a formação de um sistema integrado latino-americano/transatlântico de capacidades de defesa. A Europa tem vasta experiência na harmonização de culturas militares, práticas e visões institucionais europeias divergentes, e uma extensa tradição de coordenação civil-militar, sendo este um requisito específico da União Europeia (Tratado de Lisboa, art. 43). Estas iniciativas podem ser implementadas por países latino-americanos.

Portanto, o planejamento para as crises atuais requer a construção de uma rede de respostas cujo foco esteja na construção de capacidade em vez de focar no planejamento por cenários (OCDE, 2013). Consequentemente, para se preparar para as novas crises, as forças armadas devem concentrar-se também em liderança, capacidade de inovação e sistemas que permitam a cooperação. Assim, é importante estabelecer, dentro da cadeia formal de comando e estrutura, um sistema de gestão de crises baseado na coordenação de grupos escaláveis de especialistas civis e militares capazes de: 1) identificação oportuna de uma ameaça e do que é necessário para enfrentá-la; 2) avaliação de recursos, capacidades e opções existentes e necessários em face à ameaça; e 3) implementação das opções escolhidas dentro de um quadro integrativo (Leite, 2011).

Portanto, é também necessário implementar mecanismos de ativação que possam acionar a resposta a uma nova crise. A política tradicional é o desenvolvimento de sistemas de alerta precoce que detectem a ocorrência de uma ameaça e rapidamente iniciem os protocolos de resposta. Estes sistemas são capazes de identificar ameaças por meio de um monitoramento intenso e compartilhamento de informações, tais como sistemas de monitoramento de desastres naturais, por exemplo (OCDE, 2013). No entanto, devido à sua natureza difusa e à velocidade com que surgem, as novas crises não são necessariamente detectadas com frequência por meios tradicionais de alerta precoce. Estas novas situações exigem o desenvolvimento de capacidades de previsão estratégica a fim de perceber e identificar os mais tênues sinais, presentes no início de uma crise, que frequentemente passam despercebidos. Para desenvolver tais capacidades, as forças armadas devem implementar uma rede de inteligência multidisciplinar e sistemas de alerta rápido, como o sistema europeu ARGUS, conectado ao órgão estratégico e operacional de cada força e sob o comando e controle integrativo do Ministério da Defesa.

Esta situação agrava outro problema da resposta inicial a novas crises. Tradicionalmente, no princípio da crise, as partes envolvidas em sua gestão montam o que se denomina "quadro operacional". Nas crises tradicionais, o quadro operacional é traçado por meio de monitoramento preciso do desenvolvimento da crise. Em outras palavras, as forças armadas e as agências envolvidas identificam a dimensão do problema, estimam seu alcance e impacto, preveem como pode evoluir e planejam as responsabilidades das autoridades no processo de resposta (OCDE, 2013). Contudo, pelo fato de as novas crises não terem precedentes ou terem efeitos discretos, podem não apresentar um quadro operacional claro. Suas ameaças e efeitos são difusos, rápidos e inéditos. Portanto, as forças armadas precisam estar preparadas para iniciar um processo de construção de sentido para, primeiramente, entender o que realmente está acontecendo e qual é a dimensão do problema (OCDE, 2015). Para tanto, é necessário estabelecer o arcabouço normativo, estrutural e procedimental de uma cultura de construção de sentido nas forças armadas. Isto pode ser

the more operational military documents and doctrines such as FMs and Technical Methodological Manuals of Risk Management. Given the complexity of the new crisis and the difficulties in engaging in sense-making and allocating the scarce resources, once again we have the need for designing a more permanent civil-military coordination structure formed by flexible stand-by clusters that form and connect according to operational and strategic needs even before the crisis begins. In all cases, NATO's CDP, elements of which are being incorporated by several Latin American armed forces, provides an excellent blueprint of exactly such capability building based not only on civil-military cooperation, interoperability but also on a hybrid and decentralised response to an emerging risk.

These examples also point to another key factor in crisis management: leadership. Implementing an integrated and coordinated response network requires trust and resilience. Leadership is essential in this process as it is key to mobilise the different stakeholders and communicate with civil society (OECD, 2013). To manage the population's trust and expectations, military and civil leaders must constantly communicate with the public during the crisis. In traditional communication approaches, leaders usually update the status of the crisis, provide technical information and inform about the measures being adopted (OECD, 2013). Although this communication with civil society is still very important, such an approach is not enough to deal with crises arising within the new information environment. In view of the characteristic uncertainties of new crises, adjusting expectations and building trust is essential for good leadership. To be able to achieve this, communications must not only inform about the state of affairs but must also transmit values to the audience and manage anxieties. The military leadership, thus, has a key role in this process as it must convey sincerity, stability and competence in order to manage civil society's ever-changing expectations. This is a process called "meaning making" (OECD, 2015). In order to establish successful communication during crisis, military leaders must make extensive use of new communication strategies, tools and vehicles. This is not only because social media has a broader reach but also because it is precisely in this environment that the greatest amount of misinformation is spread (OECD, 2015). Global crises now occur in an environment in which information (and disinformation) flows quickly and in a decentralised manner. This has a double effect. On the one hand, it allows relevant information about the crisis to quickly reach a significant number of people. On the other hand, it also allows disinformation to be disseminated. State and non-sate actors disseminate disinformation using varying methods and degrees of sophistication. This wide spectrum of disinformation can bring short and long-term risks that can be potentially fatal. Another related aspect enhanced by social media is the need for leaders to be accountable. Military and civil leaders must respond adequately to civil society's demands and expectations related to the crisis (OECD, 2015). New communication tools allow the population to conduct a more intense and detailed scrutiny of each measure adopted by the authorities. This is why the armed forces must increasingly pay attention to external communications and the use of social media and other types of communication. Leaders need to transmit to the audience the fundamental confidence and serenity needed in times of crisis as accountability becomes an ever more sensitive issue due to the intense scrutiny that the new informational environment allows.

alcançado por meio da inclusão explícita de tal estrutura, consciência e princípios nos respectivos planejamentos e estratégias nacionais de defesa e nos documentos e doutrinas militares mais operacionais, tais como MFs e Manuais Técnicos da Metodologia de Gestão de Riscos. Dada a complexidade das novas crises e as dificuldades para o engajamento na construção de sentido e na alocação dos recursos escassos, mais uma vez, tem-se a necessidade de elaborar uma estrutura civil-militar de coordenação mais permanente, formada por grupos flexíveis de prontidão que se formem e se conectem de acordo com necessidades operacionais e estratégicas antes mesmo de a crise ter início. Em todo caso, o CDP da OTAN, cujos elementos estão sendo incorporados por várias forças armadas latino-americanas, é um excelente exemplo deste exato desenvolvimento de capacidades baseado não somente na cooperação e interoperabilidade civil-militar, como também em uma resposta híbrida e descentralizada a um risco emergente.

Estes exemplos também indicam outro fator-chave na gestão de crise: liderança. A implementação de uma rede de respostas integradas e coordenadas requer confiança e resiliência. A liderança é essencial neste processo, pois é uma chave para a mobilização das diferentes partes interessadas e a comunicação com a sociedade civil (OCDE, 2013). Para administrar a confiança e as expectativas da população, líderes militares e civis devem comunicar-se constantemente com o público durante a crise. Nas abordagens tradicionais de comunicação, os líderes normalmente apresentam uma atualização sobre o status da crise, fornecem informações técnicas e informam sobre as medidas que estão sendo adotadas (OCDE, 2013). Apesar de esta comunicação com a sociedade civil ainda ser muito importante, tal abordagem não é suficiente para lidar com as crises que surgem no novo ambiente de informação. Em face das incertezas características das novas crises, ajustar as expectativas e conquistar a confiança é essencial para uma boa liderança. Para que isto seja alcançado, as comunicações, além de informar sobre o estado da situação, também devem transmitir valores e administrar as ansiedades do público. A liderança militar, portanto, tem um papel-chave neste processo, pois deve transmitir sinceridade, estabilidade e competência para administrar as expectativas em constante mudança da sociedade civil. Este processo é chamado de "construção de significados" (OCDE, 2015). A fim de estabelecer uma comunicação bem-sucedida durante a crise, líderes militares devem fazer amplo uso de novas estratégias, ferramentas e veículos de comunicação, não apenas porque a mídia social tem um alcance maior, mas também porque é precisamente neste ambiente que se dissemina a maior quantidade de desinformação (OCDE, 2015). As crises globais ocorrem agora em um ambiente no qual a informação (e a desinformação) fluem rapidamente e de forma descentralizada. Isto tem duas consequências. Por um lado, permite que informações relevantes sobre a crise rapidamente alcancem um grande número de pessoas. Por outro lado, permite a disseminação de desinformação. Atores estatais e não estatais disseminam desinformação usando vários métodos e diferentes graus de sofisticação. Este amplo espectro de desinformação pode acarretar riscos de curto e de longo prazo com o potencial de serem fatais. Outro aspecto relacionado, intensificado pela mídia social, é a necessidade da responsabilização de líderes. Líderes militares e civis devem responder adequadamente às demandas e expectativas da sociedade civil relativas à crise (OCDE, 2015). Novas ferramentas de comunicação permitem à população um escrutínio mais intenso e detalhado de cada medida adotada pelas autoridades. Por esta razão, as forças armadas devem prestar cada vez mais atenção às comunicações externas e ao uso da mídia social e outros tipos de comunicação. Os líderes precisam transmitir ao público a

Policy Recommendations

Having in mind that the current global risk environment comprises several critical geopolitical, military, environmental, societal and economic uncertainties that can develop quickly and through unforeseen ways;

Considering both the leadership role and expertise of European and South-American armed forces in multi-dimensional and comprehensive global crisis management and their close relationship and coordination with civilian actors through established CMCO (civil-military coordination) standards;

Noting that effective risk management can also be a tool of resilience and an instrument for national and regional competitive advantage;

And considering that the OECD global crisis-management model and recommendations can provide a powerful roadmap to face current challenges;

This paper recommends that — in relation to the new global crisis — the European and South American armed forces should:

I. establish and cooperate in developing a multi-dimensional, all-hazard, approach to global crises management as a tool of national resilience, preparedness and responsiveness for both continents;

To this end:

a) further their civil-military coordination experience in multidimensional crisis management acquired in operations such as the Atalanta operation in Somalia, the MINUSTAH in Haiti or even the current COVID-19 crisis;

b) review the national defence plans and strategies and other normative guidelines to explicitly adopt a comprehensive, whole-of-society approach to risk management and its communication in order to promote the effective integration of the model into the governance of the armed forces, including their decision-making processes;

c) designate strategic, tactical and operational stakeholders, from both the private and public sectors, to engage in constant revisions of the national and global risk assessments;

d) develop preparedness for the unknown and unexpected in their strategic and crisis management assessments by moving from a threat-based planning approach to a method grounded in capabilities-based planning;

II. strengthen international cooperation and develop the transatlantic interoperability in crisis management by:

a) cooperating to exchange the transatlantic experience in crisis management;

b) developing joint standard operating procedures, pre-defined emergency plans, conventional training and drills to deal with traditional global crises;

c) promoting international cooperation for setting up global risk monitoring systems and early warning systems for new, unprecedented crises;

confiança e a serenidade fundamentais necessárias em tempos de crise, pois a responsabilização torna-se uma questão cada vez mais delicada devido ao intenso escrutínio permitido pelo novo ambiente de informação.

Recomendações de políticas

Tendo em mente que o ambiente de risco global atual engloba várias incertezas críticas geopolíticas, militares, ambientais, sociais e econômicas que podem evoluir rapidamente e de maneiras imprevistas;

Considerando tanto o papel e a experiência de liderança das forças armadas europeias e sul-americanas na gestão de crises globais multidimensionais e abrangentes, quanto suas relações próximas e coordenação com atores civis através de padrões de CMCO (coordenação civil-militar);

Observando que a gestão efetiva de risco também pode ser uma ferramenta de resiliência e um instrumento de vantagem competitiva nacional e regional;

E considerando que o modelo e as recomendações de gestão de crise global da OCDE podem fornecer um poderoso mapa para enfrentar os atuais desafios;

O presente trabalho recomenda que — em relação à nova crise global — as forças armadas europeias e sul-americanas deveriam:

I. estabelecer e cooperar para o desenvolvimento de uma abordagem multidimensional, para todos os perigos, quanto à gestão de crises globais como ferramenta de resiliência nacional, prontidão e responsividade para os dois continentes;

Para tal fim:

a) ampliar sua experiência de coordenação civil-militar em gestão de crises multidimensionais adquirida em operações como a operação Atalanta na Somália, a MINUSTAH no Haiti, ou até na atual crise da Covid-19;

b) revisar os planos e estratégias nacionais de defesa e outras diretrizes normativas para que adotem explicitamente uma abordagem abrangente, incluindo toda a sociedade, quanto à gestão de risco e sua comunicação para promover a integração efetiva do modelo na governança das forças armadas, inclusive em seus processos decisórios;

c) designar partes interessadas estratégicas, táticas e operacionais dos setores público e privado para participarem de revisões constantes das avaliações de risco nacional e global;

d) desenvolver prontidão para o desconhecido e o inesperado em suas avaliações estratégicas e de gestão de crises, passando de uma abordagem de planejamento baseada em ameaças para um método ancorado no planejamento baseado em capacidades;

d) cooperating to implement a transborder network of flexible and scalable civil and military resources to improve resilience and response capabilities to new, unpredictable international crisis;

e) undertake inter-agency and international cooperation exercises;

III. further develop the European and South American strategic and intelligence capacity for concept development and risk anticipation, especially the ability to detect, observe and understand before decision makers act by:

a) creating forums, briefings and other channels for the continuously sharing of knowledge about past and current events with relevant and trusted stakeholders including the media, the third sector, academics, business associations;

b) developing a broader trusted civilian/military support network to assist decision-making, communication and emergency responses;

c) strengthening and developing early detection and "sense making" capacity through multidisciplinary, interagency systems that integrates both military and civilian knowledge and resources;

d) fostering specialised multi-disciplinary networked clusters that can be rapidly mobilised and scaled up not only for crisis response capacities, but also for "sense making" and coordination of strategic crisis management structures;

e) harmonizing and increasing the interoperability of the European and South American crisis response teams.

IV. build on previous European and South American experience with multidimensional crisis management in which the civil-military coordination model was adopted (such as MINUSTAH and Atalanta) and design a more comprehensive whole-of-society approach to risk management by also:

a) acting preventively through proactive public-private partnerships (PPPs) between the military and the civil society in order to strengthen structural and non-structural infra-structure as a mean to reduce critical risk and increase resilience;

b) identifying key capabilities and knowledge to preserve the information and systems foundations and thus guarantee the effective functioning of the economic and social systems;

c) developing networked mechanisms to quickly coordinate and mobilise resources across both governmental levels and the civil society;

d) developing an adaptive and scalable approach to crisis management by fostering a specialised network of both military and civilian specialists that can be selectively and dynamically consulted depending on the contingent characteristics of the crisis. The network can help to make sense of incomplete information, complex scenarios and respond to unprecedented crises;

e) developing and promoting shared visions of common civil/military values in the governance and management of critical risks;

II. reforçar a cooperação internacional e desenvolver a interoperabilidade transatlântica na gestão de crises através de:

a) cooperação no intercâmbio de experiências transatlânticas sobre gestão de crises;

b) desenvolvimento de procedimentos operacionais conjuntos, planos emergenciais pré-definidos, treinamentos convencionais e exercícios para lidar com crises globais tradicionais;

c) promoção de cooperação internacional para a criação de sistemas globais de monitoramento de risco e de alerta precoce para crises novas, sem precedentes;

d) cooperação para a implementação de uma rede transfronteiriça de recursos flexíveis e escaláveis civis e militares para aumentar a resiliência e capacidade de resposta a crises internacionais novas e imprevisíveis;

e) realizar exercícios de cooperação interagências e internacionais;

III. avançar no desenvolvimento da capacidade estratégica e de inteligência europeia e sul-americana para o desenvolvimento da conceituação e antecipação de risco, especialmente a capacidade de detectar, observar e entender antes de os tomadores de decisão agirem:

a) criando fóruns, comunicados e outros canais para o compartilhamento contínuo de conhecimento sobre eventos passados e atuais com partes interessadas relevantes e de confiança, inclusive a mídia, o terceiro setor, acadêmicos e associações empresariais;

b) desenvolvendo uma rede de apoio civil/militar mais ampla e de confiança para apoiar a tomada de decisões, comunicação e respostas de emergência;

c) reforçando e desenvolvendo capacidades de detecção e "construção de sentido" precoces através de sistemas multidisciplinares e interagências que integrem conhecimentos e recursos militares e civis;

d) fomentando grupos especializados multidisciplinares interconectados que possam ser rapidamente mobilizados e escalados não somente para capacidades de resposta a crises, mas também para a "construção de sentido" e coordenação de estruturas estratégicas de gestão de crise;

e) harmonizando e aumentando a interoperabilidade das equipes de resposta europeias e sul-americanas.

IV. incrementar a experiência europeia e sul-americana existente com gestão multidimensional de crise em que tenha sido adotado o modelo de coordenação civil-militar (como MINUSTAH e Atalanta) e elaborar uma abordagem mais abrangente, que inclua toda a sociedade, para a gestão de risco, também:

a) agindo preventivamente através de parcerias público-privadas (PPPs) proativas entre os militares e a sociedade civil para fortalecer a infraestrutura estrutural e não-estrutural como uma maneira de reduzir riscos críticos e aumentar a resiliência;

f) enhancing the capacity for risk scanning, early warning and risk assessment through PPP trusted networks to help monitor, detect and identify critical disruptions and are linked to the decision makers;

g) creating two-way communication channels between the military, the government and civilian sectors.

V. strengthening the role of the European and South American armed forces in global crisis management by:

a) strengthening the military leadership in crises by improving their communication via internet technology, including the use of social media for enhancing meaning-making communication;

b) strengthening and broadening trans-border intelligence networks;

c) investing in robust proactive surveillance, monitoring and alert networks and systems;

d) promoting both internal and international interoperability and information sharing.

In summation, new global crises are unprecedented and/or have discreet effects thus lacking a clear operational picture. As crises become global, responses need to be networked and focused on capacity building rather than scenario planning. Traditional early warning techniques require re-shaping to develop strategic foresight capabilities and a multidisciplinary intelligence network capable of engaging in sense-making processes. However, the necessity of a networked response also blurs the civil/military divide as the requirement to mobilise different stakeholders and use new communication strategies arise. Political rivalries, ideological extremism and lack of leadership negatively impacted the initial response phase and become the main drivers of the crisis themselves. Hence, the civil-military nexus on global risk management and the armed forces are increasingly entangled between politics and crisis management.

Thus, as new crises have a strong transnational, cross-border nature, unilateral and uncoordinated responses become increasingly a less effective option and demands both inter-state and civil-military cooperation. In this sense, the importance of cooperation and information sharing between different stakeholders should be an increasing concern for the armed forces. It is no longer possible to face today's crises by centralizing responses as the characteristics of the events and the environment in which they take place require hybrid, dynamic, multilevel and multisectoral actions. It is essential that all different stakeholders coordinate their preparedness and responses in order to effectively build a more resilient society and — in some cases — to simply "make sense" of the crisis. The design of a monitoring and response civil-military network that shares common values, principles and approaches amongst its members becomes increasingly important. Accordingly, it is also important that shared principles and values between the European and South American armed forces are aligned with broader scientific and technically specialised knowledge. It is equally important that the cooperation between the two continents is intensified and strengthened. As described

b) identificando capacidades e conhecimentos chave para preservar informações e as fundações dos sistemas, assim garantindo o funcionamento efetivo dos sistemas econômico e social;

c) desenvolvendo mecanismos articulados para rapidamente coordenar e mobilizar recursos nas esferas governamentais e na sociedade civil;

d) desenvolvendo uma abordagem de gestão de crise que seja adaptativa e escalável, ao fomentar uma rede especializada de especialistas civis e militares que possam ser seletiva e dinamicamente consultados, dependendo das características do contingente da crise. A rede pode ajudar a construir sentido a partir de informações incompletas, cenários complexos e responder a crises sem precedentes;

e) desenvolvendo e promovendo visões compartilhadas de valores civis/militares comuns na governança e gestão de riscos críticos;

f) aumentando a capacidade de varredura de risco, alerta precoce e avaliação de risco através de redes confiáveis de PPPs para ajudar no monitoramento, detecção e identificação de rupturas críticas, com conexão com os tomadores de decisões;

g) criando canais bidirecionais de comunicação entre os setores militar, governamental e civil.

V. reforçar o papel das forças armadas europeias e sul-americanas:

a) fortalecendo a liderança militar em crises, aprimorando sua comunicação com tecnologia de internet, incluindo o uso de mídias sociais para aprimorar comunicações de construção de significado;

b) fortalecendo e ampliando as redes de inteligência transfronteiriças;

c) investindo em vigilância proativa robusta, monitoramento e redes e sistemas de alerta;

d) promovendo interoperabilidade interna e internacional e o compartilhamento de informações.

Em suma, as novas crises globais não têm precedentes e/ou têm efeitos discretos e, portanto, não apresentam um quadro operacional claro. À medida que as crises se tornam globais, as respostas devem ser articuladas e devem focar na construção de capacidades em vez de focar no planejamento por cenários. As técnicas tradicionais de alerta precoce devem ser reformuladas para desenvolver capacidades estratégicas de previsão e uma rede de inteligência multidisciplinar capaz de se engajar em processos de construção de sentido. Contudo, a necessidade de uma resposta articulada também torna menos clara a divisão civil/militar à medida que surge a necessidade de mobilizar diferentes partes interessadas e utilizar novas estratégias de comunicação. As rivalidades políticas, o extremismo ideológico e a falta de liderança exerceram um impacto negativo sobre a fase inicial de resposta e tornaram-se os maiores impulsionadores da crise. Com isso, o nexo civil-militar sobre gestão de risco global e as forças armadas se veem cada vez mais emaranhados entre a política e a gestão de crise.

above, sense-making and meaning-making are a crucial element in the management of modern crisis. The combination of the European and South American military experience in managing complex global crises with key private and academic sector stakeholders as well as with the scientific and technical knowledge of both continents are all fundamental to obtain a broader situational awareness and resilience against the ever more common "unprecedented" global crisis.

Sources consulted or recommended

COHEN, Raphael S.; CHANDLER, Nathan; EFRON, Shira; FREDERICK, Bryan; HAN, Eugeniu; KLEIN, Kurt; MORGAN, Forrest E.; RHOADES, Ashley L.; SHATZ, Howard J.; and SHOKH, Yuliya, *The Future of Warfare in 2030: Project Overview and Conclusions***.** Santa Monica, CA: RAND Corporation, 2020.

LEITE, Márcio D. A. *Planejamento Estratégico das Forças Armadas Baseado em Capacidades: Reflexos para o Exército Brasileiro.* 60 Seminário do Livro Branco de Defesa Nacional, 2011.

MAZARR, Michael J.; BAUER, Ryan; CASEY, Abigail; HEINTZ, Sarah and MATTHEWS, Luke J., *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment*. Santa Monica, CA: RAND Corporation, 2019.

OECD. *Future Global Shocks: Improving Risk Governance.* Organization of Economic Cooperation and Development. 2011.

OECD. *OECD Risk Management: Strategic Crisis Management*. Organization of Economic Cooperation and Development. 2013.

OECD. *The Changing Face of Strategic Crisis Management.* OECD Reviews of Risk Management Policies, OECD Publishing, Paris. 2015.

WENDLING, Cécile. *The Comprehensive Approach to Civil-Military Crisis Management: A Critical Analysis and Perspective.* Institut de Recherche Stratégique de l'Ecole Militaire, IRSEM Report, Paris, 2010.

Portanto, como as novas crises têm uma forte natureza transnacional e transfronteiriça, respostas unilaterais e não coordenadas são opções cada vez menos eficientes e demandam cooperação civil-militar e entre Estados. Neste sentido, a importância da cooperação e do compartilhamento de informações entre as diferentes partes envolvidas pode ser uma questão cada vez mais importante para as forças armadas. Não é mais possível enfrentar as crises atuais centralizando as respostas, pois as características dos eventos e o ambiente em que estes ocorrem demandam ações híbridas, dinâmicas, em múltiplos níveis e multissetoriais. É essencial que todas as diferentes partes envolvidas coordenem sua prontidão e resposta para efetivamente construir uma sociedade mais resiliente e — em alguns casos — para simplesmente "compreender" a crise. Torna-se cada vez mais importante a elaboração de uma rede civil-militar de monitoramento e resposta que compartilhe valores, princípios e abordagens comuns entre seus membros. Assim sendo, também é importante que os princípios e valores comuns entre as forças armadas europeias e sul-americanas estejam alinhados com conhecimentos científicos e tecnicamente especializados mais amplos. É igualmente importante que a cooperação entre os dois continentes se intensifique e se fortaleça. Conforme descrito acima, a construção de sentido e a construção de significado são elementos cruciais na gestão de crises modernas. A combinação das experiências militares europeias e sul-americanas na gestão de crises globais complexas com as principais partes envolvidas dos setores privado e acadêmico e também com o conhecimento científico e técnico dos dois continentes são fundamentais para a obtenção de uma consciência situacional mais ampla e resiliência contra as crises globais "sem precedentes" cada vez mais comuns.

Fontes consultadas ou recomendadas

COHEN, Raphael S.; CHANDLER, Nathan; EFRON, Shira; FREDERICK, Bryan; HAN, Eugeniu; KLEIN, Kurt; MORGAN, Forrest E.; RHOADES, Ashley L.; SHATZ, Howard J.; and SHOKH, Yuliya, *The Future of Warfare in 2030: Project Overview and Conclusions*. Santa Monica, CA: RAND Corporation, 2020.

LEITE, Márcio D. A. *Planejamento Estratégico das Forças Armadas Baseado em Capacidades: Reflexos para o Exército Brasileiro*. 6º Seminário do Livro Branco de Defesa Nacional, 2011.

MAZARR, Michael J.; BAUER, Ryan; CASEY, Abigail; HEINTZ, Sarah and MATTHEWS, Luke J., *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment*. Santa Monica, CA: RAND Corporation, 2019.

OCDE. *Future Global Shocks: Improving Risk Governance.* Organization of Economic Cooperation and Development. 2011.

OCDE. *OECD Risk Management: Strategic Crisis Management*. Organization of Economic Cooperation and Development. 2013

OCDE. *The Changing Face of Strategic Crisis Management.* OECD Reviews of Risk Management Policies, OECD Publishing, Paris. 2015.

WENDLING, Cécile. *The Comprehensive Approach to Civil-Military Crisis Management: A Critical Analysis and Perspective*. Institut de Recherche Stratégique de l'Ecole Militaire, IRSEM Report, Paris, 2010.

Gilberto M. A. Rodrigues

Professor associado e coordenador do Programa de Pós-Graduação em Relações Internacionais da Universidade Federal do ABC (UFABC). Pesquisador Produtividade DT do CNPq. Foi pesquisador visitante na Universidade de Duisburg-Essen, Alemanha (Capes-Print) e *visiting scholar* (Fulbright) na Universidade de Notre Dame, USA.

Associate Professor and coordinator of the Postgraduate Program in International Relations at the Federal University of ABC (UFABC). Researcher with a Productivity Grant for Technological Development (DT) from the National Council for Scientific and Technological Development (CNPq). He was a visiting researcher at the University of Duisburg-Essen, Germany (Capes-Print) and visiting scholar (Fulbright) at the University of Notre Dame, USA.

Tadeu Morato Maciel

Pós-doutorando (PNPD/CAPES) e professor colaborador no Programa de Pós-Graduação em Estudos Estratégicos da Defesa e Segurança e na Graduação em Relações Internacionais do Instituto de Estudos Estratégicos (INEST) da Universidade Federal Fluminense (UFF).

Postdoctoral student (PNPD/CAPES) and collaborating Lecturer in the Postgraduate Program in Strategic Studies in Defence and Security and in the Graduate Program in International Relations at the Institute of Strategic Studies (INEST) at the Fluminense Federal University (UFF).

O lado oculto da lua: fatores desagregadores das missões de paz para as relações civis-militares brasileiras

The hidden side of the Moon: disruptive factors of peace missions for Brazilian civil-military relations

Gilberto M. A. Rodrigues
Tadeu Morato Maciel

Resumo executivo

O lado visível das missões de paz desperta interesse de internacionalistas e diplomatas envolvidos na prevenção e resolução de conflitos. Diante do perfil multidimensional das missões da ONU no pós-Guerra Fria, a promoção da paz inclui assistência às diversas causas ambientais, políticas, econômicas e socioculturais dos conflitos. Esse cenário tem exigido que o componente militar das missões potencialize suas competências para além dos combates diretos, envolvendo negociações com a sociedade civil, as autoridades governamentais e a diplomacia. Para Desch (1999), a atuação em missões de paz traz importantes benefícios para as relações civis-militares de países que passaram por uma transição recente de regimes autoritários para governos democráticos. Em contrapartida, Dwyer (2015) e Kenkel (2021) problematizam a capacidade que essas experiências teriam para contribuir com o controle civil em relação aos militares nos países de origem. Sobre o Brasil, Hoelscher e Norheim-Martinsen (2014) afirmam que a participação de militares nas pacificações no Rio de Janeiro, em sinergia com a

Executive summary

The visible side of peacekeeping missions is what draws the attention of internationalists and diplomats involved in conflict prevention and resolution. Given the multidimensional nature of UN missions in post-Cold War days, promoting peace includes attending to various environmental, political, economic and sociocultural causes of conflict. This scenario has required that the military component of missions increase their competence level beyond direct combat, to include negotiation skills with civil society, government authorities and diplomacy. According to Desch (1999), acting in peace missions brings important benefits to civil-military relations in countries that have recently transitioned from authoritarian regimes to democratic governments. In contrast, Dwyer (2015) and Kenkel (2021) doubt that these experiences contribute to civilian control over the military in their countries of origin. About Brazil, Hoelscher and Norheim-Martinsen (2014) state that the participation of military personnel in peacekeeping operations in Rio de Janeiro, in synergy with the experience of the UN mission in Haiti (MINUSTAH), are

a symptomatic example of the Latin American military tradition of interfering in public order management, thus hindering the consolidation of the Brazilian democracy. During the Bolsonaro administration (2019-), the leading role of military Ministers belonging to the "Haiti Group" showed how Brazil's military participation in MINUSTAH was more important as an experiment in public security actions, than as a way of strengthening Rule of Law values (RODRIGUES; MACIEL, 2019). The central question posed by this policy paper is: do peace missions contribute to civil-military relations in Brazil? Based on a literature review, the authors first analyse the "hidden side of the Moon", that is, how Brazilian military participation in peace missions have had a disruptive effect on civil-military relations in the domestic context; and, finally, they recommend actions to mitigate such effects.

Context and relevance of the issue

On the visible side of the Moon, lunar landscapes can be seen with the naked eye, thus arousing curiosity and feeding the imagination of scientists, poets and romantics. Similarly, the apparent legacy of peace missions mobilises a growing interest on the part of experts and policy makers dealing with multilateral issues associated with the promotion of peace. Observers have noted that, in the 1990's, the supply and demand mechanism of peace operations started to change, moving from chapter VI (peacekeeping) to chapter VII (peace enforcement) of the UN Charter, in the context of so-called "stabilisation" missions. Since the defence of impartiality presented the UN with the dilemma of standing idly by and watching the massacres in Rwanda, Somalia, and Bosnia, there was more room for the use of force, as well as for aid and state reform actions. Human rights began to gain normative ground, pointing to a movement in which the predominance of the rights of States in relation to those of individuals was challenged. Not coincidentally, humanitarian motivations have been increasingly used in the justifications for UN intervention, such as the responsibility to protect.

Part of this trend was included in the report *An Agenda for Peace* presented by Secretary General Boutros-Ghali in 1992. In this document, peace operations are seen as the first stage of the pacification and reconstruction process of fragile societies, providing "support for the transformation of weak national structures and *capabilities* and for the strengthening of new democratic institutions" (UNITED NATIONS, 1992). The United Nations Stabilisation Mission in Haiti (MINUSTAH), in operation from 2004 to 2017, is one of the prime examples of the multidimensional and militarised stance taken by peace operations.

Haiti's vulnerabilities, instabilities, and violence were used to revive the argument, in force since the early 1990's (especially by members of the North Atlantic Treaty Organisation - NATO), that it was a "bankrupt state" in need of "recovery" through joint intervention by the international community (FUKUYAMA, 2005). This is because the fragility of the Haitian State would make it "vulnerable" to new threats of the so-called global governance (such as human rights violations).

However, at that time, the main international forces interested in stabilising Haiti (especially the US) were more prone to concentrating their efforts on direct action in

experiência na missão da ONU no Haiti (MINUSTAH), seria um exemplo sintomático da tradição militar latino-americana de intervir na gestão da ordem pública, o que poderia prejudicar a consolidação da democracia brasileira. Na gestão Bolsonaro (2019-), o protagonismo dos ministros militares do "Grupo do Haiti" indica que a atuação militar brasileira na MINUSTAH foi mais importante como terreno de experimentação para ações de segurança pública do que para o fortalecimento de valores comprometidos com o Estado de Direito (RODRIGUES; MACIEL, 2019). A pergunta central deste *policy paper*: as missões de paz contribuem para as relações civis-militares no Brasil? A partir de revisão bibliográfica e consulta a fontes primárias, os autores analisam o "lado oculto da lua", ou melhor, os efeitos desagregadores da participação de militares brasileiros em missões de paz no que tange às relações civis-militares em âmbito doméstico e recomendam ações alternativas para mitigá-los.

Contexto e importância do problema

No lado visível da lua, podem ser vistas a olho nu as paisagens lunares que provocam a curiosidade e alimentam o imaginário de cientistas, poetas e românticos. De forma semelhante, o legado aparente das missões de paz mobiliza o crescente interesse de especialistas e *policy makers* envolvidos nos temas multilaterais associados à promoção da paz. Os observadores das mudanças tanto na oferta quanto na demanda das operações de paz puderam notar como, a partir dos anos 1990, elas avançaram do capítulo VI (manutenção da paz) para o capítulo VII (imposição da paz) da Carta da ONU, no contexto das chamadas missões de "estabilização". Tendo em vista que a defesa da imparcialidade colocava a ONU diante do dilema de assistir, de forma inerte, aos massacres em Ruanda, Somália e Bósnia, houve maior espaço para o emprego da força, além de ações assistenciais e de reforma do Estado. Os direitos humanos começaram a ganhar terreno normativo, apontando para um movimento no qual se contestava a predominância dos direitos dos Estados em relação àqueles inerentes aos indivíduos. Não por acaso, motivações humanitárias estiveram cada vez mais presentes nas justificativas de intervenções da ONU, a exemplo da *responsabilidade de proteger.*

Parte dessa tendência constava no relatório *Uma Agenda para a Paz*, apresentado pelo Secretário-Geral Boutros-Ghali em 1992. Nesse documento, as operações de paz são vistas como um primeiro estágio do processo de pacificação e reconstrução de sociedades fragilizadas, possibilitando "o suporte à transformação de estruturas e *capabilities* nacionais deficientes e para o fortalecimento de novas instituições democráticas" (UNITED NATIONS, 1992). A Missão das Nações Unidas para Estabilização do Haiti (MINUSTAH), vigente entre 2004 e 2017, é um dos exemplos mais sintomáticos do perfil multidimensional e militarizado assumido pelas operações de paz.

As vulnerabilidades, instabilidades e violências que o Haiti atravessava foram utilizadas para a retomada do argumento, vigente desde o início da década de 1990 (especialmente por parte de membros da Organização do Tratado do Atlântico Norte - OTAN), de que aquele era um "Estado falido", que precisava ser "recuperado" por meio de uma intervenção conjunta da comunidade internacional (FUKUYAMA, 2005). Isto porque a fragilidade do Estado haitiano o tornaria "sensível" às novas ameaças à chamada governança global (tais como as violações de direitos humanos).

other regions of the world. One of the most prominent examples was Afghanistan, which suffered an intervention by the US and its NATO allies in 2001, in response to the terrorist attacks of September 11 of that year. From 2002 onwards, Afghanistan was also a stage for UN action, through the United Nations Assistance Mission in Afghanistan (UNAMA). Unlike MINUSTAH, this was a political mission, without peacekeeping forces, requested by the government of Afghanistan to help establish peace and development.

Like Haiti, Afghanistan was considered a typical case where problems resulted from state bankruptcy. According to some analysts and policymakers (FUKUYAMA, 2005) it required a comprehensive process of State (re)construction. In both cases, the extensive presence of foreign military forces pervaded the reconstruction efforts, with an emphasis on security objectives. The focus on counterinsurgency, as practiced by NATO in Afghanistan, contributed to the militarisation of stabilisation missions like MINUSTAH (KENKEL, 2021). While the mission in Afghanistan was conducted by NATO military forces, the presence of Latin American countries in the Haiti peace mission was described as the most appropriate solution for a multidimensional mission in that Caribbean country.

Armed with the discourse of "non-indifference" and "diplomacy of solidarity" (HIRST, 2012), Brazil presented itself as a major player and led the military component of the UN peace operation in Haiti. The performance of Brazilian military forces throughout the duration of MINUSTAH has encouraged debates about the effects of this mission on civil-military relations at home. The robust use of force in this type of stabilisation mission tends to enhance the armed forces' tendency to act at the national level. That, in turn, may heighten difficulties for civilian control over military actions in their countries of origin.

Criticism of political choices

In 2004, when MINUSTAH was created, Secretary General Kofi Annan released a report evaluating the UN's experiences and challenges in promoting justice and the Rule of Law in conflict and post-conflict societies. The report highlighted the urgent need for restoring the Rule of Law, stressing that "justice, peace and democracy are not mutually exclusive objectives, but rather mutually reinforcing imperatives" (UNITED NATIONS, 2004a, p. 1). In this document, the Rule of Law was described as "a principle of governance in which all persons, institutions and entities, public and private, including the State itself, are accountable to laws that are publicly promulgated, equally enforced and independently adjudicated, and which are consistent with international human rights norms and standards" (UNITED NATIONS, 2004a, p. 4).

In the same report, the Haiti mission was included in the list of operations that would have important aspects involving the Rule of Law. In experiences such as MINUSTAH, the military component engages in a wide range of tasks related to guaranteeing the Rule of Law, which fragile States such as Haiti would not be able to ensure. Resolution 1,542 (2004) of the Security Council, which officially established MINUSTAH, states that one of its functions is "to support the Transitional Government as well as Haitian human rights institutions and groups in their efforts to promote and protect human

Todavia, naquele momento, as principais forças internacionais interessadas na estabilização do Haiti (especialmente os EUA) estariam mais inclinadas a despender esforços com atuações diretas em outras regiões do mundo. Um dos principais exemplos era o Afeganistão, que sofreu uma intervenção dos EUA e seus aliados da OTAN em 2001, em resposta aos ataques terroristas de 11 de setembro daquele ano. A partir de 2002, o Afeganistão também foi palco para a atuação da ONU, por meio da Missão de Assistência das Nações Unidas no Afeganistão (UNAMA). Diferente da MINUSTAH, esta era uma missão política, sem forças de manutenção da paz, criada a pedido do governo do Afeganistão para auxiliar no estabelecimento da paz e do desenvolvimento.

Em comum com o Haiti, o Afeganistão era considerado um caso paradigmático dos problemas oriundos da falência estatal, o que exigiria, na opinião de alguns analistas e *policymakers* (FUKUYAMA, 2005), um amplo processo de (re)construção de Estado. Em ambos os casos, a ampla presença de forças militares estrangeiras permeou os esforços de reconstrução, com ênfase nos objetivos de segurança. O foco na contra-insurgência, como praticado pela OTAN no Afeganistão, contribuiu para a militarização dos mandatos de estabilização, a exemplo da MINUSTAH (KENKEL, 2021). Enquanto a missão no Afeganistão era conduzida por militares da OTAN, a presença de países latino-americanos na missão de paz no Haiti era descrita como uma solução mais apropriada para a condução de uma missão de caráter multidimensional no país caribenho.

Munido com o discurso da "não indiferença" e da "diplomacia da solidariedade" (HIRST, 2012), o Brasil apresentava-se como ator de destaque no Haiti, ao liderar o componente militar da operação de paz da ONU no país. A atuação dos militares brasileiros durante toda a vigência da MINUSTAH tem fomentado debates sobre os efeitos dessa missão nas relações civis-militares em âmbito doméstico. O uso robusto da força nesse tipo de missão de estabilização tende a reforçar as tendências de atuação das Forças Armadas em âmbito doméstico, podendo amplificar, por exemplo, as dificuldades de controle civil sobre a atuação dos militares em seus países de origem.

Crítica das opções políticas adotadas

Em 2004, ano de criação da MINUSTAH, o Secretário-Geral Kofi Annan lançou um relatório no qual refletia sobre as experiências e desafios da ONU para a promoção da justiça e do Estado de Direito em sociedades em conflito ou pós-conflito. Ao destacar a urgência da restauração do Estado de Direito, o relatório ressaltava que a "justiça, paz e democracia são não objetivos mutuamente exclusivos, mas sim imperativos que se reforçam mutuamente" (UNITED NATIONS, 2004a, p. 1). Neste documento, o *rule of law* era descrito como "um princípio de governança no qual todas as pessoas, instituições e entidades, públicas e privadas, incluindo o Estado em si, devem estar sujeitos a leis que são publicamente promulgadas, implementadas de maneira equitativa e julgadas de maneira independente, e que sejam consistentes com as normas e padrões do direito internacional e dos direitos humanos" (UNITED NATIONS, 2004a, p. 4).

No mesmo relatório, a missão no Haiti é incluída nos exemplos de operações que teriam importantes componentes de mobilização do Estado de Direito. Em experiências como a MINUSTAH, o componente militar assume um rol amplo de tarefas relacionadas à

rights, particularly of women and children, in order to ensure individual accountability for human rights abuses and redress for victims" (UNITED NATIONS, 2004b).

However, how to guarantee that fundamental rights will not be violated by the mission itself, even though it should help to strengthen protection mechanisms instead? (VERDIRAME, 2011). Regarding the lack of accountability of French soldiers in the accusation of sexual abuse of minors during a peace mission in the Central African Republic, Sengupta (2015) points out that the UN has no effective legal authority to prosecute or punish a country's soldiers. Despite the organisation's announced "zero tolerance" policy for sexual abuse, for example, the implementation of accountability processes would be hampered by a complex architecture, hindered by long delays, unknown or inconclusive results, and a lack of assistance to victims.

In the case of MINUSTAH, there are still "hidden" obstacles for the mission's ability to foster the consolidation of democracy and the revitalisation of Haiti's justice system. As a negative legacy, it is worth mentioning the cholera epidemic unleashed by Nepalis in the military component of the mission, and the human rights violations committed by soldiers against the Haitian population, including women and children (SEITENFUS, 2019). For example, the case in which Pakistani troops were accused of abusing a mentally handicapped teenager made the headlines. Although the Haitian Senate approved a resolution to have the soldiers tried in Haiti, a meeting between Pakistani representatives and the mission's secretary general, Hervé Ladsous, allowed the accused to return to their country of origin. In these proceedings, the results of the UN investigation were not properly disclosed, there was no public court martial for the accused and victims were not given any compensation. Meanwhile, Pakistani troops continued to participate in peacekeeping missions.

This was not an isolated case, as MINUSTAH had one of the highest numbers of sexual abuse allegations among UN missions around the world. For example, in early 2015, MINUSTAH was responsible for 45 percent of all allegations of sexual abuse against UN troops, even though it represented less than seven percent of all peacekeeping forces at that time. Such violations resulted in the phenomenon known as "MINUSTAH babies", in view of the large number of pregnancies resulting from abuse carried out by blue helmets (JOHNSTON, 2015).

As leader of the military component, Brazil had to deal with the various allegations of human rights violations. Some of the accusations were also directed at Brazilian military personnel. Complaints filed with the Commission on Human Rights and Minorities in Brazil, reported alleged abuses by Brazilian troops in Haiti, especially in relation to the use of excess violence in occupation and policing operations of poor areas of the capital, Port-au-Prince (MACEDO, 2008). A tell-tale episode occurred in 2005, when General Augusto Heleno (Minister of the Institutional Security Office in the current Jair Bolsonaro administration) commanded a mission in the Cité Soleil neighbourhood, on the outskirts of Port-au-Prince. The operation, known as "Iron Fist", lasted about seven hours and fired over 22,000 rounds against thin-walled houses. Although the mission was considered a success by General Heleno (CASTRO; MARQUES, 2019), several human rights groups called it a massacre, claiming that dozens of civilians (including

garantia do *rule of law*, as quais os Estados considerados fragilizados como o Haiti não teriam a capacidade de assegurar. Na Resolução 1542 (2004) do Conselho de Segurança, que criou oficialmente a MINUSTAH, consta como uma de suas funções "apoiar o Governo de Transição, bem como as instituições e grupos de direitos humanos haitianos em seus esforços para promover e proteger os direitos humanos, especialmente de mulheres e crianças, a fim de garantir a responsabilidade *(accountability)* individual pelos abusos dos direitos humanos e indenização às vítimas" (UNITED NATIONS, 2004b).

Todavia, como garantir que os direitos fundamentais não serão violados pela própria missão, que deveria ajudar no fortalecimento dos mecanismos de proteção? (VERDIRAME, 2011). Sobre a falta de responsabilização de soldados franceses pela acusação de abuso sexual de menores durante a missão de paz na República Centro-Africana, Sengupta (2015) destaca que a ONU não tem efetiva autoridade legal para processar ou punir os soldados de um país. Apesar da anunciada política de "tolerância zero" da organização para abusos sexuais, por exemplo, a aplicabilidade de processos de *accountability* seria prejudicada por uma arquitetura complexa, atravessada por longos atrasos, resultados desconhecidos ou inconclusivos, e a falta de assistência às vítimas.

No caso da MINUSTAH, há entraves ainda "ocultados" quanto à capacidade da missão em favorecer a consolidação da democracia e a revitalização do sistema de justiça do Haiti. Como legado negativo, cabe destacar a epidemia de cólera desencadeada por nepaleses do componente militar da missão e as violações de direitos humanos cometidas por soldados contra a população haitiana, incluindo mulheres e crianças (SEITENFUS, 2019). Por exemplo, ganhou evidência o caso no qual tropas paquistanesas foram acusadas de abusar de um adolescente com deficiência mental. Apesar de o Senado haitiano ter aprovado uma resolução para que os soldados fossem julgados no Haiti, uma reunião entre representantes paquistaneses e o secretário-geral da missão, Hervé Ladsous, possibilitou o retorno dos acusados para o país de origem. Nesse processo, os resultados da investigação da ONU não foram devidamente divulgados, não houve corte marcial pública para os acusados e as vítimas não receberam qualquer compensação. Enquanto isso, as tropas paquistanesas continuaram a participar de missões de paz.

Tal caso não foi um exemplo isolado, visto que a MINUSTAH foi uma das maiores fontes de alegações de abuso sexual em missões da ONU em todo o mundo. Por exemplo, no início de 2015, a MINUSTAH foi responsável por 45 por cento de todas as alegações de abuso sexual contra tropas da ONU, apesar de representar menos de sete por cento de todo o contingente das missões de paz naquele momento. Tais violações resultaram no fenômeno "bebês da MINUSTAH", tendo em vista a grande quantidade de gestações resultantes de abusos realizados por capacetes azuis (JOHNSTON, 2015).

Por exercer a liderança do componente militar, o Brasil precisou lidar com as diversas denúncias de violações de direitos humanos. Parte dessas acusações eram voltadas, inclusive, a militares brasileiros, como se vê nas denúncias apresentadas à Comissão de Direitos Humanos e Minorias no Brasil, contra supostos abusos das tropas brasileiras no Haiti, especialmente em relação ao excesso de violência nas operações de ocupação e policiamento em áreas pobres da capital, Porto Príncipe (MACEDO, 2008). Um episódio sintomático ocorreu em 2005, quando o General Augusto Heleno (atual Ministro do

women and children) had died in the crossfire. Similar accusations, related to the excessive use of force, were directed at the Brazilian military during the pacification of slums in Rio de Janeiro.

The experience acquired in Haiti was essential for the subsequent pacification processes in Rio de Janeiro slums, making Brazil an important example of the synergy between peace missions and domestic stabilisation actions (MÜLLER; STEINKE, 2018). One of the most evident examples of this link occurred in 2010, during the pacification of the Complexo do Alemão and Penha communities. The "Peace Forces" were composed of approximately 800 soldiers, 60% of whom had been in MINUSTAH, and had also been deployed for public security functions, such as patrolling poor areas of Rio de Janeiro (ARAÚJO, 2010).

Harig (2015) emphasises that the legal status of the military in recent operations in the slums of Rio de Janeiro was inspired by MINUSTAH. Regarding alleged abuses by soldiers during Operation Rio, the Defence Minister at that time, Nelson Jobim, suggested that future intervention missions in slums take place under legal protection comparable to that of troops in UN peacekeeping missions. In fact, the Army had only accepted to participate in Operation Archangel, in 2010, after being assured that potential errors in soldiers' actions would not be tried in civilian courts.

The role of the Brazilian military in domestic public security actions and in UN peacekeeping missions, as well as its strong presence in the Executive Branch during the Bolsonaro administration, may help (re)produce the former image of the Army — intended primarily for the defence of national borders — as a supposedly authorised intervener in Brazilian politics. The incorporation of active and retired military officers in the Bolsonaro administration strengthens the idea of pacification as a *modus operandi* for intervention and social control. The actions of the Bolsonaro administration's first two years point to the deterioration of democratic mechanisms and institutions, and to a legalised violation of human rights. To be noted is the proposal to amend the Penal Code to include *defence of lawfulness*, a type of immunity for on-duty police and military forces acting in "For the Guarantee of Law and Order" (GLO) operations. A step back with regard to human rights is seen in both domestic and foreign policy agendas. In fact, Brazil has abandoned the progressive positions it had already consolidated at the UN, which promoted gender and migration issues, among others.

The appointment of a large number of military personnel under the administration of President Bolsonaro requires a research agenda to verify whether the intervention of the armed forces in the domestic environment has reached a new level. Brazilian-style pacification, employed under the Brazilian command of MINUSTAH, and the use of this expertise in isolated, long-lasting interventions in the domestic sphere, is at the core of President Bolsonaro's administrative vision (RODRIGUES; MACIEL, 2019). A close look at the pacification projects in Brazil is essential for the much-needed analysis of the current role of the military in the Brazilian democratic regime.

Evaluation, regulation and follow-up mechanisms are required to help verify to what extent and how external and domestic pacification/stabilisation missions are

Gabinete de Segurança Institucional do governo Jair Bolsonaro) comandou uma missão no bairro *Cité Soleil*, na periferia de Porto Príncipe. Batizada de "Punho de Ferro", a operação durou cerca de sete horas e disparou mais de 22 mil balas em meio às casas de paredes finas. Embora o General Heleno tenha considerado a missão um sucesso (CASTRO; MARQUES, 2019), vários grupos de direitos humanos a classificaram como um massacre, alegando que dezenas de civis (incluindo mulheres e crianças) morreram no fogo cruzado. Acusações semelhantes, relacionadas ao excesso do uso da força, foram direcionadas aos militares brasileiros nas pacificações de favelas do Rio de Janeiro.

A experiência adquirida no Haiti foi essencial para os posteriores processos de pacificação nas favelas cariocas, colocando o Brasil como um importante exemplo da sinergia entre missões de paz e ações domésticas de estabilização (MÜLLER; STEINKE, 2018). Um dos momentos mais evidentes dessa vinculação ocorreu em 2010, na pacificação do Complexo do Alemão e da Penha. A "Força de Paz" era formada por cerca de 800 militares, dos quais 60% participam da MINUSTAH, inclusive em funções de segurança pública, como o patrulhamento de áreas pobres da capital (ARAÚJO, 2010).

Harig (2015) ressalta que o estatuto jurídico dos militares nas recentes operações em favelas cariocas foi inspirado na MINUSTAH. Referindo-se a supostos abusos de soldados durante a Operação Rio, o então Ministro da Defesa, Nelson Jobim, sugeriu que as futuras missões de intervenção em favelas ocorressem sob proteção jurídica comparável às das tropas em missões de paz da ONU. Inclusive, o Exército somente teria aceitado participar da Operação Arcanjo, em 2010, após ter sido assegurado de que possíveis falhas de atuação dos soldados não seriam julgadas por tribunais civis.

A atuação dos militares brasileiros em ações de segurança pública doméstica e em missões de paz da ONU, e sua forte presença no poder Executivo na gestão Bolsonaro, podem ajudar a (re)produzir a antiga imagem do Exército — supostamente destinado prioritariamente à defesa extrafronteiras do País — como suposto interventor autorizado na política brasileira. A incorporação de militares da ativa e reserva na gestão Bolsonaro reforça a perspectiva da pacificação como *modus operandi* de intervenção e controle social. As ações do governo Bolsonaro, após dois anos de mandato, indicam deterioração de mecanismos e instituições democráticas e a violação legalizada dos direitos humanos. Destaca-se a proposta de alteração do código penal para permitir a *excludente de ilicitude*, modalidade de imunidade para policiais em serviço e militares atuando em operações de Garantia da Lei e da Ordem (GLO). O retrocesso na agenda governamental doméstica no que tange aos direitos humanos também se revela presente na política externa, visto que o Brasil abandonou posturas progressistas consolidadas na ONU, voltadas à defesa de questões de gênero e migrações, entre outras.

A ampla indicação de militares para a composição da gestão de Bolsonaro na Presidência da República demanda uma agenda de pesquisa que verifique se a intervenção das Forças Armadas no ambiente doméstico atingiu um novo patamar. A pacificação à brasileira, exercida durante o comando brasileiro na MINUSTAH, e a aplicação de sua expertise nas intervenções pontuais e duradouras no âmbito doméstico, está no centro nevrálgico da visão de gestão do Presidente Bolsonaro (RODRIGUES; MACIEL, 2019). Um olhar atento para os projetos de pacificação no Brasil se mostra essencial para as necessárias reflexões sobre o atual papel dos militares no regime democrático brasileiro.

connected. Peacekeeping missions are an important field for improving military diplomatic skills and training processes. For Pion-Berlin and Arceneaux (2000), for example, the military who have participated in peace missions are more "professional" and less prone to becoming involved in domestic politics. Thanks to the enhanced negotiation and management skills they acquired in foreign missions, retired and active military personnel have occupied strategic positions in the State apparatus, in posts previously held by civilians.

Moreover, the Brazilian experience in peace operations, especially in MINUSTAH, combined with the prestige the armed forces enjoy among a large segment of the population, has contributed to legitimizing an increasing militarisation of public security and the use of the armed forces for policing purposes ("policialisation") (RODRIGUES, 2016). In this sense, Sotomayor (2004) understands that military actions in Haiti did not contribute to strengthening democratic practices in Brazil or to improving civil-military relations. In several fronts, the Brazilian military might be replicating the militarised organisational practices that were triggered in peace missions (and which, in turn, had also been influenced by previous actions in the area of public security in the domestic context). This militarised action encourages a lack of accountability, whether at the individual or institutional level, in relation to excesses committed by soldiers.

Finally, this process of "policialisation" and politicisation of the military is not limited to countries in the Southern Hemisphere. It is worthwhile making a comparison with other NATO members that took part in the Afghanistan intervention (albeit one that did not reach the same level of consensus as MINUSTAH, approved by the Security Council). France was active in NATO operations in Afghanistan for 13 years and remains an important contributor to UN peacekeeping missions to this date. Nonetheless, recently, it faced public questioning by armed forces' representatives. In April and May 2021, some 2,000 retired and active-duty military (including 24 generals) wrote two open letters that said that there was a risk of civil war and threatened an intervention if the French government did not "eradicate dangers" such as Muslims and immigrants. The authors described themselves as military personnel of a younger generation, who had participated in operations abroad (such as that in Afghanistan), where they had fought the "Islamic enemy" (REIS, 2021). Although motivations differ, we find features in common with Brazil: the "fictionalisation of the enemy" (who appears as a risk to public order), the appropriation of the idea that the military are authorised interveners in the domestic environment, and the recurring violation of the "discretionary duty" by armed forces representatives.

Brazilian military experiences in peace missions served rather as an experimentation ground for public security actions, than as a form of strengthening Rule of Law values. Could we implement actions that assign to the Brazilian military the task of a democratic peacekeeper (LEVIN et. al., 2017), thus contributing to the establishment of robust democracies and the advancement of human rights in foreign as well as in domestic missions?

From the point of view of international legitimacy, UN peace operations are underpinned by the UN Charter, with the Security Council exercising control over and

Há a necessidade de mecanismos de avaliação, regulação e acompanhamento que ajudem a verificar em que medida e de que maneira se dá a conexão entre missões externas e domésticas de pacificação/estabilização. As missões de paz são um campo importante de aprimoramento das habilidades diplomáticas e dos processos de treinamento dos militares. Para Pion-Berlin e Arceneaux (2000), por exemplo, os militares que participam de missões de paz seriam mais "profissionais" e se envolveriam menos em questões políticas domésticas. Contudo, a maior capacidade de negociação e as habilidades de gestão adquiridas em missões externas têm permitido a militares da ativa e reformados uma atuação em posições estratégicas no aparelho estatal, ocupando cargos predominantemente exercidos por civis.

Além disso, a experiência brasileira em operações de paz, especialmente na MINUSTAH, em conjunto com o prestígio das Forças Armadas junto a grande parcela da população, tem contribuído com a legitimação do avanço da militarização da segurança pública e da policialização das Forças Armadas (RODRIGUES, 2016). Nesse sentido, Sotomayor (2004) entende que a atuação dos militares no Haiti não colaborou para o fortalecimento de práticas democráticas no Brasil ou para a melhoria das relações civis-militares no país. Os militares brasileiros estariam replicando em diversas frentes as práticas organizacionais militarizadas que foram acionadas em missões de paz (e que já eram, por sua vez, influenciadas por atuações precedentes na área de segurança pública em âmbito interno). Essa atuação militarizada favorece a ausência de responsabilização, seja em nível individual, seja institucional, em relação a excessos cometidos por soldados.

Por fim, esse processo de policialização e politização dos militares não se resume a países do Sul Global. Cabe uma comparação com membros da OTAN que participaram da intervenção no Afeganistão (a qual não teve uma anuência semelhante à MINUSTAH, aprovada pelo Conselho de Segurança). Recentemente, a França, que atuou nas operações da OTAN no Afeganistão por 13 anos e se mantém como importante colaboradora das missões de paz da ONU, enfrentou questionamentos públicos por parte de representantes das Forças Armadas. Em abril e maio de 2021, cerca de 2.000 militares da reserva e da ativa (incluindo 24 generais) escreveram duas cartas abertas afirmando haver o risco de uma guerra civil e ameaçaram uma intervenção caso o governo francês não "erradique perigos", tais como islâmicos e imigrantes. Os autores da carta descreveram-se como militares de uma geração mais jovem, que participou de operações no exterior (como no Afeganistão), nas quais combateram o "inimigo islâmico" (REIS, 2021). Embora existam diferentes motivações e nuances em comum com o Brasil, verifica-se a "ficcionalização do inimigo" (o qual colocaria em risco a ordem pública), a apropriação do discurso dos militares como interventores autorizados em ambiente doméstico e a violação recorrente do "dever de discrição" por parte de representantes das Forças Armadas.

As experiências de militares brasileiros em missões de paz serviram mais como locais de experimentação para ações de segurança pública do que para o fortalecimento de valores comprometidos com o Estado de Direito. Assim, seria possível estabelecer ações que associem o militar brasileiro à concepção de *peacekeeper* democrático (LEVIN et. al., 2017) que contribuiria para o estabelecimento de democracias robustas e para o avanço dos direitos humanos em missões no exterior e em ambiente doméstico?

monitoring them within a power cleavage that encompasses North-South relations, global governance and a minimum of accountability. The same cannot be said of operations under NATO mandate, especially in Afghanistan, where there is *another kind of legitimacy*, biased and built on the interests of the Northern Hemisphere, with the argument that one needs to impose *civilisation on barbarism*. In NATO's intervention in Afghanistan, the transparency of operations is notoriously reduced to a minimum in the eyes of public opinion, as is the problem of the non-disclosed use of drones in summary executions and military actions outside the protocol and norms of International Humanitarian Law.

In sum, what are the main disruptive factors of the UN peacekeeping missions, as they are kept on the hidden side of the Moon (or kept out of the spotlight for the press and public opinion)? Problem No. 1 - Impunity of security agents for crimes committed during their mandate; Problem No. 2 - Countries under the mandate of UN peacekeeping missions become laboratories for military training and sites where to put into practice states of exception, and their experience becomes potentially threatening to the democratic regime of countries in which a military state exercises historical power as arbitrator or guarantor of political institutions, especially in the Global South. Testimonials from Brazilian MINUSTAH force commanders are unanimous in highlighting the importance of participating in peace missions as a kind of training for real-life situations (CASTRO; MARQUES, 2019). However, in the case of MINUSTAH, for a Brazilian military component whose country of origin has been increasingly using the armed forces for actions of domestic control, this training occurred during domestic disturbances.

Policy recommendations

All six policy recommendations suggested by the authors aim to mitigate problems 1 and 2 above, in order to improve and strengthen the legitimacy and legality of UN peace missions, through mechanisms of transparency and non-repetition.

1 - International Public Hearings: all force commanders must take part in at least one international public hearing, organised by the UN's Department of Peacekeeping Operations (DPKO). Accredited NGOs must have free access to these hearings, which are used to report to public opinion, at the end of the mission's mandate renewal period;

2 - National Public Hearings: The military departments in charge of recruiting, preparing and deploying military personnel for peace missions must hold public hearings, with broad participation of the civil society and the press, to account for the participation of the country's military component in each UN peace mission, as a prerequisite to continue participating in new missions;

3 - Greater rigidity in the recruitment of troop contributing countries: Evaluation mechanisms by the UN must clarify and demand a reference standard for the democratic control expected of troop-contributing countries, as a way of reducing the risk of peacekeeping missions becoming incubators of authoritarian tendencies;

Do ponto de vista da legitimidade internacional, as operações de paz da ONU estão amparadas na modelagem da Carta da ONU, com o Conselho de Segurança exercendo sobre elas controle e monitoramento dentro de uma clivagem de poder que engloba as relações Norte-Sul, a governança global e um mínimo de *accountability*. O mesmo não se pode dizer das operações sob mandato da OTAN, sobretudo no Afeganistão, onde há uma *outra legitimidade*, parcial e construída com base nos interesses do Norte Global, sob o argumento da necessidade de impor *a civilização à barbárie*. Na intervenção da OTAN no Afeganistão, a transparência das operações é notoriamente reduzida ao mínimo diante da opinião pública, a exemplo da problemática sobre o uso não declarado de drones em execuções sumárias e ações militares fora do protocolo e das normas do Direito Internacional Humanitário.

Em síntese, quais são os problemas centrais que constituem fatores desagregadores das missões de paz da ONU, escondidas (ou mantidas fora dos holofotes da imprensa e da opinião pública) no "lado oculto da lua"? Problema nº 1 – impunidade dos agentes de segurança por crimes cometidos durante o mandato; Problema nº 2 – transformação dos países sob mandato de uma missão de paz da ONU em laboratórios de treinamento militar e de práticas de estados de exceção, cuja experiência se torna potencialmente ameaçadora para o regime democrático de países em que o estamento militar exerce histórico poder de árbitro ou garantidor das instituições na política, especialmente no Sul Global. Depoimentos de *force commanders* brasileiros na MINUSTAH são unânimes em destacar a importância da participação em missões de paz como forma de treinamento em situações reais (CASTRO; MARQUES, 2019). Entretanto, no caso da MINUSTAH, esse treinamento foi realizado em distúrbios internos, para um componente militar brasileiro cujo país de origem vem progressivamente utilizando as Forças Armadas para ações de controle doméstico.

Recomendações de políticas

As seis recomendações de políticas adotadas pelos autores visam a mitigar os problemas 1 e 2 mencionados, a fim de aprimorar e fortalecer a legitimidade e a legalidade das ações das missões de paz da ONU, via mecanismos de transparência e **não-repetição**.

1 - Audiências Públicas (public hearings) internacionais: todos os *force commanders* devem participar de pelo menos uma audiência pública internacional, sob os auspícios do Departamento de Operações de Paz da ONU (DPKO), de livre acesso às ONGs credenciadas, para prestar contas à opinião pública, ao fim do período de renovação de mandato da missão;

2 - Audiências públicas nacionais: Os departamentos militares encarregados do recrutamento, preparação e envio de militares para missões de paz devem realizar audiências públicas, com ampla participação da sociedade civil e da imprensa, para prestar contas da participação do componente militar do país em cada missão de paz da ONU, como condição para seguir participando de novas missões;

3 - Maior rigidez no recrutamento de países contribuintes de tropas: Deve haver a ampliação de mecanismos de avaliação por parte da ONU que explicitem e demandem

4 - Withdrawal of countries from peace missions due to human rights violations: If there is proof that human rights or humanitarian laws have been violated by a country's peacekeeping forces, that country shall enter into quarantine for at least three years, and for those three years it shall be prohibited from participating in new missions or renewing its troops in existing ones.

5 - Enhancing civil supervision mechanisms: In terms of the relationship between the armed forces and Brazilian democracy, Congress and the civil society need to collaborate further in the country's decision to join a UN peace mission. Also, there must be greater civilian access to the accountability mechanisms of military offenders.

6 -Temporary exclusion of troops-contributing countries from peace missions: Countries whose security forces have contributed to the destabilisation/change of their own country's political regime, in conflict with the Democratic Rule of Law, must be/remain excluded from missions.

Bibliographical references and recommendations

ARAÚJO, Vera. General da Brigada Paraquedista que já comandou as tropas brasileiras no Haiti vai comandar a [...]. ***O Globo***, 08 December 2010. <https://oglobo.globo.com/rio/general-da-brigada-paraquedista-que-ja-comandou-as-tropas-brasileiras-no-haiti-vai-comandar-a-2913513>. Accessed 29 August 2014.

CASTRO, Celso. MARQUES, Adriana (orgs.). *Missão Haiti: a visão dos force commanders*. Rio de Janeiro: Editora FGV, 2019.

DESCH, Michael. *Civilian Control of the Military: The Changing Security Environment***.** Baltimore: John Hopkins University Press, 1999.

DWYER, Maggie. Peacekeeping abroad, trouble making at home: mutinies in West Africa. ***African Affairs***, v. 114, n. 455, 2015, pp. 206-225.

FUKUYAMA, F. *Building States: Government and Organization in the 21st Century.* Rio de Janeiro: Rocco, 2005.

HARIG, Christoph. Peacekeeping in Haiti: A Laboratory for Pacification in Rio de Janeiro? *Strife,* May 28 2015. <http://www.strifeblog.org/2015/05/28/pea cekeeping-in-haiti-a-laboratory-for-pacification-in-rio-de-janeiro/>. Accessed 20 January 2017.

HIRST, Monica. Aspectos Conceituais e Práticos da Atuação do Brasil em Cooperação Sul-Sul: os casos de Haiti, Bolívia e Guiné-Bissau. Texto p/ Discussão 1687, IPEA, Brasília, 2012.

HOELSCHER, Kristian; NORHEIM-MARTINSEN, Per M. Urban violence and the militarization of security: Brazilian "peacekeeping" in Rio de Janeiro and Port au Prince. ***S****mall Wars & Insurgencies*, v. 25, n. 5/6, 2014, pp. 957-975.

JOHNSTON, Jake. *UN Points to MINUSTAH as "Model of Accountability" for Sexual Abuse Cases***.** CEPR - Centre for Economic and Policy Research, 27 May. 2015. < https://cepr.net/un-points-to-minustah-as-model-of-accountability-for-sexual-abuse-cases/>. Accessed 05 April 2021.

um padrão de referência de controle democrático esperado por parte dos países contribuintes de tropas, como forma de dirimir o risco das missões de paz se tornarem incubadoras de tendências autoritárias;

4 - Suspensão da participação de países em missões de paz por violações de DH: Uma vez comprovadas violações de direitos humanos ou do direito humanitário por soldados da missão de paz de um país, este deve entrar em quarentena por, no mínimo, três anos, período em que estaria vedado de participar de novas missões ou renovar suas tropas nas existentes.

5 - Ampliação dos mecanismos de supervisão civil: Quanto à relação entre Forças Armadas e a dinâmica democrática brasileira em específico, **é preciso** ampliar a capacidade do Legislativo e da sociedade civil em colaborar na decisão do país de aderir a uma missão de paz da ONU, além da ampliação de acesso civil aos mecanismos de responsabilização de militares infratores.

6 - Exclusão temporária de países contribuintes de tropas para missões de paz: Países cujas forças de segurança contribuam para a desestabilização/mudança de regime político em conflito com o Estado Democrático de Direito de seu país devem ser/permanecer excluídos das missões.

Fontes consultadas ou recomendadas

ARAÚJO, Vera. General da Brigada Paraquedista que já comandou as tropas brasileiras no Haiti vai comandar a [...]. ***O Globo***, 08 dez. 2010. Disponível em: <https://oglobo.globo.com/rio/general-da-brigada-paraquedista-que-ja-comandou-as-tropas-brasileiras-no-haiti-vai-comandar-a-2913513>. Acesso em: 29 ago. 2014.

CASTRO, Celso. MARQUES, Adriana (orgs.). *Missão Haiti: a visão dos force commanders.* Rio de Janeiro: Editora FGV, 2019.

DESCH, Michael. *Civilian Control of the Military: The Changing Security Environment*. Baltimore: John Hopkins University Press, 1999.

DWYER, Maggie. Peacekeeping abroad, trouble making at home: mutinies in West Africa. *African Affairs*, v. 114, n. 455, 2015, pp. 206-225.

FUKUYAMA, F. *Construção de Estados: governo e organização no século XXI.* Rio de Janeiro: Rocco, 2005.

HARIG, Christoph. Peacekeeping in Haiti: A Laboratory for Pacification in Rio de Janeiro? *Strife*, 28 mai. 2015. Disponível em: <http://www.strifeblog.org/2015/05/28/pea cekeeping-in-haiti-a-laboratory-for-pacification-in-rio-de-janeiro/>. Acesso em: 20 jan. 2017.

HIRST, Monica. *Aspectos Conceituais e Práticos da Atuação do Brasil em Cooperação Sul-Sul: os casos de Haiti, Bolívia e Guiné-Bissau.* Texto p/ Discussão 1687, IPEA, Brasília, 2012.

HOELSCHER, Kristian; NORHEIM-MARTINSEN, Per M. Urban violence and the militarisation of security: Brazilian "peacekeeping" in Rio de Janeiro and Port au Prince. *Small Wars & Insurgencies*, v. 25, n. 5/6, 2014, pp. 957-975.

KENKEL, Kai M. Stability abroad, instability at home? Changing UN peace operations and civil–military relations in Global South troop contributing countries. Contemporary Security Policy, vol. 42:2, 2021, pp. 225-240.

LEVIN, Jamie et al. A test of the democratic peacekeeping hypothesis: Coups, democracy, and foreign military deployments. Journal of Peace Research. Vol. 58 (3), 2020, pp. 355-367.

MACEDO, Idhelene. Direitos Humanos recebe denúncia contra tropas no Haiti. Agência Câmara de Notícias, 20 August. 2008. <https://www.camara.leg.br/noticias/121713-direitos-humanos-recebe-denuncia-contra-tropas-no-haiti/>. Accessed 15 January 2015.

MÜLLER, Frank; STEINKE, Andrea. Criminalizing encounters: MINUSTAH as a laboratory for armed humanitarian pacification, Global Crime, 19: 3-4, 2018, pp. 228-249.

PION-BERLIN, David; ARCENEAUX, Craig. Decision Maker or Decision Takers? Military Missions and Civilian Control in Democratic South America. Armed Forces and Society, n. 26, v. 3, 2000, pp. 413-426.

REIS, Paulo N. Militares franceses acusam Macron e o seu governo de "covardia" e "perversão". Publico.pt, 10.05.2021. <https://www.publico.pt/ 2021/05/10/mundo/noticia/militares-franceses-acusam-macron-cobardia-perversao-1961943>. Accessed May 12 2021.

RODRIGUES, Gilberto M. A.; MACIEL, Tadeu M. Pacificação à brasileira? O paradigma de Caxias, a Minustah e o governo de Jair Bolsonaro. Revista Brasileira de Estudos de Defesa, v. 6, n. 2. July/December. 2019, pp. 13-36.

RODRIGUES, Thiago M. S. Narcotráfico, Militarização e Pacificações: novas securitizações no Brasil. In: DOS PASSOS, R.; FUCCILLE, A. (Orgs.). Visões do Sul: crise e transformações do sistema internacional. Vol. 2, Marília: Of. Universitária, São Paulo: Cultura Acadêmica, 2016.

SEITENFUS, Ricardo. A ONU e a epidemia de cólera no Haiti. São Paulo: Alameda, 2019.

SENGUPTA, Somini. Allegations Against French Peacekeepers Highlight Obstacles in Addressing Abuse. The New York Times, May 25 2015. <https://www.nytimes.com/2015/05/26/world/europe/allegations-against-french-peacekeepers-highlight-obstacles-in-addressing-abuse.html>. Accessed 20 May 2021.

SOTOMAYOR, Arturo C. The Myth of the Democratic Peacekeeper: Civil-Military Relations and the United Nations. Baltimore: Johns Hopkins University Press, 2014.

UNITED NATIONS. An Agenda for Peace: Preventive diplomacy, peacemaking and peace-keeping. Report of the Secretary-General, adopted by the Summit Meeting of the Security Council, A/47/277, January 1992.

UNITED NATIONS. The rule of law and transitional justice in conflict and post-conflict societies. Report of the Secretary-General, S/2004/616, 2004a.

UNITED NATIONS. Resolution 1542. Security Council, S/RES/1542, 2004b.

VERDIRAM, Guglielmo. The UN and Human Rights: Who Guards the Guardians? New York: Cambridge University Press, 2011.

JOHNSTON, Jake. *UN Points to MINUSTAH as "Model of Accountability" for Sexual Abuse Cases*. CEPR – Center for Economic and Policy Research, 27 mai. 2015. Disponível em: < https://cepr.net/un-points-to-minustah-as-model-of-accountability-for-sexual-abuse-cases/>. Acesso em: 05 abr. 2021.

KENKEL, Kai M. Stability abroad, instability at home? Changing UN peace operations and civil–military relations in Global South troop contributing countries. *Contemporary Security Policy*, vol. 42:2, 2021, pp. 225-240.

LEVIN, Jamie ***et al***. A test of the democratic peacekeeping hypothesis: Coups, democracy, and foreign military deployments. *Journal of Peace Research*. Vol. 58 (3), 2020, pp. 355-367.

MACEDO. Idhelene. Direitos Humanos recebe denúncia contra tropas no Haiti. *Agência Câmara de Notícias*, 20 ago. 2008. Disponível em: <https://www.camara.leg.br/noticias/121713-direitos-humanos-recebe-denuncia-contra-tropas-no-haiti/>. Acesso em: 15 jan. 2015.

MÜLLER, Frank; STEINKE, Andrea. Criminalising encounters: MINUSTAH as a laboratory for armed humanitarian pacification, ***Global Crime***, 19: 3-4, 2018, pp. 228-249.

PION-BERLIN, David; ARCENEAUX, Craig. Decision Maker or Decision Takers? Military Missions and Civilian Control in Democratic South America. *Armed Forces and Society*, n. 26, v. 3, 2000, pp. 413-426.

REIS, Paulo N. Militares franceses acusam Macron e o seu governo de "cobardia" e "perversão". *Publico.pt*, 10.05.2021. Disponível em: <https://www.publico.pt/ 2021/05/10/mundo/noticia/militares-franceses-acusam-macron-cobardia-perversao-1961943>. Acesso em: 12 mai. 2021.

RODRIGUES, Gilberto M. A.; MACIEL, Tadeu M. Pacificação à brasileira? O paradigma de Caxias, a Minustah e o governo de Jair Bolsonaro. *Revista Brasileira de Estudos de Defesa*, v. 6, n.2. jul./dez. 2019, pp. 13-36.

RODRIGUES, Thiago M. S. Narcotráfico, Militarização e Pacificações: novas securitizações no Brasil. In: DOS PASSOS, R.; FUCCILLE, A. (Orgs.). *Visões do Sul: crise e transformações do sistema internacional.* Vol. 2, Marília: Of. Universitária, São Paulo: Cultura Acadêmica, 2016.

SEITENFUS, Ricardo. *A ONU e a epidemia de cólera no Haiti.* São Paulo: Alameda, 2019.

SENGUPTA, Somini. Allegations Against French Peacekeepers Highlight Obstacles in Addressing Abuse. *The New York Times,* 25 mai. 2015. Disponível em: <https://www.nytimes.com/2015/05/26/world/europe/allegations-against-french-peacekeepers-highlight-obstacles-in-addressing-abuse.html>. Acesso em: 20 mai. 2021.

SOTOMAYOR, Arturo C. *The Myth of the Democratic Peacekeeper: Civil-Military Relations and the United Nations*. Baltimore: Johns Hopkins University Press, 2014.

UNITED NATIONS. *An Agenda for Peace: Preventive diplomacy, peacemaking and peace-keeping.* Report of the Secretary-General, adopted by the Summit Meeting of the Security Council, A/47/277, January 1992.

UNITED NATIONS. *The rule of law and transitional justice in conflict and post-conflict societies.* Report of the Secretary-General, S/2004/616, 2004a.

UNITED NATIONS. *Resolution 1542*. Security Council, S/RES/1542, 2004b.

VERDIRAME, Guglielmo. *The UN and Human Rights: Who Guards the Guardians?* New York: Cambridge University Press, 2011.

Veronica F. Azzi

Veronica F. Azzi é pesquisadora de pós-doutorado na Escola de Ciências Sociais da Fundação Getúlio Vargas. Doutora e Bacharel em Relações Internacionais pela PUC-Rio. Sua pesquisa foca a área de segurança, principalmente Forças Armadas, militarização, pacificação e fragilidade estatal.

Veronica F. Azzi is a postdoctoral researcher at the School of Social Sciences at Fundação Getúlio Vargas. She holds a PhD and Bachelor's degree in International Relations from PUC-Rio. Her research focuses on the area of security, mainly the Armed Forces, militarization, pacification and State fragility.

Marcelo M. Valença

Marcelo M. Valença é professor adjunto na Escola de Guerra Naval (EGN). Doutor em Relações Internacionais e Bacharel em Direito. Sua pesquisa opera na convergência entre o Direito e a Política Internacional, principalmente no campo da Segurança e da Política Externa.

Marcelo M. Valença is adjunct professor at the Naval War College (EGN). He holds a PhD in International Relations and a Bachelor's degree in Law. His research focuses on the convergence between Law and International Politics, mainly in the field of Security and Foreign Policy.

Ameaças transnacionais, violência estrutural e militarização: promovendo a cooperação civil-militar para a construção da paz

Transnational threats, structural violence and militarization: promoting civil-military cooperation for peacebuilding

Veronica F. Azzi
Marcelo M. Valença

Introdução

A preocupação das agendas políticas internacionais e dos formuladores de políticas públicas na área da segurança com as chamadas "novas ameaças" não é recente. O termo vem sendo utilizado para conjugar diferentes tipos de eventos que desafiam instituições, interesses e valores nacionais, englobando temas como meio ambiente, desenvolvimento, migração e crimes transnacionais, cada qual demandando respostas específicas para a sua solução. Tais ameaças, classificadas como novas, se potencializam diante do denominador comum de que sua origem é normalmente atribuída ao exterior dos Estados, fora das fronteiras nacionais. Por um lado, a combinação de uma origem externa à ameaça ao seu potencial de afetar a segurança e ordem nacionais faz com que formuladores de políticas públicas e analistas busquem assegurar prioridade e senso de urgência na resolução dessas questões.

Por outro lado, a atual conjuntura de ausência de guerras interestatais em um ambiente pós-Guerra Fria alicerçado no sistema ONU de segurança coletiva vem contribuindo para uma recente tendência de militarização das respostas a esses

Introduction

The so-called "new threats" have been a concern of international political agendas and public policy makers in the security area for quite some time. The term has been used in reference to various events that challenge national institutions, interests and values, including issues such as the environment, development, migration and transnational crimes, each demanding a unique response and solution. These new threats amplify one another, given the fact that they have a common source: they originate abroad, outside national borders. On the one hand, the combination of an external origin to the threat and its potential to affect national security and order makes policy makers and analysts seek to ensure priority and a sense of urgency in resolving these issues.

On the other hand, the current lack of interstate wars in a post-Cold War environment based on the UN system of collective security has contributed to the recent trend of militarised responses to these challenges. As a result, the Armed Forces have been increasingly used inside national borders, whether in humanitarian peace missions, such

as *Operação Acolhida* (Operation Welcome) in Brazil, or to support the state security apparatus, fostering governance. In this context, current security policies are faced with a challenge: although the absence of interstate wars might suggest a drastic reduction in violence at the international level, that is not what happens in reality, as violent practices are progressively being observed within national borders. The fact that the armed forces have been asked, by the executive branches of different States, to implement increasingly militarised practices of domestic surveillance and patrolling seems to point to a change into a structural pattern of violence.

The call for war — on drugs, organised crime, or foreign values that denigrate national ones — is a political rhetoric that leads to a sense of urgent response, and at the same time suggests the need to eliminate the threat by whatever means. This policy brief analyses the role played by cooperation between the armed forces and civil institutions in dealing with these new threats, as it has been frequently seen as a way of pushing away these threats and the agents that produce them.

Although the purpose of direct violent demonstrations (i.e., aggressive practices that resemble militarised actions) is to reduce violence, imposing a pacification model leads to the aggravation of pre-existing socioeconomic conditions that may, in turn, correlate with the cause that initially motivated the pacification process, thus characterizing structural violence. Such violence consists, broadly speaking, of social and/or institutional obstacles that prevent individuals from having their basic needs met. It affects society in an asymmetric way, with violence being disguised as socioeconomic inequalities that are taken for granted, based on the political discourse, expressed, for example, in the limited access to public goods and services, and justified by the idea of meritocracy.

Militarisation of security in Latin America and Europe

Although responses to these challenges may be relatively different in Latin America and Europe with regard to the nature of threats observed, both continents have in common the idea that these threats are to be eliminated by using the armed forces as part of the public security apparatus. This use is expressed based on a militarised rationale in which phenomena such as militarism, militarisation and the military operate outside the logic of war, but rooted into the social fabric with a structural violence that we shall refer to here as pacification.

Latin America and Europe have dealt with the issue of violence in a historically different way, but they are both seen as peaceful continents, where the incidence of armed conflicts is lower than in other regions of the world. Despite tensions that lasted until the 1980s between Brazil and Argentina, the Latin American regional powers have not been at war since at least the 19th century. Over the years, the region has developed a unique legal tradition that includes principles of national sovereignty, non-intervention and peaceful dispute resolution, thus avoiding foreign intervention and the involvement of extra-regional powers backed by legal mechanisms (KACOWICZ, 2005 apud MARES; KACOWICZ, 2015, pp. 18-9) (HERZ, 2010, p. 602). Norms of sovereignty and equality between states have been deeply rooted

desafios. Dessa forma, o emprego das Forças Armadas dentro das fronteiras nacionais dos próprios Estados tem sido cada vez mais comum, seja em missões de paz de natureza humanitária como a operação Acolhida no Brasil, ou para apoiar o aparato estatal de segurança, fomentando a governança. Nesse contexto, observa-se, ao mesmo tempo, um desafio para as atuais políticas de segurança caracterizado por uma ausência de guerras interestatais que, a priori, sugeriria uma drástica redução da violência em nível internacional, mas que não denota isso, uma vez que práticas violentas vem sendo cada vez mais observadas dentro das fronteiras Estatais dos próprios Estados. Práticas cada vez mais militarizadas, de vigilância e patrulhamento internos realizados por Forças Armadas a pedido dos poderes Executivos dos Estados, parecem apontar para uma mudança no padrão da violência que é expressa através da violência estrutural.

O chamamento a uma guerra — às drogas, ao crime organizado ou a valores estrangeiros que denegrirão os pátrios — constitui retórica política que leva a um senso de urgência na reação, ao mesmo tempo em que sugere a necessidade de eliminar a ameaça com todos os meios possíveis. Este *policy brief* analisa o papel da cooperação entre forças armadas e instituições civis para lidar com essas novas ameaças, o que vem sendo comumente observado como forma de solução para afastar as mesmas e os agentes que as produzem.

Deste modo, apesar de a tendência de manifestações da violência direta, i.e., práticas de agressão que remetem a ações militarizadas, ser a de reduzir a violência, a imposição de um modelo de pacificação leva ao agravamento de condições socioeconômicas pré-existentes e que, de certa maneira, podem apresentar correlação com as causas que inicialmente motivaram o processo de pacificação, configurando elementos que caracterizam a violência estrutural. Tal violência consiste, grosso modo, em obstáculos sociais e/ou institucionais que impedem o atendimento de condições e necessidades básicas dos indivíduos. A violência incide de uma forma assimétrica na sociedade, onde se mascara sob a forma de desigualdades socioeconômicas naturalizadas pela retórica política, que se expressa, por exemplo, na limitação no acesso a bens e serviços públicos justificada por discursos de meritocracia.

A militarização da segurança na América Latina e na Europa

Ainda que as respostas dadas a esses desafios possam apresentar uma natureza relativamente diferente no caso da América Latina e da Europa no que tange à natureza das ameaças observadas nos dois continentes, ambos têm em comum o senso de eliminação dessas ameaças a partir do emprego das Forças Armadas como parte do aparato de segurança estatal. Tal emprego, por sua vez, expressa-se com base em uma lógica militarizada na qual fenômenos como o militarismo, militarização e militares operam fora da lógica da guerra, mas permeando o tecido social com uma violência estrutural que aqui chamaremos de pacificação.

Apesar de lidarem de forma historicamente distinta com a questão da violência, a América Latina e a Europa são vistos como continentes pacíficos, onde a incidência de conflitos armados é inferior a outras regiões do mundo. Apesar de tensões que perduraram até a década de 1980 entre Brasil e Argentina, as potências regionais latino-americanas não entram em guerra desde ao menos o século XIX. Ao longo dos anos, a

in the region's tradition and legal framework, and have always been present in relations between the countries. An emphasis on borders as the limits of national States, and as elements that distinguish an (inter)national environment from an autonomous domestic environment, has created a distinction in which, while one is perceived as collaborative in terms of international cooperation, the other includes, of itself, by implication, a more violent domain, with the violent use of sovereign practices to maintain order internally.

By stressing the principle of non-intervention, Latin American countries reinforce their sovereign prerogative to promote violence internally so as to maintain domestic order. This paradox leads to a strong contrast between high levels of domestic disorder and social violence (even in democratic governments), and a relative degree of peace among these states (HURRELL, 1998, p. 537). Structural violence operates in these spaces, naturalizing inequalities and social violence practices. Hence, relative peace in the region comes at the expense of high levels of domestic violence. The violence observed in Latin American civil wars is also relevant to explain international relations, raising the following question: "how can Latin American countries be so fiercely violent against domestic enemies, and yet be willing to follow international rules against foreign rivals?" (MARES; KACOWICZ, 2015, p. 16).

The tradition of defending the principle of non-interference in domestic affairs has become an essential component of the regional understanding of international security. Therefore, many challenges are faced as domestic affairs and, as such, they are free from international scrutiny. Also, the weaknesses of Latin American States, originated from structural domestic causes with high levels of social violence and deep historical roots, have been exacerbated by challenges such as drug trafficking and related crime, social inequality and marginalisation. Structural violence is a constant in Latin American development and has been reproduced in a naturalised way over the centuries. Given this trend, the state security apparatus has turned "inwards", and the State has continued to be a reference for security, (HURRELL, 1998) as related to the prevention of direct violence.

In response to the proliferation of crime since the early 1990s, Latin American countries have used military or police units composed of special forces (as in the case of BOPE in Brazil) to physically control and regain state power in many territories controlled by private players. Such actors may include criminal gangs and organised crime groups involved in drug trafficking — which, over time, took on the vacuum left by the State and used funds from illegal activities to provide public goods and services that were lacking in those locations. (FELBAB-BROWN, 2011). In Brazil specifically, such threats have been observed, to a large extent, in operations to guarantee law and order, the so-called Op GLO (acronym in Portuguese)[1], against the so-called APOP (acronym in Portuguese)[2], players that threaten law and order at the domestic level, showing how threats are interpreted in a flexible away, at the discretion of the executive branch (MINISTÉRIO DA DEFESA DO BRASIL, 2014).

[1] Operations for the guarantee of law and order.

[2] Agents against public order.

região desenvolveu uma tradição jurídica distinta que incorporou princípios de soberania nacional, não intervenção e resolução pacífica de disputas, responsável por evitar a intervenção estrangeira e o envolvimento de poderes extrarregionais, respaldados por mecanismos legais (KACOWICZ, 2005 *apud* MARES; KACOWICZ, 2015, pp. 18-9) (HERZ, 2010, p. 602). Dessa forma, as normas de soberania e de igualdade entre estados foram fortemente inscritas na tradição da região, no arcabouço legal que lá se desenvolveu e no que tange às relações entre os países da mesma. A ênfase nas fronteiras como limites dos Estados nacionais como elementos que distinguem um ambiente (inter)nacional de um ambiente doméstico autônomo criou uma distinção na qual, enquanto um é retratado como colaborativo em termos da cooperação internacional, o outro inclui, por si só, por implicação, um domínio mais violento, onde se observa o exercício violento de práticas soberanas para a manutenção da ordem internamente.

Ao frisar o princípio da não-intervenção, os países latino-americanos reforçam sua prerrogativa soberana de promover a violência internamente para a manutenção da ordem doméstica. Mesmo assim, esse paradoxo leva a uma relação de forte contraste, que se dá entre altos níveis de desordem doméstica e violência social (mesmo em governos democráticos) e um grau relativo de paz entre tais Estados (HURRELL, 1998, p. 537). A violência estrutural opera nesses espaços, naturalizando desigualdades e práticas de violência social. Dessa forma, a relativa paz na região ocorre em detrimento de altos níveis de violência internamente. A violência observada nas guerras civis latino-americanas também é relevante para explicar as relações internacionais, pois levanta a questão de "como os países latino-americanos podem ser tão sangrentos contra inimigos domésticos e ainda assim estarem dispostos a seguir regras internacionais contra rivais estrangeiros?" (MARES; KACOWICZ, 2015, p. 16).

A tradição de defesa do princípio da não-interferência em assuntos internos tornou-se um elemento constitutivo da interpretação regional do conceito da segurança internacional, resultando em um tratamento e uma classificação de muitos desafios como assuntos domésticos, que, em consequência, estão comumente livres do escrutínio internacional. Por sua vez, as fraquezas estatais dos países latino-americanos, cujas raízes estão relacionadas às causas domésticas estruturais que variam de altos níveis de violência social — com profundas raízes históricas que foram exacerbadas por desafios como o tráfico de drogas e a criminalidade a ele relacionada — à desigualdade social e marginalização. A violência estrutural é uma constante no desenvolvimento latino-americano e se reproduz, de forma naturalizada, ao longo dos séculos. Diante dessa tendência, os aparatos de segurança estatal voltaram-se mais ainda "para dentro", de forma que a referência à segurança continuou a ser o Estado (HURRELL, 1998) e a segurança, dizer respeito à prevenção da violência direta.

Em resposta à proliferação do crime desde o início da década de 1990, países latino-americanos fizeram uso de unidades militares ou polícias compostas por forças especiais (como no caso do BOPE, no Brasil) para controlar fisicamente e retomar o poder estatal de muitos territórios controlados por agentes privados. Tais atores podem incluir gangues criminais e organizações do crime organizado de tráfico — que, ao longo do tempo, assumiram o vácuo de poder estatal nesses locais e começaram a prover bens públicos na medida em que eram financiados por práticas ilícitas (FELBAB-BROWN, 2011). No Brasil,

Despite the distinctions reflected normatively in everyday life, when analysing enforcement practices within national borders, one can detect militarised security policies in which policing and the enforcement of law and order are organised by means of a series of (para)military "security forces", which some have called "politicisation of the military", concurrently with the "militarisation of the police" (GRAHAM, 2011). The involvement of the armed forces in such forms of social control sheds light on the phenomenon of "militarisation of law enforcement", which can occur even in the absence of ideological motivations (STAVRIANAKIS; SELBY, 2013). Their involvement is limited to functions traditionally assigned to the police, that is, maintaining order, so "the connection between militarisation, securitisation and mundane security practices occur in the name of counterinsurgency and public safety" (STAVRIANAKIS; STERN, 2018, p. 4).

Europe, in turn, is experiencing the longest period of peace in its history, with no major armed interstate conflicts since the end of World War II. The formation and expansion of the European Union brought an end to historical insecurities among countries, but was unable to overcome the feeling of insecurity in dealing with nationals from other regions. This image of peace and the absence of conflicts collides with prevention strategies to deter threats and maintain order that, on the one hand, prevent the incidence of direct violence, and, on the other, increase structural violence and social asymmetry.

On the European continent and in other countries of the global north, such as the United States, militarisation has manifested itself in spectacular practices of surveillance and patrolling of urban mega-events, mostly sports-related (BOYLE; HAGGERTY, 2009), as well as in issues regarding migration flows, for example. In recent years in particular, there have been changes: on the one hand, a higher degree of involvement of Latin American countries in domestic security, on the other, European interest in curbing the increase of organised crime in the continent, as well as its actions on European soil, based on a rationale of prevention against new security threats that permeate the so-called security-development nexus (ARANTZA, 2018).

The shift of international security (also) to the internal scope of States

At the end of the Cold War, a significant number of armed conflicts were domestic in nature. They differed from the traditional strategic military issues noted above, for which reason the debate on how to react to internal threats became part of international political agendas, in addition to reactions to traditional foreign threats (BUZAN; HANSEN, 2009). Furthermore, there was a shift in the literature, from war and militarism, it started to focus on security. It was in this context that the debate on securitisation took shape, "to address issues related to the limits of security, when it starts and ends and what it does or does not do". However, it was argued that the relationship between militarism and security had not been sufficiently discussed in political and academic domains. As a result, related themes, such as militarisation and

especificamente, tais ameaças vêm sendo observadas, em grande medida, em operações de garantia da lei e da ordem, as chamadas Op GLO, contra os chamados APOP[1], agentes que ameaçam a lei e a ordem em nível doméstico, o que evidencia uma interpretação de ameaça maleável, a critério do Executivo (MINISTÉRIO DA DEFESA DO BRASIL, 2014).

Apesar da diferenciação refletida normativamente no dia a dia, ao analisar práticas coercitivas no âmbito das fronteiras nacionais, torna-se possível conceber políticas de segurança militarizadas nas quais o exercício do policiamento e do cumprimento da lei e da ordem é organizado através de uma série de "forças de segurança" (para)militares, o que alguns chamaram de "policização dos militares", concomitantemente com uma "militarização da polícia" (GRAHAM, 2011). O envolvimento das Forças Armadas em tais formas do exercício do controle social traz à tona o fenômeno da "militarização do cumprimento da lei", que pode ocorrer mesmo na ausência de motivações ideológicas (STAVRIANAKIS; SELBY, 2013). Ainda que seu envolvimento esteja limitado a funções tradicionalmente atribuídas à polícia, de manutenção da ordem como função social, "a conexão entre práticas de militarização, securitização e práticas mundanas de segurança em nome da contrainsurgência e da segurança pública" (STAVRIANAKIS; STERN, 2018, p. 4).

A Europa, por sua vez, experimenta o maior período de paz de sua história, sem conflitos interestatais armados de grandes proporções desde o final da II Guerra Mundial. A formação e expansão da União Europeia permitiu a superação das inseguranças históricas entre os países, mas não foi capaz de superar o sentimento de insegurança em relação a nacionais de outras regiões. Essa imagem de paz e ausência de conflitos esbarra em estratégias de prevenção contra ameaças e de manutenção da ordem que, se, por um lado, previnem a incidência da violência direta, por outro, aumentam a violência estrutural e a assimetria social.

No continente europeu e em outros países do norte global, como os Estados Unidos, a militarização tem sido expressa em práticas espetaculares de vigilância e patrulhamento de megaeventos urbanos, em sua maioria esportivos (BOYLE; HAGGERTY, 2009), bem como em questões de fluxos migratórios, por exemplo. Nos últimos anos em especial, vêm sendo observadas mudanças, por um lado, caracterizadas por um maior grau de envolvimento dos países da América Latina na segurança doméstica, que têm demonstrado, especificamente, por outro, um interesse europeu de conter o aumento do crime organizado no continente, bem como sua atuação em solo europeu embasada em uma justificativa de prevenção contra novas ameaças de segurança que perpassam o chamado nexo de segurança-desenvolvimento (ARANTZA, 2018).

O deslocamento da segurança internacional (também) para o âmbito interno dos Estados

Ao final da Guerra Fria, parte significativa dos conflitos armados era de natureza doméstica. Dessa forma, diferiam dos assuntos militares estratégicos tradicionais observados anteriormente e, por isso, o debate sobre como reagir a ameaças internas passou a fazer parte das agendas políticas internacionais, além das reações às ameaças tradicionais externas (BUZAN; HANSEN, 2009). Além disso, observou-se na literatura uma mudança de

[1] Agentes Perturbadores da Ordem Pública (Nota do Revisor).

the military, had not yet been studied outside the logic of wars, so there was a gap to be filled in this regard (STAVRIANAKIS; STERN, 2018, 4) (STAVRIANAKIS; SELBY, 2013, p. 10).

This gap in academic literature and in the design of public policies represents a limitation that can be partially explained by the fact that the armed forces, as an institution, continue to be strongly associated by the literature with external threats to the State and with the political image of an "international" potentially hostile environment, in contrast with a stable and peaceful domestic order. Based on the assumption that including such themes was not enough to transcend those limits, which are not only territorial, but also ontological and epistemological, as they reflect how security is understood and conceived, we can see how they are linked to the sovereign logic of security where the State is the main unit of analysis. In addition to revealing epistemological limitations, this finding might help explain why the military were excluded from the agenda, even as the domestic sphere of States received greater attention from academics. As an object of study, militarisation has traditionally been treated as a function of sovereign states and, not coincidentally, has been dismissed by the literature as new themes — such as practices of violence within states, migration and transnational threats — came to overshadow extended security agendas. Despite this trend and the increase in domestic use of national armed forces in the post-Cold War period, militarisation and militarism are still understudied.

At the same time, an epistemological limitation in the concept of security uncovers the inability to understand and study the armed forces as institutions apart from their historical "significance", usually related to strategy and war studies and fighting external threats to the State. The latter represents an obstacle to theorizing the military in terms of how this State security institution relates to and deals with threats originated domestically. For this reason, academic debate continues to emphasise the fact that military dynamics bring to light the absence or incomplete theorisation of militarism (EASTWOOD, 2018, p. 51).

Conclusions and recommendations for the prevention of structural violence

Apparently, when studying violence in contemporary liberal States, the literature has been tied to those borders, where the military's prerogative continues to be international security. In other words, the themes of violence, war and the State continue to be linked to our way of thinking about militarism. As long as this is the case, our reflexions will not be able to deal with the challenges that are currently observed — mostly challenges that occur within State borders.

Therefore, the recommendations are:

1) we believe that the biggest obstacle presented by this problem is the fact that such limitation of the Armed Forces to the territorial concepts of modern sovereignty in liberal States overshadows the acknowledgement of all forms of violence and force exercised by the security apparatus inside the borders of Nation States. So, forces

enfoque que fugia do tema da guerra e do militarismo para o tema da segurança. Foi nesse contexto que o debate sobre securitização ganhou corpo, "para abordar questões relativas aos limites da segurança, de quando ela se inicia e se acaba e o que ela faz ou deixa de fazer". No entanto, foi levantado que a forma como o militarismo se relacionava com a segurança não tinha sido suficientemente explorado em discussões políticas e acadêmicas e, consequentemente, que temas a ele afins, como militarização e militares, ainda não tinham sido estudados fora da lógica de guerras e que havia uma lacuna a ser preenchida nesse sentido (STAVRIANAKIS; STERN, 2018, 4) (STAVRIANAKIS; SELBY, 2013, p. 10).

Tal *gap* na literatura acadêmica e na formulação de políticas públicas representa uma limitação que pode ser parcialmente explicada pelo fato de que as Forças Armadas, enquanto instituição, continuam a ser fortemente associadas na literatura a ameaças externas ao Estado e ao imaginário político de um ambiente "internacional" potencialmente hostil *vis-à-vis* uma ordem doméstica estável e pacífica. Ao partir do pressuposto de que a inclusão de tais temas não foi suficiente para transcender tais limites, não só territoriais, como também ontológicos e epistemológicos, pois refletem como a segurança é entendida e, consequentemente, concebida, é possível perceber como esses estão atrelados à lógica soberana de segurança onde o Estado é a principal unidade de análise. Além de revelar tais limitações epistemológicas, tal constatação poderia ajudar a explicar algumas razões pelas quais os militares foram colocados à parte das agendas na medida em que o âmbito doméstico dos Estados recebeu uma maior atenção entre os acadêmicos. Enquanto objeto de estudo, a militarização tem sido tradicionalmente tratada como uma função dos Estados soberanos e, não por acaso, foi afastada da literatura conforme novos temas passaram a dominar as agendas de segurança estendida, tais como práticas de violência no âmbito dos Estados, migrações e ameaças transnacionais. Apesar de tal tendência e do aumento do emprego doméstico de forças armadas nacionais no período do pós-Guerra Fria, a questão da militarização e do militarismo é, ainda, pouco estudada.

Ao mesmo tempo, tal limitação epistemológica de como a segurança é concebida revela uma inabilidade de se conceber e estudar as Forças Armadas como uma instituição dissociada da sua "significância" histórica, comumente observada nos estudos estratégicos e de guerra e orientada para ameaças advindas de fora do Estado, o que constitui um empecilho para uma teorização dos militares em termos de como essa instituição do aparato de segurança estatal se relaciona e lida com ameaças cuja origem e expressão são atribuídas ao âmbito doméstico nacional. Por essa razão, o debate acadêmico continua a frisar o fato de que as dinâmicas militares revelam uma ausência ou teorização incompleta do tema do militarismo (EASTWOOD, 2018, p. 51).

Conclusões e prescrições para a prevenção da violência estrutural

Ao que parece, tudo indica que, para se estudar violência nos Estados liberais contemporâneos, a literatura está atrelada a tais fronteiras, nas quais a prerrogativa dos militares continua a ser a segurança internacional. Em outras palavras, os temas da violência, guerra e o Estado seguem atrelados às nossas reflexões acerca do militarismo. Enquanto for esse o caso, nossas reflexões não serão capazes de dar conta dos desafios que se observam atualmente — em sua maioria, desafios que ocorrem dentro das fronteiras do Estado.

must be engaged as part of an interagency cooperation effort to normalise politics and reduce practices that lead to forms of structural violence.

2) the deployment of the armed forces promotes a sense of urgency that is politically reflected in the rhetorical use of the "war on" as a form of response aimed at eliminating threats. Therefore, the actions of the armed forces must be compatible with the set of public security policies developed or implemented for the social, economic and political development of the State.

3) theoretical and particularly empirical studies need to focus on the concepts of militarism, militarisation and "war", and to review their meaning, so that the current security threats observed in practice may be addressed and the necessary public policies may be designed. This will enable the study of cases and situations in which military power emerges and operates more effectively.

Such study is necessary because the way in which militarism, militarisation and "war" are treated in the literature directly influences the way in which public policies in the field of security are designed and implemented in practice.

In this case, we might ask ourselves not only whether the absence of war means peace, but whether the absence of war necessarily means a reduction in violence. Faced with a global scenario of less and less wars between States, this seems to be a relevant question if we want to understand the current phenomena of violence, even within the territorial limits of States.

The idea of pacification comes from this combination between direct and structural violence. It is a phenomenon that involves threat, intimidation and surveillance to restructure political and social relations in a coercive way (BARON et al., 2019). The inclusion and exclusion process resulting from pacifications becomes evident when it operates effectively: direct violence is suppressed, as it would affect the political order. However, its impacts reinforce social structures of exclusion and marginalisation, increasing the incidence of structural violence in this process of social reorganisation and naturalisation of the political order. Thus, pacification processes that impose violence coming from the State causing violent ruptures, are not aberrations, but rather tools to strengthen elements of social inequality (BARON et al, 2019).

The result of securitizing these new threats within the scope of domestic agendas is the creation of zones of social inclusion and exclusion. The rationale of pacification processes suggests that the use of military components would deter threats and promote a return to normal social conditions, as a result of the lack of violence in the region controlled by military forces. With the militarisation of responses to such new threats, society might be given a false sense of safety because of the lack of violence — whether due to the overt presence of security forces or to the actual or perceived removal of these threats to more peripheral areas of the city.

Following these recommendations implies taking into account that the armed forces are traditionally oriented towards existential external threats, especially wars, where

Para tanto, recomenda-se:

1) acreditamos que o maior empecilho identificado diante do referido problema é o fato de que tal limitação, que atrela as Forças Armadas aos conceitos territoriais da soberania moderna nos Estados liberais, ofusca um reconhecimento apropriado de todas as formas através das quais a violência e a força são exercidas pelo aparato de segurança dentro dos limites das fronteiras dos Estados-nação. Deste modo, as forças devem ser envolvidas como parte de um esforço de cooperação interagência para a normalização da política e a redução de práticas que levem a formas de violência estrutural.

2) o emprego das forças armadas estimula o senso de urgência que se reflete politicamente no emprego retórico da "guerra ao" como forma de resposta visando a eliminação de ameaças. Sendo assim, a atuação das forças armadas deve ser compatível com o conjunto de políticas públicas de segurança desenvolvidas ou implementadas para o desenvolvimento social, econômico e político do Estado.

3) investigações, em sua dimensão teórica e sobretudo empírica, precisam abordar os conceitos de militarismo, militarização e "guerra" de forma a repensar o seu significado para abordar as atuais ameaças à segurança observadas na prática e poder, assim, formular as políticas públicas nesse campo que visam abordá-las. Assim, será possível se estudar casos e situações nas quais o poderio militar emerge e opera de forma mais eficaz.

Uma investigação nesse sentido faz-se necessária, pois a forma como o militarismo, a militarização e a "guerra" são tratados na literatura influi diretamente na forma como as políticas públicas no campo da segurança são pensadas e implementadas na prática.

Nesse caso, poderemos nos perguntar não apenas se a ausência de guerras significa paz, mas, sim, se a ausência de guerras denota, necessariamente, uma redução da violência. Diante de um cenário global de cada vez menos guerras entre Estados, essa parece ser uma pergunta cabível se quisermos entender os atuais fenômenos de como a violência tem sido exercida, mesmo dentro dos limites territoriais dos Estados.

A ideia da pacificação recai nessa combinação de violência direta e estrutural. Ela é um fenômeno que envolve ameaça, intimidação e vigilância para reestruturar as relações políticas e sociais de forma coercitiva (BARON et al., 2019). O processo de inclusão e exclusão decorrente das pacificações fica evidenciado quando ele opera de forma efetiva: há a supressão da violência direta, já que esta afetaria a ordem política. Contudo, seus impactos reforçam as estruturas sociais de exclusão e marginalização, aumentando a incidência da violência estrutural nesse processo de reorganização social e naturalização da ordem política. Desse modo, processos de pacificação que impõem uma violência vinda do Estado e promovem rupturas violentas não são aberrações, mas ferramentas para reforçar os elementos de desigualdade social (BARON et al, 2019).

A síntese resultante da securitização dessas novas ameaças no âmbito das agendas domésticas resulta na criação de zonas de inclusão e exclusão sociais. A lógica subjacente aos processos de pacificação sugere que o emprego de componentes militares afastaria as ameaças e promoveria o retorno das condições sociais normais decorrentes da ausência de violência na região sob controle das forças militares. Contudo,

the use of force is required at a higher degree. As a result, this prerogative of the military using a higher degree of force must be adjusted by public policy makers, to meet the needs of internal governance in the enforcement of law and order.

References and Suggested Literature

ARANTZA, Arana Gomez. 'The EU and Latin America: A real security and development nexus or a superficial one?' In: SERVENT, Ariadna Ripoll; TRAUNER, Florian (eds). **The Routledge Handbook of Justice and Home Affairs Research.** Abingdon; New York: Routledge, 2018.

BARON, Ilan Zvi; HAVERCROFT, Jonathan; KAMOLA, Isaac; KOOMEN, Jonneke; MURPHY, Justin; PRICHARD, Alex. Liberal Pacification and the Phenomenology of Violence. **International Studies Quarterly,** Volume 63(1), pp. 199-212, March 2019.

BOYLE, Philip; HAGGERTY, Kevin D.'Spectacular Security: Mega-Events and the Security Complex'. **International Political Sociology**, Volume 3, pp. 257–274, 2009.

BUZAN, Barry; HANSEN, Lene. **The Evolution of International Security Studies.** Cambridge: Cambridge University Press, 2009.

HUNDRED, Miguel Angel. **Blood and Debt: War and the Nation-State in Latin America.** University Park: Pennsylvania State University Press, 2002.

EASTWOOD, James. 'Rethinking militarism as ideology: The critique of violence after security'. **Security Dialogue** Special Issue on Militarism and Security: Dialogue, possibilities and limits. Vol. 49(1-2), pp. 44-56, 2018.

FAGEN, Patricia Weiss. 'Repression and State Security.' In: CORRADI, Juan E.; WEISS, Patricia; GARRETÓN, Manuel Antonio (eds). **Fear at the Edge: State Terror and Resistance in Latin America.** Berkeley and Los Angeles: University of California Press, 1992.

FELBAB-BROWN, Vanda. **Law Enforcement Actions in Urban Spaces Governed by Violent Non-State Entities: Lessons from Latin America.** Western Hemisphere Security Analysis Center. Applied Research Center, Florida International University. September 2011.

GALTUNG, Johan. **Violence, Peace, and Peace Research.** Oslo: International Peace Research Institute, 1969.

GRAHAM, Stephen. **Cities Under Siege: The New Military Urbanism.** London: Verse Books, 2011.

HERZ, Monica. 'Concepts of Security in South America.' **International Peacekeeping**, pp. 598-612, 2010.

HURRELL, Andrew. Security in Latin America. **International Affairs**, 74, Volume 3, pp. 529-546, 1998.

JANOWITZ, Morris. **Military Institutions and Coercion in the Developing Nations** (expanded edition). Chicago and London: The University of Chicago Press, 1977.

a militarização das respostas a essas novas ameaças pode oferecer à sociedade uma falsa sensação de segurança ao construir a imagem da ausência de violência — seja por conta da presença ostensiva de forças de segurança ou do afastamento, real ou percebido, dessas ameaças para regiões metropolitanas periféricas.

Seguir tais recomendações implica necessariamente em levar em consideração que as forças armadas são forças tradicionalmente voltadas para ameaças externas existenciais, principalmente guerras, onde o uso da força se faz necessário em maior grau. Portanto, é preciso também levar em conta que a prerrogativa de maior grau do recurso à força por parte do aparato militar precisa ser ajustada pelos agentes formuladores de políticas públicas de forma a reduzi-lo e ajustá-lo às demandas de governança interna no exercício da manutenção da lei e da ordem.

Referências/sugestões de leitura

ARANTZA, Arana Gómez. 'The EU and Latin America: A real security and development nexus or a superficial one?' In: SERVENT, Ariadna Ripoll; TRAUNER, Florian (eds). **The Routledge Handbook of Justice and Home Affairs Research**. Abingdon; New York: Routledge, 2018.

BARON, Ilan Zvi; HAVERCROFT, Jonathan; KAMOLA, Isaac; KOOMEN, Jonneke; MURPHY, Justin; PRICHARD, Alex. Liberal Pacification and the Phenomenology of Violence. **International Studies Quarterly**, Volume 63(1), pp. 199-212, March 2019.

BOYLE, Philip; HAGGERTY, Kevin D. 'Spectacular Security: Mega-Events and the Security Complex'. **International Political Sociology**, Volume 3, pp. 257–274, 2009.

BUZAN, Barry; HANSEN, Lene. **The Evolution of International Security Studies**. Cambridge: Cambridge University Press, 2009.

CENTENO, Miguel Angel. **Blood and Debt: War and the Nation-State in Latin America**. University Park: Pennsylvania State University Press, 2002.

EASTWOOD, James. 'Rethinking militarism as ideology: The critique of violence after security'. **Security Dialogue** Special Issue on Militarism and Security: Dialogue, possibilities and limits. Vol. 49(1-2), pp. 44-56, 2018.

FAGEN, Patricia Weiss. 'Repression and State Security.' In: CORRADI, Juan E.; WEISS, Patricia; GARRETÓN, Manuel Antonio (eds). **Fear at the Edge: State Terror and Resistance in Latin America**. Berkeley and Los Angeles: University of California Press, 1992.

FELBAB-BROWN, Vanda. **Law Enforcement Actions in Urban Spaces Governed by Violent Non-State Entities: Lessons from Latin America**. Western Hemisphere Security Analysis Center. Applied Research Center, Florida International University. September 2011.

GALTUNG, Johan. **Violence, Peace, and Peace Research**. Oslo: International Peace Research Institute, 1969.

GRAHAM, Stephen. **Cities Under Siege: The New Military Urbanism**. London: Verso Books, 2011.

HERZ, Monica. 'Concepts of Security in South America.' **International Peacekeeping**, pp. 598-612, 2010.

KACOWICZ, Arie M. **The Impact of Norms in International Society: The Latin American Experience, 1881-2001**. Notre Dame: University of Notre Dame Press, 2005.

NUNN, Frederick M. 'Foreign Influences on the South American Military: Professionalization and Politicization.' In: SILVA, Patricio (ed). **The Soldier and the State in South America: Essays in Civil-Military Relations**. New York and Hampshire: Palgrave, pp. 13-37, 2001.

NEOCLEOUS, Mark. **War Power, Police Power**. Edinburgh: Edinburgh University Press, 312 p., 2014.

SEAS, David R; KACOWICZ, Arie M. (eds.). 'Security Studies and Security in Latin America: The first 200 years.' **Routledge Handbook of Latin American Security**. Abingdon and New York: Routledge, pp. 11-29, 2015.

MINISTRY OF DEFENSE OF BRAZIL. **Garantia da Lei e da Ordem: MD33-M-10 – 2a Ed.** 3 de fevereiro de 2014. Available at: https://edisciplinas.usp.br/pluginfile.php/483786/mod_resource/content/1/Portaria%20MD_2%20Ed_%20Garantia%20da%20Lei%20e%20da%20Ordem_Jan%202014.pdf [accessed June 6, 2019].

STAVRIANAKIS, Anna; SELBY, Jan. **Militarism and International Relations in the 21st century**. London: Routledge, 2013.

STAVRIANAKIS, Anna; STERN, Mary. 'Military and Security: Dialogues, Possibilities and Limits'. **Security Dialogue** Special Issue on Militarism and Security: Dialogue, possibilities and limits. Vol.49(1-2), pp. 3-18, 2018.

HURRELL, Andrew. Security in Latin America. **International Affairs**, 74, Volume 3, pp. 529-546, 1998.

JANOWITZ, Morris. **Military Institutions and Coercion in the Developing Nations** (expanded edition). Chicago and London: The University of Chicago Press, 1977.

KACOWICZ, Arie M. **The Impact of Norms in International Society: The Latin American Experience, 1881-2001**. Notre Dame: University of Notre Dame Press, 2005.

NUNN, Frederick M. 'Foreign Influences on the South American Military: Professionalization and Politicization.' In: SILVA, Patricio (ed). **The Soldier and the State in South America: Essays in Civil-Military Relations**. New York and Hampshire: Palgrave, pp. 13-37, 2001.

NEOCLEOUS, Mark. **War Power, Police Power**. Edinburgh: Edinburgh University Press, 312 p., 2014.

MARES, David R; KACOWICZ, Arie M. (eds). 'Security Studies and Security in Latin America: The first 200 years.' **Routledge Handbook of Latin American Security**. Abingdon and New York: Routledge, pp. 11-29, 2015.

MINISTÉRIO DA DEFESA DO BRASIL. **Garantia da Lei e da Ordem: MD33-M-10 – 2a Edição**. 3 de fevereiro de 2014. Disponível em: https://edisciplinas.usp.br/pluginfile.php/483786/mod_resource/content/1/Portaria%20MD_2%20Ed_%20Garantia%20da%20Lei%20e%20da%20Ordem_Jan%202014.pdf [acesso em 6 de junho de 2019]

STAVRIANAKIS, Anna; SELBY, Jan. Militarism and International Relations in the 21st Century. London: Routledge, 2013.

STAVRIANAKIS, Anna; STERN, Maria. 'Militarism and Security: Dialogues, Possibilities and Limits'. **Security Dialogue** Special Issue on Militarism and Security: Dialogue, possibilities and limits. Vol.49(1-2), pp. 3-18, 2018.

Cauê Pimentel

Cauê Pimentel é diplomata, Bacharel em Relações Internacionais pela UNESP (2010) e Doutor em Ciência Política pela USP (2018).

Cauê Pimentel is a diplomat, Bachelor in International Relations from UNESP (2010) and holds a PhD in Political Science from USP (2018).

Governança da segurança no Atlântico Sul: multilateralismo, cooperação e rivalidade

Security governance in the South Atlantic: multilateralism, cooperation, and rivalry

Cauê Pimentel*

SUMÁRIO EXECUTIVO/ RESUMO

Este *paper* discute as principais características da governança de segurança do Atlântico Sul, em especial de seu núcleo dinâmico no Golfo da Guiné. Demonstra como a arquitetura de cooperação adotada até o momento rendeu poucos resultados devido ao seu caráter *ad-hoc* e altamente fragmentado, com sobreposição de esforços por vários países. Alternativamente, o *paper* propõe iniciativas que Europa e América do Sul poderiam adotar em direção a uma governança mais eficiente e pragmática em torno de problemas prementes, com destaque para a pirataria. Isso inclui o aumento da troca de informações entre os atores envolvidos, o estabelecimento de um currículo mínimo de treinamento comum e o compartilhamento de responsabilidades de segurança, com possível emprego de uma força-tarefa de segurança com responsabilidades compartilhadas. Defende-se, por fim,

* As opiniões contidas neste texto são de inteira responsabilidade do autor e não representam as posições do Ministério das Relações Exteriores.

EXECUTIVE SUMMARY/ SUMMARY

This paper discusses the main features of South Atlantic security governance, particularly its dynamic core in the Gulf of Guinea. It demonstrates how the cooperation architecture adopted so far has yielded few results owing to its *ad hoc,* highly fragmented character, in which several countries' efforts overlap. This paper proposes alternative initiatives that Europe and South America could adopt towards a more efficient, pragmatic governance concerning pressing problems, with an emphasis on piracy. These include increasing the exchange of information between the actors involved, establishing a standard minimum common training curriculum, and sharing security responsibilities, with the possibility of employing a security task force with shared responsibilities. Finally, it argues that a coordinated presence of Europeans and South Americans in the Gulf of Guinea can work

* The opinions contained in this text are the sole responsibility of the author and do not represent the positions of the Ministry of Foreign Affairs.

as confidence-building and gains in projection for the two continents in a region that, in recent years, has been the target of renewed geostrategic interest.

The South Atlantic is a maritime space of great geostrategic relevance for South America, Europe, and Africa. In recent decades, new regional security dynamics, such as the emergence of new threats or the discovery of abundant natural resources, have sparked renewed interest in the region's maritime security. Concurrently with the growing presence of China on the West African coast, these dynamics have given new prominence to the Atlantic maritime space in global geopolitical strategies.

Consequently, since the middle of the last decade, there has been a considerable increase in the involvement of several countries in the region, notably from the European Union (EU) and South America, especially Brazil, in the quest to exercise some regional leadership regarding security. Consequently, the list of organisations with a mandate or an interest in regional security issues in the South Atlantic continues to grow; it includes, but is not limited to, ZOPACAS[1], AFRICOM[2], the African Union, the EU[3], NATO, the Gulf of Guinea Commission, ECOWAS[4], ECCAS[5], the G7++ FoGG Group[6], the CPLP[7], the United Nations (UN - and its specialised agencies such as UNODC[8]), the IMB[9] and Interpol, among others. Added to this is an abundance of bilateral partnerships and private actors' networks operating in the region, resulting in a complex mosaic of agents and agendas.

At first sight, the result is a paradoxical phenomenon: if, on the one hand, security practices are intensified, creating diffuse, non-hierarchical cooperation networks, which could contribute to increasing the positive externalities of security, on the other hand, the use of scarce resources (military and budgetary) is fragmented, there is competition for the region's agenda-setting and there are consequences to geopolitical rivalries, since others can perceive the cooperation between two actors as a loss of influence or a threat to strategic interests. In the South Atlantic, this scenario reveals a kind of "race for cooperation", mainly along the west coast of Africa, with several powers seeking to position themselves as priority partners of the countries in the region in terms of security. In turn, African riparian countries take advantage of this renewed interest in their geopolitical position as a source of partnership diversification and, consequently, of greater bargaining power.

Owing to these characteristics, the South Atlantic is a model empirical case of what the specialised bibliography characterises as "security governance." The concept

1 South Atlantic Peace and Cooperation Zone.

2 African Command Centre, sponsored by the United States.

3 By means of, for instance, the "European Union Maritime Security Strategy", in addition to its bilateral engagement with countries in the region.

4 Economic Community of West African States.

5 Economic Community of Central African States.

6 G7++ Friends of the Gulf of Guinea, which includes countries from the Gulf of Guinea, the G7 and other partners such as Brazil.

7 Community of Portuguese Language Countries.

8 United Nations Office on Drugs and Crime.

9 International Maritime Bureau.

que uma presença coordenada de europeus e sul-americanos no Golfo da Guiné pode funcionar como construção de confiança e ganhos de projeção para os dois continentes em uma região que, nos últimos anos, tem sido alvo de renovado interesse geoestratégico.

O Atlântico Sul é um espaço marítimo de grande relevância geoestratégica para a América do Sul, a Europa e a África. Nas últimas décadas, novas dinâmicas regionais de segurança, como o surgimento de novas ameaças ou a descoberta de recursos naturais abundantes, despertaram um interesse revigorado pela segurança marítima da região. Concomitantemente com a ascensão chinesa na costa ocidental africana, essas dinâmicas deram novo valor ao espaço marítimo atlântico nos cálculos geopolíticos globais.

Como consequência, desde meados da década passada, houve um crescimento notável no engajamento de diversos países na região, notadamente da União Europeia (UE) e da América do Sul, em especial do Brasil, na busca de exercer algum tipo de liderança regional em matéria de segurança. Consequentemente, a lista de organizações com algum mandato ou interesse em temas de segurança regional do Atlântico Sul não para de crescer: inclui, não exaustivamente, a ZOPACAS[1], o AFRICOM[2], a União Africana, a UE[3], a OTAN, a Comissão do Golfo da Guiné, a ECOWAS[4], a ECCAS[5], o Grupo G7++ FoGG[6], a CPLP[7], as Nações Unidas (e suas agências especializadas, como a UNODC[8]), o IMB[9] e a Interpol, entre outras. Soma-se, ainda, a profusão de parcerias bilaterais e as redes de atores privados atuantes na região, resultando em um mosaico complexo de agentes e agendas.

O resultado é um fenômeno, à primeira vista, paradoxal: se, por um lado, há adensamento de práticas de segurança que criam redes difusas e não-hierárquicas de cooperação, o que contribuiria para aumentar as externalidades positivas de segurança, por outro, verifica-se fragmentação no uso de recursos escassos (militares e orçamentários), competição pelo *agenda-setting* da região e reflexo em rivalidades geopolíticas, uma vez que a cooperação entre dois atores pode ser percebida por outros como perda de influência ou ameaça a interesses estratégicos. Esse cenário aduz, no Atlântico Sul, uma espécie de "corrida por cooperação", principalmente ao longo da costa ocidental oeste africana, com diversas potências buscando se posicionar como parceiros prioritários dos países da região, em matéria de segurança. Por sua vez, os países ribeirinhos africanos aproveitam esse interesse renovado em sua posição geopolítica como fonte de diversificação de parcerias e, consequentemente, aumento do seu poder de barganha.

Por essas características, o Atlântico Sul configura caso empírico modelar do que a

1 Zona de Paz e Cooperação do Atlântico Sul.

2 African Command Center, patrocinado pelos Estados Unidos.

3 Por meio, por exemplo, da "European Union Maritime Security Strategy", além de seu engajamento bilateral com os países da região.

4 Economic Community of West African States (Nota do Revisor.)

5 Economic Community of Central African States.

6 G7++ Friends of the Gulf of Guinea, que inclui países do Golfo da Guiné, do G7 e outros parceiros, como o Brasil.

7 Comunidade de Países de Língua Portuguesa (Nota do Revisor.)

8 United Nations Office on Drugs and Crime.

9 International Maritime Bureau.

seeks to explain the growing intersection of multilateral initiatives to solve regional security problems concurrently with maintaining the competitive dynamics among the system's main actors. The result is neither a cohesive, peaceful security community nor an area marked by the dominance of a *hegemon* or power bloc. Instead, it is a zone with an intense overlapping of initiatives on security issues, with an intersection of cooperation/competition arrangements and an incidence of extra-regional dynamics and inter-power rivalries that go beyond the limits of the South Atlantic. In this context, no power manages to impose itself as the only regional security provider. Consequently, there is a process of fragmentation of security cooperation concomitant with a power balance dynamic (ADLER, GREVE, 2009; KIRCHNER, SPERLING, 2008).

In this scenario, four characteristics define the regional security architecture: 1) the existence of a high number of institutions and multilateral groups involving different state actors, with a substantial overlap of initiatives; 2) the low degree of institutionalisation of these mechanisms; 3) the low level of intra-regional interdependence and the high degree of extra-regional dependence, especially in matters of defence and security; and 4) the strong asymmetry of intraregional and extra-regional military capabilities.

These dynamics serve to explain the broad spectrum of changes that permeate the South Atlantic as a whole, but manifest themselves with particular intensity in the Atlantic sub-complex of the Gulf of Guinea, a logistic hub through which sensitive logistical routes pass — most of Brazil's oil imports, 40% of Europe's imports, and 25% of the USA's imports — and where twelve essential ports for the African economy are located, spread along more than six thousand densely populated kilometres of coastline. Every day, over 1,500 vessels cross the region, in which significant fishing and energy resources lie. This dynamism attracts illegal activities, such as drug trafficking, illegal fishing, and, above all, piracy. For these reasons, the Gulf of Guinea has become a hotspot in the South Atlantic, concentrating most of the region's multilateral cooperation initiatives in maritime security.

In practice, there is more cooperation, but not necessarily with better results: despite the growing number of security initiatives, there is, year after year, an increase in threats in the region, which, in 2020, registered a 20% increase in the number of pirate attacks compared to the previous year, a record high, with an average of one attack every two days, in an area that currently accounts for 95% of all kidnappings of sailors and hijacking of vessels globally. There is a noticeable opposite trend to what has been happening in the Gulf of Aden, on the other side of the African continent, where the cooperation of several actors — in an area with even more prominent geopolitical rivalries, due to the active presence of powers such as India, China, Russia, the US, and the EU, not to mention local rivalries between riparian Gulf countries — has dramatically reduced the number of pirate attacks along the Somali coast. This comparison attests to the complexity of the situation in the Gulf of Guinea. Moreover, it raises the question of why the cooperation architecture adopted in the region has not achieved the expected results.

It is worth noting that, on the one hand, the security of maritime spaces can be

bibliografia especializada caracteriza como "governança da segurança", conceito que busca explicar a crescente intersecção de iniciativas multilaterais para resolver problemas regionais de segurança concomitantemente com a manutenção de dinâmicas de competição entre os principais atores do sistema. O resultado não é nem uma comunidade de segurança coesa e pacífica, nem uma zona marcada pela dominância de um *hegemon* ou de um bloco de poder, mas, sim, uma zona com intensa sobreposição de iniciativas ("*overlap*") em temas de segurança, com intersecção de arranjos de cooperação/competição e com incidência de dinâmicas extrarregionais e rivalidades interpotências que extrapolam os limites do Atlântico Sul. Nesse quadro, nenhuma potência consegue se impor como único provedor de segurança regional e, consequentemente, há um processo de fragmentação da cooperação em segurança concomitantemente com a presença de dinâmicas de balança de poder (ADLER, GREVE, 2009; KIRCHNER, SPERLING, 2008).

Em um cenário desse tipo, quatro características definem a arquitetura de segurança regional:
1) a existência de um alto número de instituições e agrupamentos multilaterais envolvendo diversos atores estatais, com forte sobreposição de iniciativas;
2) o baixo grau de institucionalização desses mecanismos;
3) o baixo nível de interdependência intrarregional e o alto grau de dependência extrarregional, principalmente em temas de defesa e segurança;
4) forte assimetria de capacidades militares intrarregional e extrarregional.

Essas dinâmicas servem para explicar o amplo espectro de dinâmicas que perpassam o Atlântico Sul como um todo, porém se manifestam com particular intensidade no subcomplexo atlântico do Golfo da Guiné, *hub* logístico por onde passam rotas logísticas sensíveis — a maior parte das importações de petróleo do Brasil, 40% das importações da Europa e 25% dos EUA — e onde estão localizados doze portos essenciais para a economia africana, distribuídos em mais de seis mil quilômetros de costa, com alta densidade populacional litorânea. Diariamente, mais de 1.500 embarcações cruzam a região, na qual jazem importantes recursos pesqueiros e energéticos. Esse dinamismo atrai atividades ilegais, como o narcotráfico, a pesca ilegal e, sobretudo, a pirataria. Por esses motivos, o Golfo da Guiné tornou-se um *hotspot* no Atlântico Sul, concentrando a maior parte das iniciativas de cooperação multilateral em segurança marítima da região.

Na prática, coopera-se mais, mas não necessariamente com melhores resultados: apesar do número crescente de iniciativas em matéria de segurança, há, ano a ano, um agravamento das ameaças na região que, em 2020, registrou um aumento de 20% no número de ataques piratas em relação ao ano anterior, número recorde, com média de um ataque a cada dois dias, em uma zona que atualmente contabiliza 95% de todos os sequestros de marinheiros e embarcações, em nível global. Percebe-se uma tendência contrária ao que vem acontecendo no Golfo de Áden, do outro lado do continente africano, onde a cooperação de diversos atores — em uma área com rivalidades geopolíticas inclusive mais proeminentes, devido à presença ativa de potências como Índia, China, Rússia, Estados Unidos e UE, sem contar as rivalidades locais entre os países ribeirinhos do Golfo — reduziu drasticamente o número de ataques piratas partindo da costa somali. Essa comparação atesta a complexidade da situação no Golfo da Guiné e lança a pergunta sobre o porquê de a arquitetura de cooperação adotada na região não ter logrado os resultados esperados.

classified as a collective problem with far-reaching transnational effects. Conversely, it can be seen as a "global public good" and a factor in strengthening interdependence among States, encouraging greater cooperation among different actors to increase security provision for this common good, maximizing collective gains. On the other hand, maritime security also functions as an ambiguous symbol in international relations — or as a security dilemma and a problem of "national interest" — which results in competitive dynamics on the use of maritime space and becomes a means of power projection. There are diplomatic and military interests that drive a country to seek to position itself as a priority provider of security in the region, forging alliances and, thus, projecting itself as the regional leader in the security agenda.

Brazil, for example, sees the South Atlantic as an essential vector for its national identity, and as a condominium over which it aims to perform its role as a medium power, insulating the region from the influence of forces it perceives as "extra-regional," such as China or the North Atlantic countries. Europe, in turn, sees the region as a global strategic asset that was partially neglected during the 1990s, but where it is imperative to regain its historical position of prestige and influence. In this sense, it sees the region as a component in an expanded Euro-Atlantic framework. Moreover, Brazil considers that it has responsibilities towards African countries, a legacy of the colonisation process, which generates both closeness and repulse from the African elites in the region's decision-making process. Some countries within the EU, such as Portugal, in particular, see the Atlantic as a priority space for their prominence as relevant international actors and promote this agenda both bilaterally and by means of joint actions with the EU or the CPLP. Each country understands the region differently and, consequently, sees its role in the local architecture in equally different ways, thus shaping the cooperation options preferred by actors, affecting results.

An excessively decentralised and fragmented cooperation generates redundant initiatives around the same theme, with the consequent dispersion of resources that are already scarce. When there is no complementarity between these cooperation projects, there is a loss of effectiveness in using resources, especially military ones, while transaction costs to solve a problem may increase, contrary to the liberal theory expectation that more cooperation is always positive. As is the case in the Gulf of Guinea, overly complex regimes lose their effectiveness, which may result in their feeding competition between initiatives back into the picture rather than fostering convergence (DREZNER, 2009).

At least three cooperation modalities illustrate these security governance dilemmas in the Gulf of Guinea: the provision of training to African naval forces, the increase in joint military exercises, and the creation of maritime traffic monitoring systems. Moreover, there is significant room for closer coordinated action between Europe and South America in each modality, as will be discussed later.

The training of civilians and military personnel from other countries in security and defence matters has become a fundamental component of the contemporary armed forces' "defence diplomacy" (SACHAR, 2003). It builds trust between States, helps prevent conflicts, increases interoperability of forces, allows the alignment of strategic

Vale destacar que a segurança dos espaços marítimos pode ser classificada como um problema coletivo, com efeitos transnacionais de amplo alcance. De fato, ela pode ser encarada como um "bem público global" e fator de estreitamento da interdependência entre Estados, o que incentivaria, portanto, maior cooperação entre diferentes atores, de forma a aumentar a provisão de segurança para esse bem comum, maximizando os ganhos coletivos. Por outro lado, a segurança marítima também opera como como um símbolo ambíguo nas relações internacionais — ou como um dilema de segurança e um problema de "interesse nacional" — que resulta em dinâmicas concorrenciais sobre o uso do espaço marítimo e como recurso de projeção de poder. Há interesses diplomáticos e militares para que um país busque colocar-se como provedor prioritário de segurança na região, moldando alianças e, assim, projetando-se como líder regional da agenda de segurança.

O Brasil, por exemplo, enxerga o Atlântico Sul como vetor importante de sua identidade nacional e como condomínio sobre o qual ambiciona exercer seu papel de potência média, insulando-o da influência de potências que percebe como atores "extrarregionais", tais como a China ou os países do Atlântico Norte. A Europa, por sua vez, percebe a região como um ativo estratégico global parcialmente negligenciado durante os anos 1990, mas onde é imperativo retomar sua histórica posição de prestígio e influência. Nesse sentido, entende a região como componente de uma moldura euro-atlântica expandida, na qual possui responsabilidades para com os países africanos, herança do processo de colonização, a qual gera aproximação e repulsão por parte de elites africanas no processo de tomada de decisão. Dentro da UE, alguns países em especial, como Portugal, veem o Atlântico como um espaço prioritário para sua projeção como ator internacional relevante, e promovem essa agenda tanto no plano bilateral quanto por meio das ações conjuntas com a UE ou com a CPLP. Cada país entende a região de uma forma diferente e, consequentemente, enxerga o seu papel na arquitetura local de forma igualmente distinta. Isso molda as opções de cooperação preferida pelos atores, com impactos nos resultados.

A cooperação excessivamente descentralizada e fragmentada gera iniciativas redundantes em torno de um mesmo tema, com consequente dispersão de recursos que já são escassos. Quando não há complementariedade entre esses projetos de cooperação, há perda de efetividade no emprego de recursos, sobretudo militares, e os custos de transação para resolver um problema podem aumentar, contrariando a expectativa da teoria liberal de que mais cooperação é sempre algo positivo. Regimes exageradamente complexos, como no caso do Golfo da Guiné, perdem em efetividade e podem acabar retroalimentando a concorrência entre iniciativas, ao invés de fomentar convergência (DREZNER, 2009).

Ao menos três modalidades de cooperação ilustram esses dilemas da governança de segurança no caso do Golfo da Guiné: a oferta de treinamento para forças navais africanas, o aumento nos exercícios militares conjuntos e a criação de sistemas de monitoramento do tráfego marítimo. Em cada um deles, há espaço significativo para uma ação coordenada mais estreita entre Europa e América do Sul, como se discutirá mais adiante.

O treinamento de civis e militares de outros países em matéria de segurança e defesa converteu-se em um componente fundamental da "diplomacia de defesa" das forças

visions, and facilitates cooperation to tackle common threats. It is, therefore, an essential aspect of foreign and defence policy in times of peace.

In the Gulf of Guinea, a good part of the training offered to the navies of the African countries of the South Atlantic coast takes place bilaterally and *ad hoc*, which generates an overlap of initiatives and projects that, instead of complementing each other, end up replicating efforts and dispersing resources. Recently, in 2019, a document — entitled *Maritime Security in the Gulf of Guinea: Training Matrix and Planning Report,* sponsored by CIC[10] — drafted a roadmap for the training of the region's armed forces, which was to be implemented over three years, by 2021. The lack of financial and human resources, however, prevented the implementation of the plan. In this case, there is a structural problem of competition with other initiatives: the CIC depends exclusively on international donors to function. Additionally, there are incentives for those countries that prefer to offer bilateral training to imprint their national flag on the cooperation provided. For example, Brazil, France, and the United Kingdom are key players in providing training to African armed forces, but they act primarily through bilateral arrangements, with little coordination and integration. The overlapping of efforts that undermines the impact that this modality of cooperation could have is evident.

Military exercises are similarly heterogeneous, but are a more sensitive topic since they are hybrid actions of cooperation and deterrence. On the one hand, maritime exercises are trust-building modalities, increasing interoperability of naval forces and bringing security doctrines closer together. On the other hand, they also serve to establish military presence in strategic areas and to display deterrent capabilities to potential rivals. The interpretation of a given exercise as a positive factor of cooperation or a sign of threat and rivalry depends on subjective aspects of State actors and the role that they believe they play in the region[11]. Military exercises are, therefore, dual activities, encompassing cooperation and deterrence (LE MIÈRE, 2014).

In recent years, the South Atlantic has seen a profusion of bilateral and multilateral exercises. Some exercises are noteworthy, as they include a large number of participating countries: the *Obangame Express*, created in 2011 by the US AFRICOM; the *Grand Nemo*, created in 2018 by France; the *Felino,* created in 2000 by CPLP[12]; and the *Eku Kugbe,* spearheaded by Nigeria in 2016, in which a Chinese vessel participated for the first time in 2018. In addition to these examples, there is a myriad of smaller exercises, bilateral or plurilateral. There is often a significant overlap of States participating in these exercises, demonstrating how each power seeks to lead an initiative so that it can exert its influence on security issues in the region. If, on the one hand, this overlap theoretically enables the dissemination of good security practices, on the other hand,

[10] Inter-regional Coordination Centre (CIC), created in 2014, which merged the Regional Maritime Centre of Central Africa and the Regional Maritime Centre of West Africa, precisely aiming to reduce overlapping cooperation efforts.

[11] See, for instance, the negative repercussions in diplomatic circles and in the South American press on the naval exercise carried out between the United Kingdom and the US in the Falkland Islands, in the beginning of the year 2021.

[12] Unlike the other exercises mentioned, the *Felino* is not limited to the Gulf of Guinea setting, but is certainly representative of Brazilian and Portuguese ambitions to lead their own training initiatives in the strategic environment of the South Atlantic.

armadas contemporâneas (SACHAR, 2003). Cria confiança entre Estados, ajuda na prevenção de conflitos, aumenta a interoperabilidade de forças, permite alinhamento de visões estratégicas e facilita a cooperação, visando atacar ameaças comuns. Constitui, portanto, uma vertente importante da política externa e de defesa, em tempos de paz.

No Golfo da Guiné, boa parte da oferta de treinamento às marinhas dos países africanos da costa sul-atlântica se dá de forma bilateral e *ad-hoc*, o que gera uma sobreposição de iniciativas e projetos que, ao invés de se complementarem, acabam replicando esforços e dispersando recursos. Recentemente, em 2019, um documento — intitulado *"Maritime Security in the Gulf of Guinea: Training Matrix and Planning Report",* patrocinado pelo CIC[10] — esboçou um *roadmap* para o treinamento das forças armadas da região, que deveria ser implementado em um período de três anos, até 2021. A falta de recursos financeiros e humanos impediu, porém, a concretização do plano. Aqui, verifica-se o problema estrutural da concorrência com outras iniciativas: o CIC depende exclusivamente de doadores internacionais para funcionar, e há incentivos para que países prefiram oferecer treinamento bilateral, de modo a estampar sua bandeira nacional à cooperação prestada. Brasil, França e Reino Unido, por exemplo, são atores fundamentais na prestação de treinamento para forças armadas africanas, porém atuam majoritariamente por via de arranjos bilaterais, com pouca coordenação e integração. Fica evidente a sobreposição de esforços que mina o impacto que tal modalidade de cooperação poderia ter.

Exercícios militares apresentam uma heterogeneidade semelhante, porém são tema mais sensível, uma vez que se tratam de ações híbridas de cooperação e dissuasão. Exercícios marítimos são modalidades de construção de confiança, aumento de interoperabilidade de forças navais e de aproximação de doutrinas de segurança. Por outro lado, também servem para marcar presença militar em zonas estratégicas e sinalizar capacidades dissuasórias a possíveis rivais. A interpretação de um determinado exercício como fator positivo de cooperação ou sinalização de ameaça e rivalidade depende de fatores subjetivos dos atores estatais e do papel que eles enxergam desempenhar na região[11]. Os exercícios militares são, portanto, atividades duais de cooperação e dissuasão (LE MIÈRE, 2014).

Nos últimos anos, o Atlântico Sul presenciou uma profusão de exercícios bilaterais e multilaterais. Alguns exercícios merecem destaque, por incluírem um alto número de países participantes: o *Obangame Express*, criado em 2011 pelo AFRICOM estadunidense; o *Grand Nemo*, criado em 2018 pela França; o *Felino,* criado em 2000 pela CPLP[12]; e o *Eku Kugbe,* capitaneado pela Nigéria em 2016 e que, em 2018, contou pela primeira vez com a participação de uma embarcação chinesa. Além desses exemplos, há uma miríade de exercícios menores, bilaterais ou plurilaterais. Há, geralmente, grande sobreposição de Estados participantes nesses exercícios, o que demonstra, na verdade, como cada potência busca liderar uma

[10] Centro de Inter-regional de Coordenação (CIC), criado em 2014, que fundiu o Centro Regional Marítimo da África Central e o Centro Regional para Segurança Marítima da África Ocidental, justamente mirando diminuir esforços sobrepostos de cooperação.

[11] Vide, por exemplo, a repercussão negativa em meios diplomáticos e na imprensa sul-americana sobre o exercício naval realizado entre Reino Unido e Estados Unidos nas Ilhas Malvinas/Falkland, no início do ano de 2021.

[12] Diferentemente dos outros exercícios citados, o Felino não se limita ao cenário do Golfo da Guiné, mas é, certamente, representativo das ambições brasileiras e portuguesas de capitanear iniciativas próprias de treinamento no entorno estratégico do Atlântico Sul.

it works as a stage for the display of naval forces for powers that aim to take on a leading role in the regional security agenda. It also represents overlapping planning and execution costs. Again, there is a competitive aspect in cooperation proposals and little convergence of objectives.

Finally, there is also a scattering of different maritime monitoring systems in each of the region's countries in cooperation with various external partners. A crucial aspect for strengthening maritime security in the region is improving the capacity to monitor vessel traffic, which allows to identify critical action and quick response areas. In recent years, what has been observed is an advance of bilateral partnerships between countries in the region and external actors that offer their systems individually, generating a diversity of systems in operation.

These three cooperation modalities highlight the problem of overlapping resources and initiatives without tangible improvement in the region's security scenario.

What to do then? It can be seen that South America and Europe share at least three common interests in the Atlantic sub-complex of the Gulf of Guinea: providing security and stability to maritime routes (with piracy as the main obstacle); a concern about increasing the operational capacities of the region's riparian countries; and increasing their strategic presence in the region, to ensure their diplomatic and symbolic position as priority partners in South Atlantic security. Coordinated action between these two counterparts could help advance the current, fragmented and diffused model towards a stable joint presence, with shared gains among all actors involved.

This is made clear, for example, by the experience in the Gulf of Aden. Even though they are zones with different geopolitical characteristics and obstacles[13], it is possible to learn lessons from that scenario for use in the Gulf of Guinea in the South Atlantic. The creation of a maritime transit corridor, the sharing of navigation information, the dissemination of good practices among State and private actors, and the presence of international patrols coordinated with local countries were some of the elements that favoured a significant reduction in pirate attacks in the Indian Ocean (ANYIMADU, 2013) and could be replicated, with adjustments, in the Gulf of Guinea setting. Europe and South America have the material conditions and political capital needed to lead this process in close cooperation with riparian countries.

The most decisive action that changed the security scenario of the Gulf of Aden was the creation of a joint naval force, the Combined Maritime Force. Thirty-four countries formed an extensive joint force of maritime patrol, with rotating leadership and naval assets. It works, therefore, as a collaborative patrolling project, with shared but differentiated responsibilities. Its mandate is flexible and renewable, with a decision-making body that actively involves the region's countries.

[13] Two logistical differences, for example, have pragmatic implications: in the Gulf of Aden, most attacks take place in international waters, while in the Gulf of Guinea they take place in territorial waters, which presents different legal, bureaucratic and operational implications. Secondly, attacks on the Somali coast generally involved the hijacking of vessels and hostages for ransom, while in the Gulf of Guinea attacks focused on cargo theft, particularly from vessels carrying oil.

iniciativa para poder exercer sua influência sobre as questões de segurança da região. Se essa sobreposição permite, em tese, difundir boas práticas de segurança, por outro lado, funciona como palco de exibição de forças navais para potências que almejam assumir protagonismo na agenda de segurança regional. Representam, também, custos de planejamento e de execução sobrepostos. Novamente, verifica-se o aspecto concorrencial entre propostas de cooperação e pouca convergência de objetivos.

Por fim, nota-se também a difusão de diversos sistemas de monitoramento marítimo em cada um dos países da região, em cooperação com diversos parceiros externos. Um aspecto crucial para o fortalecimento da segurança marítima na região é o aprimoramento da capacidade de monitoramento do tráfego de embarcações, o que permite identificar áreas críticas de atuação e resposta rápida. O que se verifica, nos últimos anos, é o avanço de parcerias bilaterais entre países da região e atores externos que ofertam seus sistemas de forma individualizada, gerando multiplicidade de sistemas em operação.

Essas três modalidades de cooperação evidenciam o problema da sobreposição de recursos e iniciativas, sem que haja uma melhora palpável no cenário securitário da região.

O que fazer então? Percebe-se que América do Sul e Europa compartilham pelo menos de três interesses em comum no subcomplexo atlântico do Golfo da Guiné: prover segurança e estabilidade das rotas marítimas (tendo a pirataria como obstáculo principal); preocupação em aumentar as capacidades operacionais dos países ribeirinhos da região; e o aumento da presença estratégica na região, de forma a assegurar sua posição diplomática e simbólica como parceiros prioritários da segurança sul-atlântica. Uma ação coordenada entre essas duas contrapartes poderia contribuir para que o atual modelo evolua, fragmentado e difuso, em direção a uma presença estável e coordenada, com ganhos compartilhados entre todos os atores envolvidos.

É o que evidencia, por exemplo, a experiência do Golfo de Áden. Ainda que sejam zonas com características geopolíticas diferentes e obstáculos diversos[13], é possível extrair lições daquele cenário para serem aplicadas ao Golfo da Guiné, no Atlântico Sul. A criação de um corredor de trânsito marítimo, o compartilhamento de informações de navegação, a difusão de boas práticas entre atores estatais e privados e a presença de patrulhas internacionais coordenadas com países locais foram alguns dos elementos que favoreceram uma queda expressiva nos ataques piratas no Oceano Índico (ANYIMADU, 2013) e poderiam ser replicados, com adaptações, ao cenário do Golfo da Guiné. Europa e América do Sul possuem condições materiais e capital político para liderar esse processo, em estreita cooperação com países ribeirinhos.

A experiência mais decisiva para modificar o cenário securitário do Golfo de Áden foi a criação de uma força naval comum, a *Combined Maritime Force*. Ali, trinta e quatro países

[13] Duas diferenças logísticas, por exemplo, possuem implicações pragmáticas: no Golfo de Áden a maior parte dos ataques ocorre em águas internacionais, enquanto no Golfo da Guiné acontece em águas territoriais, o que tem implicações legais, burocráticas e operacionais diferentes. Em segundo lugar, os ataques na costa somali geralmente envolviam o sequestro de embarcações e reféns visando resgate, enquanto no Golfo da Guiné os ataques se concentram em roubo de carga, principalmente de embarcações que transportam petróleo.

Creating such a force in the Gulf of Guinea is no simple task. It entails bureaucratic procedures, a willingness to provide naval resources, and raises political, domestic, and international sensitivities, especially concerning the sovereignty of territorial waters. In the long run, the ambition to strengthen the operational capacity of regional navies must remain the main objective of multilateral cooperation. This, however, demands time and resources. In the short run, the swiftest way to reduce the scale of pirate attacks in the region would be the coordinated use of local and extra-regional forces.

This is because creating a stable maritime presence tackles precisely the excessively fragmented and discontinued nature of cooperation initiatives in the region. Many of the cooperation projects carried out in recent years are *ad hoc,* subject to budgetary or political variations. As a result, they are discontinued after some time, despite their initial broad ambitions.[14] Creating a force with a clear mandate for action and presence would mean an essential step in replacing this rationale with more stable cooperation, capable of delivering a genuinely effective governance model. In this way, it would be a project capable of galvanizing other initiatives that could then orbit and converge towards a unified project.

Indeed, some countries have already shown a willingness in this regard: the launch of the "coordinated maritime presence" by the EU, in partnership with Gabon, in 2021, is a step in this direction. As much as possible, it should include more actors, mainly from South America, clearly prioritising Brazil, Argentina, and Uruguay, precisely in an attempt to give greater multilateral scope to the project and thus avoid competition between similar initiatives. Recent forums, such as the G7++FoGG meetings, have demonstrated that there is a local demand for this type of solution as well as the political will from extra-regional actors to offer such cooperation. Bureaucratic differences (which require legislation updating) and political sensitivities (concerning issues of sovereignty and legitimacy) are hurdles that can hinder the creation of such a model of cooperation, but which, as the experience in the Gulf of Aden shows, are not insurmountable. It can also be seen that European and South American countries' shared leadership can be a critical symbolic factor in reducing the incidence of extra-regional rivalries in the region — especially between the US and China.

Actions such as offering training should therefore be complementary to this coordinated presence. Furthermore, seeking to design a common curriculum is imperative, as is promoting the merger of training programs provided to African countries by actors such as Brazil, the United Kingdom, France, etc. In this way, instead of competing with each other, projects offering training can be complementary and contribute to them as an element that can bring military forces closer and enhance the capacities of local actors.

Likewise, a lack of system interoperability, harmony and information exchange, mentioned above, significantly increases transaction costs to solve the same problem

[14] ZOPACAS (South Atlantic Peace and Cooperation Zone), a Brazilian initiative to project itself as a leader in defence and security in the South Atlantic, is a crucial example of this trajectory. Created in 1986, it hibernated for most of the 1990s, was revitalized in the mid-2000s, as part of emerging Brazil's renewed ambitions, but lost momentum again after 2013 (PIMENTEL, 2016).

formaram uma força conjunta de patrulha naval extensiva, com rotatividade de liderança e de presença de meios navais. Funciona, portanto, como um projeto conjunto de patrulhamento, com responsabilidades compartilhadas, porém diferenciadas. Seu mandato é flexível e renovável, contando com corpo decisório que envolve os países da região de forma ativa.

A criação de uma força desse tipo no Golfo da Guiné não é tarefa simples. Envolve trâmites burocráticos, disposição em ceder recursos navais e desperta sensibilidades políticas, domésticas e internacionais, principalmente no tocante à soberania de águas territoriais. No longo prazo, a ambição de fortalecer a capacidade de operação das marinhas locais deve permanecer como o objetivo principal da cooperação multilateral. Isso, contudo, demanda tempo e recursos. No curto prazo, a forma mais expedita de reduzir a escalada de ataques piratas na região seria o uso coordenado de forças locais e extrarregionais.

Isso porque a criação de uma presença marítima estável ataca justamente o caráter excessivamente fragmentado e descontinuado das iniciativas de cooperação na região. Muitos dos projetos de cooperação realizados nos últimos anos são *ad-hoc,* sujeitos a oscilações orçamentárias ou políticas, e são descontinuados após algum tempo, apesar de suas amplas ambições iniciais[14]. A criação de uma força com um mandato claro de ação e presença representaria um passo essencial na substituição dessa lógica por uma cooperação mais estável, capaz de entregar um modelo de governança realmente efetivo. Seria, nesse sentido, um projeto com capacidade de galvanizar outras iniciativas que poderiam então orbitar e convergir para um projeto unificado.

De fato, alguns países já sinalizaram alguma disposição nesse sentido: o lançamento da *"coordinated maritime presence"* pela UE, em parceria com o Gabão, em 2021, representa um passo nessa direção. Deveria, na medida do possível, incorporar mais atores, principalmente da América do Sul, com prioridades evidentes, do Brasil, Argentina e Uruguai, justamente em uma tentativa de dar maior amplitude multilateral ao projeto e, assim, evitar concorrência entre iniciativas semelhantes. Foros recentes, como os encontros do G7++FoGG, demonstraram que há demanda local por esse tipo de solução e há vontade política de atores extrarregionais em ofertar tal cooperação. Divergências burocráticas (que demandam atualização da legislação) e sensibilidades políticas (relativas a questões de soberania e legitimidade) são obstáculos que podem emperrar a criação de tal modelo de cooperação, mas que, como demonstra a experiência no Golfo de Áden, não são insuperáveis. Nota-se, inclusive, que a liderança compartilhada de países europeus e sul-americanos pode ser um fator simbólico importante para reduzir a incidência de rivalidades extrarregionais (sobretudo entre EUA e China) na região.

Ações como a oferta de treinamento devem ser, portanto, complementares a essa presença coordenada. É imperativo, ademais, que se busque a formulação de um currículo comum ou que se promova a fusão de programas de treinamento ofertados aos países africanos por atores como Brasil, Reino Unido, França etc. Dessa forma, ao invés

[14] A ZOPACAS, iniciativa brasileira de se projetar como líder em defesa e segurança do Atlântico Sul, é um exemplo crucial dessa trajetória. Criada em 1986, ficou hibernada durante boa parte dos anos 1990, foi revitalizada em meados dos anos 2000, parte das ambições renovadas do Brasil emergente, porém perdeu dinamismo, novamente, depois de 2013 (PIMENTEL, 2016).

since such systems are mostly offered by bilateral partnerships. The YARIS system, proposed within the framework of the Yaoundé Architecture, should, as of 2021, create such an integrated information-sharing network. It is similar to the system adopted in the Gulf of Aden by means of the SHADE platform (Shared Awareness and Deconfliction), which, in theory, should unify the information coming from a complex network of 27 observation centres. This mostly European initiative, funded by France and Demark, should expand its cooperation scope with South American countries, integrating them into the network and disseminating information as a sign of trust building and increasing interoperability that can lead to an ostensive, direct presence in the near future. Countries like Brazil, which currently offers its maritime monitoring system (SISTRAM) to countries like Cameroon and Angola, could participate in the Yaoundé Architecture and thus work towards a complementarity of European and South American initiatives.

Harmonizing these concerns and building an architecture that meets the legitimate sovereign interests of the actors involved can be an essential step towards consolidating an effective naval force in the region. Coordinating initiatives can lead to a better allocation of resources, more mature governance networks, and, consequently, better results, including diverse actors and fulfilling collective and individual agendas. Some kind of "specialisation" of cooperation can also be welcome. It is a fact that countries perform differently, depending on the cooperation modality chosen: some countries are better prepared to offer a particular type of training and suffer less local resistance to providing this type of cooperation, as shown by Brazil's and Portugal's recent success in this area (ABDENUR; NETO, 2014); other countries, such as the USA, or the EU, naturally have a greater capacity to provide and maintain naval assets[15]; there are also actors with a less direct presence in the region, but with great willingness to finance cooperation initiatives, such as the Scandinavian countries. Unfortunately, Europeans and South Americans, who have focused on the competitive aspects of cooperation, have so far underexploited this complementarity. Overcoming a maximalist logic, in which all countries try to increase their presence on all cooperation fronts, with a rationale of complementarity, may be the correct path towards creating a more solid regional governance architecture.

Combining efforts around a specific security issue can drive a convergence of the two continents in other areas, serving as a model of constructive interdependence. It is not feasible to believe that sensitive points in the South Atlantic relationship between Europe and South America — such as the Falklands/Malvinas' sovereignty — will be resolved in the short or medium run. However, the existence of these differences does not prevent cooperation on specific issues ("issue-specific security policy"), as in the case of the Gulf of Guinea. In fact, within a security governance architecture, more than creating an organisation or a regime that encompasses all the strategic aspects of a game board, it is natural that cooperation takes place around specific themes, where collective gains are accessible to all actors. Furthermore, effective collaboration

[15] It is noted that Brazil, despite the scarcity of surplus military power, has a successful experience in the UNIFIL naval mission, an expertise that could be replicated in the South Atlantic, precisely an area in which the country wants to project itself as a regional leader.

de concorrerem entre si, esses projetos de oferta de treinamento podem ser complementares e contribuírem como elemento de estreitamento entre forças militares e de aumento das capacidades dos atores locais.

Igualmente, a falta de interoperabilidade e harmonização de sistemas e de troca de informação, citados anteriormente, aumenta significativamente os custos de transação para resolver o mesmo problema, já que tais sistemas são ofertados majoritariamente por meio de parcerias bilaterais. O sistema YARIS, proposto dentro do marco da Arquitetura de Yaoundé, deverá, a partir de 2021, criar essa rede integrada de compartilhamento de informações. Trata-se de sistema parecido com o adotado no Golfo de Áden, por meio da plataforma SHADE (*"Share Awareness and De-confliction"*), que deve, em tese, unificar as informações provenientes da complexa rede de 27 centros de observação. Essa iniciativa majoritariamente europeia, patrocinada com fundos franceses e dinamarqueses, deveria ampliar seu escopo de cooperação com países sul-americanos, integrando-os à rede e usando a difusão de informações como um sinal de construção de confiança e de aumento de interoperabilidade, que podem caminhar na direção de uma presença ostensiva direta em um futuro próximo. Países como o Brasil, que atualmente oferta o seu próprio sistema de monitoramento marítimo (SISTRAM) a países como Camarões e Angola, poderiam integrar a Arquitetura de Yaoundé e, assim, trabalhar pela complementariedade de iniciativas europeias e sul-americanas.

Harmonizar essas preocupações e construir uma arquitetura que atenda aos interesses soberanos legítimos dos atores envolvidos pode ser um passo importante para a consolidação de uma força naval efetiva na região. A coordenação de iniciativas pode levar a uma melhor alocação de recursos, amadurecimento de redes de governança e, consequentemente, melhores resultados, incluindo diversos atores e satisfazendo agendas coletivas e individuais. Algum tipo de "especialização" da cooperação também pode ser bem-vindo. É fato que países performam de modo diferente, a depender da modalidade de cooperação escolhida: alguns países possuem maior vocação para oferecer determinado tipo de treinamento e sofrem menos resistências locais para prestar esse tipo de cooperação, como. por exemplo. o sucesso recente do Brasil nessa seara (ABDENUR; NETO, 2014) ou o de Portugal; outros países, como os EUA ou a EU, possuem, naturalmente, maior capacidade para disponibilizar e manter meios navais[15]; há, ainda, aqueles atores com menor presença direta na região, porém com forte disposição de financiar iniciativas de cooperação, como os países nórdicos. Essa complementariedade foi, até o momento, subexplorada por europeus e sul-americanos, que até o momento se focaram nos aspectos concorrenciais da cooperação. A superação de uma lógica maximalista, onde todos os países tentam aumentar sua presença em todas as frentes de cooperação, por uma lógica de complementariedade, pode ser um caminho para a criação de uma arquitetura mais sólida de governança regional.

A combinação de esforços em torno de um tema específico de segurança pode impulsionar a aproximação dos dois continentes em outras áreas, servindo de modelo de interdependência construtiva. Não é factível acreditar que pontos sensíveis da relação

[15] Anota-se que o Brasil, apesar da escassez de excedentes de poder militar, possui uma experiência de sucesso na missão naval da UNIFIL, *expertise* que poderia ser replicada no Atlântico Sul, justamente uma área em que o país deseja se projetar como líder regional.

around the security of the Gulf of Guinea can have a catalytic effect in building trust between Europe and South America, with spillover effects on other strategic matters.

This brief paper has tried to demonstrate that the geographic, political, and strategic condition of the South Atlantic, particularly its dynamic core in the Gulf of Guinea, has led to a specific type of security governance that has achieved suboptimal results. All actors seem willing to increase their regional presence and engage in cooperation projects; however, overlapping efforts and the competitive dimension of initiatives may not necessarily result in more security. An attempt has also been made to demonstrate that it is possible to overcome this impasse by means of more predictable cooperation, which goes beyond *ad hoc* logic and individualised projects, fostering an ambitious vision of maritime presence and complementarity of actions between European and South American partners operating in the region. However, these are bold goals as demonstrated by other strategic and feasible scenarios favouring the overcoming of rivalries and insecurities affecting the common goods that share the use of the South Atlantic's maritime routes and its resources.

Bibliography

ABDENUR, A.; MARCONDES, D. Rising Powers and the Security-Development Nexus: Brazil's Engagement with Guinea-Bissau. ***Journal of Peacebuilding & Development***, v. 9. n. 2, p. 1-16, 2014.

ADLER, E.; STRIKE, P. When Security Community Meets Balance of Power: Overlapping Regional Mechanisms of Security Governance***. Review of International Studies***, v. 35, n. 1, p. 59-84, 2009.

ANYIMADU, A. Maritime Security in the Gulf of Guinea: Lessons Learned from the Indian Ocean. Chatham House, 2013. Available in: <https://tinyurl.com/8jnr56pf>. Accessed on May 31, 2021.

DREZNER, D. The Power and Peril of International Regime Complexity. *Perspective on Politics*, v. 7, n. 1, p. 65-70, 2009.

KIRCHNER, E.; SPERLING, J. *EU Security Governance*. Manchester: Manchester University Press, 2008.

LE MIÈRE, C. *Maritime Diplomacy in the 21st Century: Drivers and Challenges*. London: Routledge, 2014.

SACHAR, B. S, Cooperation in Military Training as a Tool of Peacetime Military Diplomacy. ***Strategic analysis***, v. 27, n. 3, p.404-421, 2003.

PIMENTEL, C. O Ressurgimento da Zopacas e a Agenda de Segurança no Atlântico Sul. *Tensões Mundiais***,** v. 12, n. 22, p. 113-143, 2016.

sul-atlântica entre Europa e América do Sul — como a soberania das Ilhas Malvinas/Falklands, por exemplo — serão resolvidos no curto ou médio prazo. A existência dessas diferenças não impede, contudo, a cooperação em torno de temas específicos ("issue-specific security policy"), como o caso do Golfo da Guiné. Na verdade, dentro de uma arquitetura de governança da segurança, mais do que a criação de uma organização ou um regime que abranja todos os aspectos estratégicos de um tabuleiro, é natural que a cooperação se realize em torno de temas específicos, onde os ganhos coletivos são acessíveis a todos os atores. No mais, uma cooperação efetiva em torno da segurança do Golfo da Guiné pode ter um efeito catalizador de criação de confiança entre Europa e América do Sul, com efeito transbordante para outros assuntos estratégicos.

Este breve *paper* tentou demonstrar que as disposições geográficas, políticas e estratégicas do Atlântico Sul, e em particular de seu núcleo dinâmico no Golfo da Guiné, levaram a um determinado tipo de governança da segurança que tem alcançado resultados subótimos. Todos os atores parecem dispostos a aumentar a sua presença regional e engajarem-se em projetos de cooperação; porém, a sobreposição de esforços e a dimensão concorrencial entre diferentes iniciativas podem não necessariamente resultar em mais segurança. Tentou-se demonstrar, também, que é possível superar esse impasse por meio de uma cooperação mais previsível, que supere a lógica *ad-hoc* e individualizada dos projetos, em prol de uma visão ambiciosa de presença marítima e de complementariedade de ações entre parceiros europeus e sul-americanos atuando na região. São objetivos audaciosos, porém, como demonstram outros cenários estratégicos e exequíveis, em prol da superação de rivalidades e da insegurança que afeta bens comuns que compartilham o uso das rotas marítimas e dos recursos do Atlântico Sul.

Bibliografia

ABDENUR, A.; MARCONDES, D. Rising Powers and the Security-Development Nexus: Brazil's Engagement with Guinea-Bissau. *Journal of Peacebuilding & Development*, v. 9. n. 2, p. 1-16, 2014.

ADLER, E.; GREVE, P. When Security Community Meets Balance of Power: Overlapping Regional Mechanisms of Security Governance. *Review of International Studies*, v. 35, n. 1, p. 59-84, 2009.

ANYIMADU, A. Maritime Security in the Gulf of Guinea: Lessons Learned from the Indian Ocean. Chatham House, 2013. Disponível em: <https://tinyurl.com/8jnr56pf>. Acesso em 31 maio 2021.

DREZNER, D. The Power and Peril of International Regime Complexity. *Perspective on Politics*, v. 7, n. 1, p. 65-70, 2009.

KIRCHNER, E.; SPERLING, J. *EU Security Governance*. Manchester: Manchester University Press, 2008.

LE MIÈRE, C. *Maritime Diplomacy in the 21st Century: Drivers and Challenges*. London: Routledge, 2014.

SACHAR, B. S. Cooperation in Military Training as a Tool of Peacetime Military Diplomacy. *Strategic Analysis*, v. 27, n. 3, p .404-421, 2003.

PIMENTEL, C. O Ressurgimento da Zopacas e a Agenda de Segurança no Atlântico Sul. *Tensões Mundiais*, v. 12, n. 22, p. 113-143, 2016.

Bárbara Campos Diniz

Mestre em Política Internacional: inteligência, estratégia e combate ao terrorismo e bacharela em Relações Internacionais pela PUC Minas, Brasil. Assistente Editorial da Revista Relações Exteriores e E-Relações Internacionais. Pesquisadora membro do TRAC, CEPDE e ISAPE.

Master in International Politics: intelligence, strategy and counterterrorism and BA in international Relations from PUC Minas, Brazil. Assistant Editor at Revista Relações Exteriores and E-International Relations. Research member of TRAC, CEPDE and ISAPE.

O que podemos aprender com a UE? Políticas e Práticas Contemporâneas de Combate ao Terrorismo no Mercosul

What can we learn from the EU? Contemporary Counterterrorism Policies and Practices in Mercosur

Bárbara Campos Diniz

Sumário Executivo

O combate ao terrorismo vem sendo um dos principais objetivos da agenda de segurança internacional desde o início dos anos 2000, em consequência dos ataques terroristas de 11 de setembro nos Estados Unidos, dos atentados ocorridos na Europa em seguida e da instabilidade nas regiões do Oriente Médio e da África do Norte. A globalização e as redes sociais também contribuíram para acelerar o processo de recrutamento, radicalização e coordenação de células em todo o mundo, e facilitaram ainda a cooperação tanto entre organizações quanto com o crime organizado. O terrorismo constitui uma ameaça que nenhum Estado é capaz de enfrentar sozinho. Exige grande esforço de coordenação e cooperação multilateral para que seja eficaz. De acordo com o Banco de Dados Global sobre o Terrorismo (GTD), entre 2001 e 2018, 119.806 atentados terroristas ocorreram no mundo. Nem a Europa nem as Américas constituem o epicentro das atividades relacionadas ao terrorismo, uma vez que sofreram somente 2,9% dos atentados. No entanto, a partir dos últimos anos, a instabilidade política e social na região abriu espaço para o financiamento do terrorismo.

Executive Summary

Countering terrorism has been one of the main goals in the international security agenda since the early 2000s, after the 9/11 terrorist attacks in the US, the subsequent attacks in Europe, and the instability in the MENA region. Globalisation and social media have also helped to accelerate the process of recruitment, radicalisation, coordination of cells around the world, and facilitated cooperation not only between these organisations, but with organised crime as well. Terrorism is a threat that no state can mitigate on its own, therefore demanding that multilateral coordination and cooperation efforts be effective. According to the Global Terrorism Database (GTD), between 2001 and 2018 there was a total of 119,806 terrorist attacks committed worldwide. Much like Europe, the Americas are not a "hotspot" for terrorism-related activities, having suffered only 2,9% of these attacks. However, as of recent years, political and social instability in the region have opened up space for the financing of terrorism.

The lack of regionally coordinated efforts to counter terrorism in South America leaves the region vulnerable to terrorism-related activities, such as terrorism financing, money laundering, weapons trade, etc. Even though it is not its objective, Mercosur's lack of regional security policies, especially regarding terrorism, directly affects its efforts to establish a South American common market and to amplify its regional integration efforts. In addition to the ever-increasing transnational nexus between terrorism and organised crime, such security instabilities radically affect direct interest and investments in the region, diminishing its potential as a trade partner and damaging its economy. Thus, this paper suggests the incorporation of the South American Security Coordinator (SASC) through which agencies can monitor and facilitate the exchange of information and coordinate efforts to mitigate terrorism and organised crime within the Mercosur member states. The SASC is based substantially on the European Union's counterterrorism structures, but significantly adapted to the South American context.

Context and Issue

Before discussing the imminent threat that terrorism and organised crime pose to South American development, it is important to point out the institutional and integrational disparities between the European Union and Mercosur to better understand how a SASC could be set up. Even though the processes of regional integration have been increasingly fast-paced since the early 2000s, the objectives and the structures of the organisations themselves are alternatively complex and different, depending on the demands of the member states, the context and the region where they were created. The European process of regional integration started after World War II as an effort to recover the economy of the states affected by the war. Over decades, this integration has spilt over to other areas not closely related to a common market, such as education, the environment and regional security. Mercosur, on the other hand, since its inception in the late 1990s, has been intended to establish and expand a common market among its member states, not having had a thematic spillover as did the EU.

In addition to the intentions behind the creation of the organisations varying, there are key differences between the EU and Mercosur that affect not only decision-making and policy-making but the overall implementation of the policies as well. On the one hand, the EU is a supranational organisation, whereas Mercosur is an intergovernmental organisation. In other words, the European institutions are not directly controlled by the member states, existing and operating outside and above domestic boundaries, in which most legislative acts are binding on all member states. On the other hand, Mercosur's structure is very different to the EU's, having intergovernmental institutions with representatives of its member states. Thus, decision-making and policy-making in Mercosur are completely intergovernmental, depending on representatives directly linked to the government of the member states.

Countering terrorism within such different organisational structures is a challenge. Terrorism is not a new phenomenon and presents a set of challenges to contemporary

A ausência de esforços coordenados no âmbito regional para enfrentar essa ameaça na América do Sul deixa a região vulnerável a atividades relacionadas ao terrorismo, tais como o seu financiamento, a lavagem de dinheiro, o comércio de armas etc. Ainda que não seja seu objetivo primordial, a falta de políticas regionais de segurança por parte do Mercosul, principalmente no que se refere ao combate ao terrorismo, afeta diretamente os esforços para o estabelecimento de um mercado comum na América do Sul e para o aprofundamento de uma integração regional. Além de contribuírem para o fortalecimento do vínculo transnacional entre terrorismo e crime organizado, a instabilidade na esfera da segurança afeta diretamente os investimentos diretos e o interesse pela região, diminuindo seu potencial como parceiro comercial e de desenvolvimento econômico. Assim, este artigo sugere a incorporação da Coordenação de Segurança da América do Sul (CSAS), através do qual as agências poderão monitorar e facilitar o intercâmbio de informações e coordenar esforços para o combate ao terrorismo e o crime organizado entre os Estados Membros do Mercosul. A CSAS se baseia nos pilares das estruturas de contraterrorismo da União Europeia, porém profundamente adaptado ao contexto sul-americano.

O Contexto e a Questão

Antes de discutir a ameaça iminente que o terrorismo e o crime organizado representam para o desenvolvimento da América do Sul, é importante apontar as disparidades institucionais e integracionais entre a União Europeia e o Mercosul para melhor compreender como a CSAS poderia ser estruturada. Embora os processos de integração regional venham sendo acelerados desde o início dos anos 2000, os objetivos e a estrutura de cada organização são tão complexos quanto distintos, dependendo das demandas de cada Estado-membro, do contexto e da região onde foram criadas. O processo de integração regional na Europa teve início após a Segunda Guerra Mundial com o objetivo de recuperar a economia dos países afetados pela guerra. Ao longo de décadas, a integração foi se disseminando para outras áreas não diretamente relacionadas ao mercado comum, como educação, meio ambiente e segurança regional. O Mercosul por sua vez, tem procurado, desde de sua fundação no final da década de 1990, estabelecer e ampliar um mercado comum entre seus Estados-membros, mas não experimentou a mesma disseminação para outras áreas como foi o caso na UE.

Além das diferenças entre as intenções que impulsionaram a criação das organizações, existem diferenças fundamentais entre a UE e o Mercosul que exercem impacto tanto sobre os processos de tomada de decisões e de formulação de políticas, quanto sobre a implementacão geral das políticas públicas. A UE é uma organização supranacional, enquanto o Mercosul é uma organização intergovernamental. Em outras palavras, as instituições europeias não são diretamente controladas pelos Estados-membros. Elas existem e operam fora e acima dos limites nacionais, onde a maior parte dos atos legislativos produzem efeito jurídico sobre todos os Estados-membros. Por outro lado, a estrutura do Mercosul é muito diferente daquela da UE, formada por instituições intergovernamentais com representantes de seus Estados-membros. Assim, os processos de tomada de decisão e de formulação de políticas no Mercosul possuem um caráter profundamente intergovernamental e dependem de representantes diretamente ligados aos governos dos Estados-membros.

international relations and regional organisations, such as the lack of a universally agreed-upon definition, transnationalisation via social media and the internet, recruitment and radicalisation, and terrorism financing. As previously mentioned, even though the number of attacks in the American continent is low, South America has a vulnerability regarding the nexus between terrorism and organised crime, the financing of terrorism, as well as narcoterrorism.

Narcoterrorism is defined as terrorist actions against the state to intimidate law enforcement in order to delay or cancel drug trafficking-related operations. It is understood as an attempt by organised crime to influence a government and a society through the systematic threat of violence and fear. Nowadays, the term is also used to describe extremist organisations that use drug trafficking as a means to finance their operations. Within the confines of Mercosur, Brazil can be recognised as the epicentre of this specific type of political violence, because of the myriad of organised crime and drug trafficking organisations within its territory, and FARCs on the borders in the Amazon region.

Are the Current Policy Options Enough?

As previously mentioned, the European integration process has spilt over other problem areas along the years, and countering terrorism has been an increasingly invested area since 9/11. After discovering that part of the planning and execution of the Al-Qaeda attacks in the US were made in Europe, Europol and other EU institutions reshaped the bloc's entire counterterrorism structure in an attempt to homogenise policies, efforts and get better results. Besides establishing specific structures and groups to deal with counterterrorism, EU policymakers were successful in agreeing on a definition of terrorism and terrorists specific enough to contemplate their context, but wide enough to be adaptable to the member states' specific domestic contexts. This definition is the cornerstone of the whole structure, influencing policies and practices alike.

Another important assessment made by the EU culminated in the organisation's Counterterrorism Strategy Framework, which set up several goals for the organisation and its member states to better counter terrorism as a bloc. Even though the strategies are updated annually, the four pillars established in the early 2000s have not changed and neither have the two main objectives derived from the strategies: cooperation and the strengthening of individual capabilities. One of the biggest challenges for Mercosur's member states (and to Brazil specifically), is the porosity of their borders, which is being taken advantage of by organised crime. Even though many South American states have cooperation treaties, many of the operations are executed bilaterally instead of multilaterally.

Besides definitions, the EU has also established a task force within Europol that monitors and aids in information sharing regarding terrorism in the region. The valuable TE-SAT reports not only present the overall context, findings and terrorism trends but also inform member states and citizens alike about the number of people arrested and tried for terrorism as well as establishing terrorism typologies to help understand

O enfrentamento ao terrorismo nesse contexto caracterizado por estruturas organizacionais tão diferentes constitui uma tarefa difícil. O terrorismo não é um fenômeno novo e apresenta uma série de complexidades para as relações internacionais contemporâneas e organizações regionais, como a falta de uma definição universalmente aceita, transnacionalização através das redes sociais e da internet, recrutamento e radicalização e financiamento. Como mencionado anteriormente, embora o número de atentados no continente americano seja baixo, a América do Sul apresenta vulnerabilidade quanto aos vínculos entre o terrorismo e o crime organizado, o financiamento do terrorismo e o narcoterrorismo.

O narcoterrorismo é definido como ações terroristas contra o Estado com o objetivo de intimidar as autoridades e atrasar ou cancelar operações de repressão ao tráfico de drogas. É interpretado como a tentativa por parte do crime organizado de exercer influência sobre um governo e uma sociedade através de ameaças sistemáticas, violência e intimidação. Atualmente, o termo também é usado para descrever organizações extremistas que se utilizam do narcotráfico fara financiar suas operações. No território do Mercosul, o Brasil pode ser definido como o epicentro desse tipo específico de violência política, por conta do grande número de organizações envolvidas no crime organizado e no narcotráfico, e devido à presença das FARCs nas fronteiras da região amazônica.

As opções de política atuais são suficientes?

Conforme mencionado anteriormente, o processo de integração europeia disseminou-se para outras áreas de atuação ao longo dos anos, e o combate ao terrorismo vem recebendo cada vez mais investimentos desde os atentados de 11 de setembro. Depois de revelado que parte do planejamento e execução dos ataques da Al-Qaeda nos EUA foi realizada na Europa, a Europol e outras instituições da UE reformaram toda a estrutura de contraterrorismo do bloco para harmonizar as políticas e os esforços e obter melhores resultados. Além do estabelecimento de estruturas e grupos específicos para tratar do combate ao terrorismo, os gestores de políticas públicas da UE conseguiram um consenso em torno de uma definição para o terrorismo e terroristas que é ao mesmo tempo específica o suficiente para contemplar diversos contextos e ampla o suficiente para se adaptar aos contextos nacionais específicos de cada Estado-membro. Essa definição é o pilar de toda a estrutura e influencia tanto políticas quanto práticas.

Outra avaliação importante feita pela UE culminou na Estrutura Estratégica de Combate ao Terrorismo que estabelece diversas metas para a organização e para os Estados-membros com o intuito de aprimorar o enfretamento ao terrorismo como um bloco. Embora as estratégias sejam atualizadas anualmente, nem os quatro pilares estabelecidos no início dos anos 2000 mudaram, nem os dois principais objetivos derivados das estratégias foram alterados: a cooperação e o fortalecimento das capacidades individuais. Um dos maiores desafios dos países membros do Mercosul (e, mais especificamente, do Brasil) é a porosidade das fronteiras, utilizada pelo crime organizado em seu benefício. Embora muitos países da América do Sul tenham tratados de cooperação, muitas das operações são realizadas bilateralmente, ao invés de se adotar uma abordagem multilateral.

what kind of terrorism is most present in the region. These reports are also valuable because they can aid in adjusting policies and allocating resources according to the threat. Within Eurojust, the EU also created the Terrorism Convictions Monitor that collects in-depth information regarding the trials of individuals accused of terrorism and terrorism-related activities. All in all, the counterterrorism structure in the EU is vast and complex, ranging from societal, political, financial, and environmental to educational sectors. In retrospect, these security policies are adequate to maintain not only the stability of the bloc but also to shape counterterrorism efforts within democratic standards and societal values, extracting the issue from a heavily securitised perspective and subjecting it to the rule of law.

In 2002, Mercosur's member states agreed on the General Plan on the Reciprocity of Cooperation and Coordination for Regional Security between the Member States, in which Chapter 7 establishes policies to counter terrorism, such as the creation of a Working Group Specialised in Terrorism within the Permanent Working Groups' umbrella (that meets biannually), then creates an Integrated System for the Exchange of Information, exchange of experience, training and human resources to deal with terrorism and to prepare domestic task forces, identify actors whose interests lie on international terrorism, and establish a Model Exchange Information Form to aid in terrorism-related investigations. One of the interesting points of the latter — and one of the most problematic — is that in this chapter itself it is emphasised that states are allowed to require information on the refugee status of the person under investigation, therefore presupposing that the perpetrator is a foreigner.

Arguably, it is not Mercosur's objective to counter terrorism. However, with the strong presence of transnational organised crime and terrorism financing in the region, it is time to create a structure that works and works well in order for its member states and associates to stabilise the region. One of the major challenges that regional security faces nowadays is the intergovernmental structure on which Mercosur was created. Because all the member states have to agree with decisions and internalise them within their legal systems, there has been a constant delay in the implementation of security practices in the region.

Policy Recommendations

To counter terrorism and organised crime within the member states of Mercosur, it is proposed to establish a robust and functioning institution that works within the intergovernmental structure of Mercosur: the South American Security Coordinator (SASC). The SASC would be a transnational institution encompassing academics and policy-makers alike to better comprehend the security threats South America is facing and to develop strategies on how to better mitigate them in a coordinated and cooperative manner. Furthermore, the SASC would be a consulting institution, much like a think tank, as a tool for further integration and to assure the safety of the people and the states.

The importance should be emphasised of an institution that deals not only with the threat and nexus of terrorism and organised crime in the region, but that is

Além das definições, a UE também criou uma força-tarefa dentro da Europol que monitora e auxilia no compartilhamento de informações sobre o terrorismo na região. Os importantes relatórios do TESAT não somente apresentam o contexto geral, as investigações e as tendências do terrorismo, mas também informam os Estados-membros e os cidadãos sobre o número de pessoas detidas e julgadas por terrorismo, além de estabelecer tipologias de terrorismo para melhor compreender quais são as formas mais prevalentes na região. Os relatórios também são fundamentais, pois podem ajudar no ajuste das políticas e na alocação de recursos de acordo com a ameaça. No âmbito da Eurojust, a UE também criou o Monitoramento de Sentenças em Matéria de Terrorismo, que coleta informações detalhadas sobre os processos de indivíduos acusados de terrorismo e de atividades relacionadas com o terrorismo. Em sua totalidade, a estrutura de enfrentamento ao terrorismo na UE é vasta e complexa, abrangendo setores sociais, políticos, financeiros, ambientais e educacionais. Em retrospectiva, as políticas de segurança vêm sendo adequadas para manter a estabilidade do bloco e para formular os esforços de combate ao terrorismo, respeitando os padrões democráticos e valores sociais, afastando a questão da securitização e aproximando-a do estado de direito.

Em 2002, os países do Mercosul firmam o Plano Geral de Reciprocidade em Cooperação e Coordenação para a Segurança Regional entre Estados-membros, no qual o Capítulo 7 estabelece políticas de combate ao terrorismo, como a criação de um Grupo de Trabalho Especializado em Terrorismo no âmbito dos Grupos de Trabalho Permanentes (que realizam reuniões semestrais), criando, então, um Sistema Integrado para o Intercâmbio de Informações, troca de experiências, treinamento e recursos humanos para lidar com o terrorismo e preparar forças-tarefa nacionais e identificar os atores cujos interesses estão voltados para o terrorismo internacional e estabelecer um Formulário Padrão de Intercâmbio de Informações como auxílio às investigações relacionadas ao terrorismo. Um dos pontos interessantes deste último — e um dos mais polêmicos — é que, no próprio capítulo, é enfatizado que os estados podem solicitar informações sobre a condição de refugiado da pessoa sob investigação, supondo-se, portanto, que o autor do crime seja um estrangeiro.

Pode-se argumentar que o combate ao terrorismo não é o propósito do Mercosul. No entanto, com a forte presença do crime organizado transnacional e do financiamento do terrorismo na região, é urgente criar uma estrutura que funcione e que seja eficaz para seus Estados-membros e associados de maneira a trazer estabilidade para a região. Um dos maiores desafios enfrentados pela segurança regional atualmente é a estrutura intergovernamental sobre a qual o Mercosul foi criado. Como todos os Estados-membros devem concordar com a decisão e integrá-la a seus ordenamentos jurídicos, tem ocorrido constante atraso na implementação de práticas de segurança na região.

Recomendações de políticas

Para o combate ao terrorismo e ao crime organizado nos Estados-membros do Mercosul, propõe-se o estabelecimento de uma instituição forte e operacional que possa atuar na estrutura intergovernamental do Mercosul: o Coordenador de Segurança da América do Sul (CSAS). A CSAS seria uma instituição transnacional que incluiria acadêmicos e gestores de políticas públicas para melhor compreender as ameaças à segurança enfrentadas pela América do Sul e desenvolver estratégias sobre como combatê-las de maneira

an institution that can provide expert consultants in many security issues, such as maritime insecurity, refugee crisis, human rights violations, cross-border criminal activities, radicalisation through social media, etc. Because the focus of this policy paper is countering terrorism specifically, the following paragraphs will deal with the proposed agencies within the umbrella of the SASC, providing an initial set of goals and a structure that can be further applied to other security issues.

Thus, the creation of the Counterterrorism Regional Division (CTRD) within the structure of the SASC is proposed to optimise concessions, efforts and human resources invested in countering terrorism in the region. The CTRD would have three main priorities in counterterrorism efforts: to ensure the safety and human rights of Mercosur citizens, to prevent radicalisation and ensure the upholding of democratic values, and the promotion of transnational cooperation within the region and internationally. The CTRD would have an appointed Secretariat that would be responsible for coordinating activities, investigations, reports and datasets produced by the agencies within the Division, and to foster the counterterrorism debate within Mercosur. The CTRD Secretariat would be composed of a General Secretary, Mercosur State Representatives and International Envoys.

The General Secretary would be the head of the Division, the one who oversees the agencies' activities and CTRD's representative in forums, meetings and conferences, as well as briefing member states on the issue, reporting on the implementation of measures and proposing a future agenda. The Mercosur State Representatives would be government employees from the Ministry of Defence of the member states, being the point of contact of the members to the Division and would present the demands of their respective member states. The International Envoys, on the other hand, would be responsible for the Division's compliance with international standards, and would facilitate cooperation between the CTRD and other regional and international counterterrorism organisations to counter terrorism networks worldwide. Ideally, the Secretary, the Representatives and the Envoys would have transnational specialised team members representing Mercosur and its member states.

Alongside the CTRD Secretariat, the Division would have three co-dependent agencies: the South American Counterterrorism Coordinator (SACC), the South American Intelligence Agency (SAIA), and the Legislative Policy-Making Monitor (LPMM). The Regional Counterterrorism Coordinator (RCTC) would mirror the European Counterterrorism Coordinator's functions, that is, it would be this agency's responsibility to coordinate the work of the member states in countering terrorism; to present the policy recommendations developed by the SAIA and to propose priority for action to the member states; to monitor the implementation of Mercosur's counter-terrorism strategy; to monitor the implementation of domestic policies; and to maintain and improve communication within the SASC.

One of the critical issues in any regional integration process, while maintaining regional stability, is to cooperate with neighbouring countries. Encouraging information provision and sharing by intelligence and police agencies is vital for the coordination of multilateral operations that can make a substantial difference in combating the

coordenada e através da cooperação. Além disso, a CSAS seria uma instituição consultiva, semelhante a um *think tank* ou laboratório de ideias, constituindo uma ferramenta para uma maior integração e para garantir a segurança das pessoas e dos Estados.

Deve-se enfatizar a importância de uma instituição que venha a abordar não apenas a ameaça e o vínculo do terrorismo com o crime organizado na região, mas uma instituição que possa fornecer consultores especializados em diversas questões de segurança, tais como segurança marítima, crise de refugiados, violações de direitos humanos, atividades criminosas transfronteiriças, radicalização através das redes sociais etc. Como o foco deste *policy paper* é o combate ao terrorismo especificamente, os parágrafos a seguir se concentrarão nas agências propostas dentro da estrutura da CSAS, fornecendo um conjunto inicial de metas e estrutura que poderão ser posteriormente replicadas para outras questões de segurança.

Assim, propõe-se a criação da Divisão Regional de Contraterrorismo (DRCT) dentro da estrutura da CSAS para otimizar concessões, esforços e recursos humanos investidos no combate ao terrorismo na região. O DRCT teria três prioridades principais na luta contra o terrorismo: garantir a segurança e os direitos humanos dos cidadãos do Mercosul, prevenir a radicalização e garantir a defesa dos valores democráticos e promover a cooperação transnacional na região e internacionalmente. O DRCT contaria com a nomeação de uma Secretaria responsável pela coordenação de atividades, investigação, relatórios e conjuntos de dados produzidos pelas agências dentro da Divisão e por liderar o debate sobre o combate ao terrorismo dentro do Mercosul. A Secretaria do DRCT seria composta por um Secretário-Geral, Representantes dos Estados do Mercosul e Enviados Internacionais.

O Secretário-Geral seria o líder da Divisão, encarregado da supervisão das atividades dos organismos, de ser o representante do DRCT em foros, reuniões e conferências, bem como de informar os Estados-membros sobre a matéria, acompanhar a implementação das medidas e propor uma agenda futura. Os Representantes dos Estados do Mercosul seriam funcionários públicos do Ministério da Defesa dos Estados-membros, sendo o ponto de contato dos membros junto à Divisão e representariam as demandas de seus respectivos Estados-membros. Os Enviados Internacionais, por sua vez, seriam responsáveis pelo cumprimento das normas internacionais pela Divisão e facilitariam a cooperação entre o DRCT e outras organizações regionais e internacionais de combate ao terrorismo e com redes de contraterrorismo em todo o mundo. Recomenda-se que o Secretário, os Representantes e os Enviados tenham, em sua equipe, membros transnacionais especializados representando o Mercosul e seus Estados-membros.

Além da Secretaria do DRCT, a Divisão teria três agências interdependentes: a Coordenação de Contraterrorismo da América do Sul (CCAS), a Agência de Inteligência da América do Sul (AIAS) e o Monitoramento de Formulação de Políticas Legislativas (MFPL). A Coordenação Regional de Contraterrorismo (CRCT) espelharia as funções da Coordenação de Contraterrorismo Europeu, ou seja, seria responsabilidade desta agência coordenar o trabalho dos Estados-membros no combate ao terrorismo; apresentar as recomendações de política desenvolvidas pela AIAS e propor as prioridades de ação aos Estados-membros; monitorar a implementação da estratégia antiterrorismo do Mercosul; monitorar a implementação das políticas nacionais; e manter e melhorar a comunicação dentro do CSAS.

myriad of security threats present in the region. The South American Intelligence Agency (SAIA) would also provide operational support to member states, sharing intelligence on terrorism financing and radicalisation through social media, and promote cooperation among counterterrorism authorities. The effort of establishing transnational ways of communication, from local law enforcement agencies to the United Nations, is important to collect the necessary data and, thus, to produce the most accurate public policies that truly reflect the contextual demands of the member states. The SAIA would also incorporate the Integrated System for the Exchange of Information established in the 2002 General Plan.

The Agency would also count on Specialist Teams to collate and process information to and from member states and third parties to establish a wider perspective on counterterrorism for both strategic goals and operational purposes. These Specialist Teams would incorporate the existing Working Groups that are specialised in counterterrorism, and increase the number of members and consultants to aggregate more to the research in order to strengthen overall counterterrorism capabilities. In retrospect, these Specialist Teams would be aligned with the UN Working Groups of the Counter-Terrorism Coordination Compact to further enhance cooperation, data and resources to better implement realistic policies in South America.

Due to the transnational nature of terrorism and terrorism financing, it is important to establish an agency that can facilitate judicial cooperation between member states to prevent radicalisation and terrorist attacks, to tackle root causes related to the judicial system, and to bring perpetrators, instigators and financiers to justice. Thus, the Legislative and Policy Making Monitor (LPMM) would collect data and monitor the legislative and policy-making proceedings in the member states and ensure that individuals accused of terrorism are tried within the rule of law, based on the Eurojust Counter-Terrorism Register. The LPMM would also assist national authorities in cross-border cases and provide enforcement and judicial professionals to aid local law enforcement to build solid prosecution cases. The maintenance of democratic means is extremely important in countering terrorism because it assures that the states are not using unnecessary force and are not targeting specific minorities, refugees or the political opposition. Furthermore, the LPMM would work closely with member states institutions and regional institutions such as the OAS to advance efforts to counter terrorism.

Countering terrorism in Mercosur is an ever-growing challenge that demands regional transnational cooperation to mitigate the problem in the region. Even though terrorism is not the focus of regional cooperation, the alarming increase in the nexus between terrorism and organised crime is a 'ticking time-bomb' to policy-makers, law enforcement and governments alike. The establishment of a robust and centralised counterterrorism structure within Mercosur to aid in comprehending the threat and presenting strategies to counter terrorism does not only make the region safer, strengthening regional integration efforts, but also facilitates the exchange of information and the coordination of joint operations with other regional organisations such as the EU, AESAN and NATO. Regional stability and safety are key to ensure a brighter future for the development of South America.

Uma das questões críticas em qualquer processo de integração regional para manter a estabilidade na região é a cooperação entre países vizinhos. O incentivo ao fornecimento e compartilhamento de informações por agências de inteligência e de órgãos policiais é fundamental para a coordenação de operações multilaterais que podem trazer imensos benefícios no combate à pluralidade de ameaças à segurança presentes na região. A Agência de Inteligência da América do Sul (AIAS) também forneceria apoio operacional aos Estados-membros, compartilhando inteligência sobre o financiamento do terrorismo e a radicalização por meio das redes sociais e promoveria a cooperação entre as autoridades de combate ao terrorismo. O esforço de estabelecer meios de comunicação transnacionais, desde os órgãos locais de combate ao crime até as Nações Unidas, é fundamental para coletar os dados necessários e, assim, produzir políticas públicas mais precisas que realmente reflitam as demandas nos contextos dos Estados-membros. O AIAS também incorporaria o Sistema Integrado para o Intercâmbio de Informações estabelecido no Plano Geral de 2002.

A Agência também contaria com Equipes de Especialistas para coletar e processar informações de e para os Estados-membros e terceiros, a fim de estabelecer uma perspectiva mais ampla sobre o enfrentamento ao terrorismo, tanto para objetivos estratégicos quanto para fins operacionais. As Equipes de Especialistas incorporariam os Grupos de Trabalho existentes especializados no combate ao terrorismo e ampliariam os membros e consultores para agregar mais pesquisas e fortalecer as capacidades gerais na matéria. Em retrospectiva, as Equipes de Especialistas estariam alinhadas com os Grupos de Trabalho das Nações Unidas para o Pacto de Coordenação de Combate ao Terrorismo para aumentar ainda mais a cooperação, coleta de dados e os recursos para melhor implementar políticas realistas na América do Sul.

Devido à natureza transnacional do terrorismo e do financiamento do terrorismo, é fundamental estabelecer uma agência que possa facilitar a cooperação judiciária entre os Estados-membros para prevenir a radicalização e atentados terroristas, para combater as causas mais profundas relacionadas ao sistema judicial e para levar os autores, instigadores e financiadores do crime de terrorismo à justiça. Assim, o Monitoramento de Formulação de Políticas e de Legislação (MFPL) coletaria os dados e monitoraria os processos legislativos e de elaboração de políticas nos Estados-membros, garantindo que os indivíduos acusados de terrorismo sejam julgados em observância do Estado de Direito, com base no Registro Antiterrorismo da Eurojust. O MFPL também ajudaria as autoridades nacionais em casos transfronteiriços e forneceria profissionais de combate ao crime e da esfera judicial para ajudar as autoridades policiais locais a elaborar robustos processos de acusação. Portanto, a manutenção de meios democráticos é vital no combate ao terrorismo, uma vez que garante que os Estados não façam uso de força desnecessária e não tenham como alvo minorias específicas, refugiados e a oposição política. Além disso, o MFPL trabalharia em estreita colaboração com as instituições dos Estados-membros e instituições regionais, como a OEA, para promover os esforços de combate ao terrorismo.

O enfretamento ao terrorismo no Mercosul é um desafio cada vez maior que exige cooperação regional transnacional para combater o problema na região. Embora o terrorismo não seja o foco da cooperação regional, o aumento alarmante do vínculo entre o terrorismo e o crime organizado é uma "bomba-relógio" para gestores de políticas públicas,

Recommended Sources

ARGOMANIZ, J. **Post-9/11 institutionalisation of European Union counter-terrorism: emergence, acceleration and inertia**. In: EUROPEAN SECURITY. 2009. vol. 18(2), p. 151-172.

BURES, O. **Intelligence sharing and the fight against terrorism in the EU: lessons learned from Europol.** In: EUROPEAN VIEW. 2016. vol. 15(1), p. 57-84.

BURKOV, Y. **Counter-Terrorism Intelligence in the EU: The Case of the European Counter-Terrorism Center.** 2016. Central European University, Budapest.

DINIZ, B.C. **FROM LANGUAGE TO PRACTICE: Contemporary Counterterrorism in the European Union and the United Kingdom.** Master's dissertation. 2021. Available at: <http://www.biblioteca.pucminas.br/teses/RelacoesInternacionais_BarbaraCamposDiniz_19014.pdf>.

EUROPEAN COMMISSION. **Position Paper on Ongoing Police and Judicial Cooperation in Criminal Matters.** Task Force for the Preparation and Conduct of the Negotiations with the United Kingdom under Article 50 TEU. 2017. Available at: < https://ec.europa.eu/info/publications/position-paper-ongoing-police-and-judicial-cooperation-criminal-matters_en>.

EUROPEAN COMMISSION. **Framework for the future relationship – Police & Judicial Cooperation in Criminal Matters.** Task Force for the Preparation and Conduct of the Negotiations with the United Kingdom under Article 50 TEU. 2018. Available at: <https://ec.europa.eu/commission/sites/beta-political/files/slides_on_police_and_judicial_cooperation_in_criminal_matters.pdf>.

EUROPEAN COMMISSION. **SIRENE Cooperation.** 2018. Available at: <https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengeninformation-system/sirene-cooperation_en>.

EUROPEAN COUNCIL. **Declaration on Combating Terrorism.** Brussels. 2004. Available at:<http://www.consilium.europa.eu/uedocs/cmsUpload/DECL-25.3.pdf>.

TE-SAT.EU **Terrorism Situation and Trend Report.** 2018. EUROPOL. Available at: <https://www.europol.europa.eu/tesat-report#fndtn-tabs-0-bottom-2>.

WILKINSON, Paul. **Terrorism Versus Democracy: The Liberal State Response.** New York: Routledge, 2006.

ZIMMERMANN, D. **The European Union and Post-9/11 Counterterrorism: A Reappraisal.** In: STUDIES IN CONFLICT AND TERRORISM. 2006. vol. 29(2), p. 123-145.

autoridades policiais e governos. O estabelecimento de uma estrutura de contraterrorismo robusta e centralizada dentro do Mercosul para auxiliar na compreensão da ameaça e na apresentação de estratégias de combate ao terrorismo não só torna a região mais segura, aprofundando os esforços de integração regional, mas também facilita a troca de informações e a coordenação de operações conjuntas com outras organizações regionais, como a União Europeia, AESAN e OTAN. Estabilidade e segurança regionais são fundamentais para garantir um futuro melhor para o desenvolvimento da América do Sul.

Fontes Recomendadas

ARGOMANIZ, J. **Post-9/11 institutionalisation of European Union counter-terrorism: emergence, acceleration and inertia**. IN: EUROPEAN SECURITY. 2009. vol. 18(2), p. 151-172.

BURES, O. **Intelligence sharing and the fight against terrorism in the EU: lessons learned from Europol**. IN: EUROPEAN VIEW. 2016. vol. 15(1), p. 57-84.

BURKOV, Y. **Counter-Terrorism Intelligence in the EU: The Case of the European Counter-Terrorism Center.** 2016. Central European University, Budapeste.

DINIZ, B.C. **FROM LANGUAGE TO PRACTICE: Contemporary Counterterrorism in the European Union and the United Kingdom**. Dissertação de mestrado. 2021. Disponível em: <http://www.biblioteca.pucminas.br/teses/RelacoesInternacionais_BarbaraCamposDiniz_19014.pdf>.

COMISSÃO EUROPEIA. **Position Paper on Ongoing Police and Judicial Cooperation in Criminal Matters**. Força-tarefa para a Preparação e Condução das Negociações com o Reino Unido nos termos do artigo 50 do TEU. 2017. Disponível em: < https://ec.europa.eu/info/publications/position-paper-ongoing-police-and-judicial-cooperation-criminal-matters_en>.

COMISSÃO EUROPEIA. **Framework for the future relationship – Police & Judicial Cooperation in Criminal Matters.** Força-tarefa para a Preparação e Condução das Negociações com o Reino Unido nos termos do artigo 50 do TEU. 2018. Disponível em: <https://ec.europa.eu/commission/sites/beta-political/files/slides_on_police_and_judicial_cooperation_in_criminal_matters.pdf>.

COMISSÃO EUROPEIA. **Cooperação SIRENE**. 2018. Disponível em: <https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengeninformation-system/sirene-cooperation_en>.

CONSELHO EUROPEU. **Declaration on Combating Terrorism**. Bruxelas. 2004. Disponível em:<http://www.consilium.europa.eu/uedocs/cmsUpload/DECL-25.3.pdf>.

TE-SAT.EU **Terrorism Situation and Trend Report.** 2018. EUROPOL. Disponível em: <https://www.europol.europa.eu/tesat-report#fndtn-tabs-0-bottom-2>.

WILKINSON, Paul. **Terrorism Versus Democracy: The Liberal State Response**. Nova York: Routledge, 2006.

ZIMMERMANN, D. **The European Union and Post-9/11 Counterterrorism: A Reappraisal.** IN: STUDIES IN CONFLICT AND TERRORISM. 2006. vol. 29(2), p. 123-145.

Marília Closs

Marília Closs é doutoranda e mestra em Ciência Política pelo Instituto de Estudos Sociais e Políticos da Universidade do Estado do Rio de Janeiro (IESP-UERJ) e bacharela em Relações Internacionais pela Universidade Federal do Rio Grande do Sul (UFRGS).

Marília Closs is a doctoral student and Master in Political Science from the Institute of Social and Political Studies of the State University of Rio de Janeiro (IESP-UERJ). She holds a bachelor's degree in International Relations from the Federal University of Rio Grande do Sul (UFRGS).

De volta ao passado? (Re)Militarização da América do Sul (2015-2021) e as políticas indicadas para um regionalismo em crise

Back to the past? (Re)militarization of South America (2015-2021) and the policies recommended for a regionalism in crisis

Marília Closs

SUMÁRIO EXECUTIVO

Este *policy paper* trata sobre o processo de (re)militarização pelo qual a América do Sul vem passando desde 2015. Mesmo com a ausência de guerras ou conflitos tradicionais, o subcontinente parece ser, cada vez mais, um barril de pólvora em função do acirramento de tensões e rivalidades. Alguns elementos principais mostram isso, como a crise na Venezuela, o desmonte da arquitetura regional de cooperação, os problemas na implementação dos acordos de paz na Colômbia, o fortalecimento de um campo político de extrema-direita que mobiliza a violência de maneira pouco democrática em seus discursos e práticas, o acirramento de conflitos fronteiriços e, por fim, uma crise que parece ser conceitual a respeito do que significam regionalismos, segurança e defesa.

Não parece haver, no entanto, a formulação e a execução de políticas adequadas para o contexto. Pelo contrário: o que se vê é uma priorização cada vez menor deste tipo de agenda, junto com uma pluralidade de organismos regionais que pouco dialogam entre si. Frente a isto,

EXECUTIVE SUMMARY

This *policy paper* deals with the (re) militarization process that South America has been going through since 2015. Even in the absence of traditional wars or conflicts, the subcontinent seems to be increasingly becoming a powder keg, fuelled by the intensification of tensions and rivalries. Some key elements make it explicit, such as the crisis in Venezuela; the dismantling of the regional cooperation architecture; the problems in the implementation of the peace agreements in Colombia; the strengthening of an extreme right-wing political camp that mobilizes violence in an undemocratic way in its discourses and practices; the intensification of border conflicts; and, finally, a seemingly conceptual crisis concerning the meaning of regionalism, security and defence.

Nevertheless, there does not seem to be any adequate policy formulation or enforcement for this scenario. On the contrary: what we see is a decreasing prioritization of this type of agenda, along with a plurality of regional organizations that do not talk much to each other. Given this situation, this paper proposes

the institutional reorganization of South American as an urgent task, with separate conceptions and policies for security and defence, and giving emphasis to the development of border policies, but from the perspective of expanding the participation of civil society in building these agendas. After all, there is a need to rethink and reorganize regionalism, which can only be done with greater social participation.

BACKGROUND AND IMPORTANCE OF THE PROBLEM: a snapshot of the (re)militarization of South America

Since 2015, it has been possible to observe a process of (re)militarization in South America. The subcontinent has historically had a low number of interstate wars and traditional conflicts, which is intensified throughout the 21st century. However, **the absence of war does not mean peace**. The election of Mauricio Macri to the presidency of Argentina in 2015 marks the end of what is commonly called the "left turn" or "pink wave", a political cycle in which left or centre-left governments were in power in South America and which was accompanied by the construction of a "post-liberal regionalism" (SANAHUJA, 2012). In addition to Macri, other presidents of right-wing political parties and political camps in South America were successively elected, such as Ivan Duque (Colombia, 2018), Jair Bolsonaro (Brazil, 2018), Luis Alberto Lacalle Pou (Uruguay, 2020), and Sebastián Piñera (Chile, 2018), who was re-elected for a second term. In this new political cycle, there is a disruption of previously established security and defence scenarios, the consequences of which are the militarization of the subcontinent. This is mainly based on seven elements:

(1)The escalation of the crisis in Venezuela:

In Venezuela, the political, economic and social crisis began in 2013, with the death of Hugo Chávez and the election of Nicolás Maduro, and became more pronounced in 2014 with opposition demonstrations led, above all, by Leopoldo López, who was arrested the following year by the regime. However, 2015 marks the escalation of the crisis after the victory of the opposition to Maduro in the Legislative Assembly, leading the country's Executive and Supreme Court of Justice to oppose the Legislative (CLOSS, 2020). Since then, demonstrations have continued to take the streets — for and against Madur's administration, the latter being mostly met with repression —, just as accusations of fraud and coup attempts are frequent in the country. After the 2017 Constituent Assembly and the 2018 presidential elections, which were boycotted by a large part of the opposition, and which re-elected Maduro — Juan Guaidó proclaimed himself president of the country and, since then, has been recognized as such by the governments of several countries. To this day, Venezuela continues to experience political, economic, humanitarian, and security crises simultaneously. There is more to it, however: the crisis today has already taken regional and hemispheric dimensions.

este artigo propõe a reorganização institucional sul-americana como tarefa urgente, com concepções e políticas separadas para segurança e defesa e ênfase no desenvolvimento de políticas para fronteiras, mas a partir de uma perspectiva de ampliação da participação da sociedade civil na construção destas agendas. Afinal, é necessário repensar e reorganizar o regionalismo — e isto só pode ser feito com mais participação social.

CONTEXTO E IMPORTÂNCIA DO PROBLEMA: uma fotografia da (re)militarização da América do Sul

Desde 2015, pode-se observar um processo de (re)militarização da América do Sul. O subcontinente historicamente conta com um baixo número de guerras interestatais e de conflitos tradicionais o que, ao longo do século XXI, é intensificado. No entanto, **a ausência de guerra não significa paz**. A eleição de Mauricio Macri à presidência da Argentina em 2015 é o marco do fim do que é comumente chamado de "giro à esquerda" ou "onda rosa", ciclo político em que governos de esquerda ou centro-esquerda estiveram no poder na América do Sul e que veio acompanhado da construção de um "regionalismo pós-liberal" (SANAHUJA, 2012). Além de Macri, sucessivamente, foram eleitos outros presidentes de partidos e campos políticos à direita na América do Sul, como Ivan Duque (Colômbia, 2018), Jair Bolsonaro (Brasil, 2018), Luis Alberto Lacalle Pou (Uruguai, 2020) e Sebastian Piñera (Chile, 2018), que foi reeleito para seu segundo mandato. Neste novo ciclo político, há rupturas nos cenários de segurança e defesa construídos anteriormente; as consequências disto são a militarização do subcontinente. Isto se dá, principalmente, a partir de sete elementos:

(1) A intensificação da crise na Venezuela:

Na Venezuela, a crise política, econômica e social tem origem em 2013, com a morte de Hugo Chávez e com a eleição de Nicolás Maduro, o que se acentua em 2014, com as manifestações da oposição, lideradas, sobretudo, por Leopoldo López, preso no ano seguinte pelo regime. No entanto, 2015 é o marco da intensificação da crise após a vitória da oposição a Maduro na Assembleia Legislativa e, com isso, o executivo e o Tribunal Supremo de Justiça daquele país passam a estar em oposição ao legislativo (CLOSS, 2020). Desde então, manifestações seguem ocorrendo nas ruas — a favor e contra o governo de Maduro, sendo estas últimas, em sua maioria, recebidas com repressão —, assim como acusações de fraudes e tentativas de golpe são frequentes no país. Após a Assembleia Constituinte de 2017 e as eleições presidenciais de 2018, que foram boicotadas por grande parte da oposição e que reelegeram Maduro, Juan Guaidó se autoproclamou presidente do país e, desde então, já foi reconhecido pelos governos de diversos países. Até hoje, a Venezuela segue vivendo simultaneamente crises política, econômica, humanitária e securitária. No entanto, é mais que isto: hoje, a crise já tem dimensões regionais e hemisféricas.

(2) The weakening of UNASUR and the dismantling of the multilateral and cooperation regional architecture:

Created in 2008, the Union of South American Nations (UNASUR) was the main multilateral political coordination forum in South America, although it co-existed with other regional organizations such as Mercosur, the Andean Community, and the Organization of American States (OAS). With regard to security and defence, UNASUR and its South American Defence Council were spaces for the discussion of themes related to joint defence policies and the peaceful settlement of disputes, with emphasis on the role of the organization in the containment of the crises between Colombia, Venezuela and Ecuador (2008, when it was still being formally created), in Bolivia (2009), in Ecuador (2010), and in Paraguay (2012). In many ways, it was thanks to the construction of collective dialogue by UNASUR that security crises were prevented from evolving towards inter- or intra-state armed conflicts (CLOSS, 2020).

It is also important to note that UNASUR managed to separate the themes of security and defence, and some social agendas were no longer treated as security issues. This was an important move at a time of (global, but above all hemispheric) expansion of the concept of security so that themes would fit within it that were previously not held within the limits of security and that had different natures, origins and scopes, such as environmental, energetic and humanitarian issues (SAINT-PIERRE, 2012). In this sense, the main highlight was the regional policy to fight the transnational problem of drug trafficking, which went beyond the scope of security and defence and became the object of the South American Council on the World Drug Problem, in a process of desecuritization of the agenda (MARTINEZ; LYRA, 2015).

Since 2015, however, the scenario has started to change. With the new political cycle in the region, governments gave increasingly lower priority to UNASUR and the institution started weakening. In 2018, Argentina, Chile, Colombia, Paraguay, and Peru announced that they would no longer participate in the organization's activities indefinitely and, a few months later, Brazil announced its withdrawal. As a result, the institutional architecture that would ensure some degree of stability and dialogue in the areas of security and defence in South America was dismantled. The main consequence of this is the failure of regional organizations to build a mediation for the crisis in Venezuela (VELASCO, 2019). The OAS and the Lima Group were unable to play the role that UNASUR had previously managed to play in establishing dialogue between the parties.

(3) Instabilities in the implementation of the peace agreements in Colombia:

In 2016, the Havana Agreements were finalized which, after 4 years of negotiation, sealed peace between the Colombian government and the Fuerzas Armadas Revolucionarias de Colombia - Ejército del Pueblo (FARC-EP), an over five-decade long armed conflict. In 2018, however, Iván Duque (Centro Democrático) was elected president of the country in a campaign that placed challenging agreements at the centre of the debate. Since then, not only has the polarization regarding peace — already noticeable since

(2) O esvaziamento da UNASUL e o desmonte da arquitetura regional multilateral e de cooperação:

Criada em 2008, a União das Nações Sul-Americanas (UNASUL) era o principal espaço de coordenação política multilateral na América do Sul, ainda que coexistindo com outras organizações regionais, como o Mercosul, a Comunidade Andina e a Organização dos Estados Americanos (OEA). No que diz respeito à segurança e à defesa, a UNASUL e seu Conselho de Defesa Sul-Americano foram espaços de diálogo ao redor de temáticas para políticas conjuntas de defesa e solução pacífica de controvérsias, com destaque para a atuação na contenção das crises entre Colômbia, Venezuela e Equador (2008, quando ainda estava sendo formalmente criada), na Bolívia (2009), no Equador (2010) e no Paraguai (2012). Em diversos aspectos, foi graças à construção do diálogo coletivo a partir da UNASUL que se evitou que as crises securitárias avançassem em direção ao conflito armado inter ou intraestatal (CLOSS, 2020).

Importante notar, também, que a UNASUL logrou separar as temáticas de segurança e defesa, e algumas agendas sociais deixaram de ser tratadas como questões securitárias. Este foi um movimento importante em um momento de expansão (global, mas sobretudo hemisférica) do conceito de segurança para que, dentro dele, coubessem temas que, anteriormente, não estavam no âmbito securitário e que possuem naturezas, origens e escopos diferentes, como temáticas ambientais, energéticas e humanitárias (SAINT-PIERRE, 2012). Neste sentido, o maior destaque foi a política regional para o problema transnacional do tráfico de drogas, que saiu do escopo da segurança e da defesa e passou a ser objeto do Conselho Sul-Americano sobre o Problema Mundial das Drogas, em um processo de dessecuritização da agenda (MARTINEZ; LYRA, 2015).

Desde 2015, no entanto, o cenário começou a se alterar. Com o novo ciclo político na região, os governos passaram a priorizar cada vez menos a UNASUL, e a instituição passa a ser esvaziada. Em 2018, Argentina, Chile, Colômbia, Paraguai e Peru anunciaram que deixariam de participar das atividades da organização por tempo indeterminado e, alguns meses depois, o Brasil comunicou sua retirada. Com isso, foi desfeita a arquitetura institucional que garantia algum grau de estabilidade e diálogo nas temáticas de segurança e defesa na América do Sul. A principal materialização disto é a falência das organizações regionais em construírem a mediação da crise na Venezuela (VELASCO, 2019). A OEA e o Grupo de Lima não lograram desempenhar o papel que, em outro momento, a UNASUL conseguiu exercer no diálogo entre as partes.

(3) Instabilidades na implementação dos acordos de paz na Colômbia:

Em 2016, foram finalizados os Acordos de Havana que, depois de 4 anos de negociação, selaram a paz entre o governo da Colômbia e as Fuerzas Armadas Revolucionarias de Colombia - Ejército del Pueblo (FARC-EP), após um conflito armado que já dura mais de cinco décadas. Em 2018, no entanto, Iván Duque (Centro Democrático) foi eleito presidente do país em uma campanha que colocava o questionamento aos acordos no centro do debate; desde então, não apenas a polarização a respeito da paz — já perceptível desde o plebiscito de 2016 — aumentou, como algumas partes da própria negociação

the 2016 referendum — increased, but some items of the negotiation itself are being breached. The result is that the armed conflict still persists in Colombia, not only with guerrillas that are still active, such as the Ejército de Liberación Nacional (ELN), but also with FARC-EP dissident groups, in addition to the presence of paramilitary groups involved in the dispute.

(4) The strengthening of the far right as a political camp:

The election of Jair Bolsonaro in Brazil made the strengthening of an extreme right-wing camp in South America very clear. Beyond the moral agenda, linked to conservatism in themes such as gender and sexuality (BIROLI, 2020), there is a centrality of public security in the agendas, with its militarization as its main target. As a result, a new pattern of use of force has emerged in the subcontinent, in which violence in politics has been more present than democratic rules should allow. This camp uses discursive elements involving moral panic to create threats, such as the risks of "Venezuelization" or "communist threats that want to destroy families" as a device (GAMBOA, 2019). The construction of agendas for the securitization and militarization of public life seems to be able not only to build internal programmatic contents, but to bring together domestic and external agendas, and it does so while constantly challenging multilateralism — or "globalism". The use of violence and force has been the main programmatic content around which new and old projects are articulated by the right.

(5) The increased participation of the military in politics:

Along with the strengthening of an extreme right-wing political camp, there is a substantial increase in the number of military personnel in public office. In Bolsonaro's Brazil, 6,755 military candidates were elected for public office in 2018, and "from 2018 to 2020 the presence of military personnel in the federal administration increased by about 55%" (NOZAKI, 2021, p. 11). The Armed Forces no longer occupy only their traditional spaces in the administration, such as the Ministry of Defence and the Institutional Security Office, but they are now in ministries such as Infrastructure, Mines and Energy, Science, Technology and Communication, and Health, for example. In Maduro's Venezuela, the number of generals increased, as did their influence in the government (VELASCO, 2019). This is taking place in the context of the already persistent "identity crisis of the South American military" after the redemocratization processes of the 1990s (FUCCILLE, 2003). With the expansion of the use of the Armed Forces in public security agendas in countries like Brazil and Colombia, the military identity crisis is deepening. Finally, it is also worth noting that the responses to the covid-19 pandemic in several countries in Latin America were based primarily on military procedures (PASSOS; ACÁCIO, 2021).

(6) Increased border tensions:

Since 2015, an increase in border conflicts has been apparent. In addition to the building of walls, such as the one between Argentina and Paraguay (Posadas-Encarnación),

estão sendo desrespeitadas. O resultado é que o conflito armado segue vigente na Colômbia, não apenas com guerrilhas que ainda estão ativas, como o Ejército de Liberación Nacional (ELN), mas também com grupos dissidentes das FARC-EP, além da presença de grupos paramilitares envolvidos na disputa.

(4) O fortalecimento da extrema-direita como campo político:

A eleição de Jair Bolsonaro no Brasil deixou claro que há um fortalecimento do campo de extrema-direita na América do Sul. Para além da agenda moral, ligada ao conservadorismo em temas como gênero e sexualidade (BIROLI, 2020), há a centralidade da segurança pública nas agendas, com a militarização desta como principal bandeira. Há, com isto, um novo padrão de uso da força no subcontinente em que a violência, na política, tem sido mais presente do que as regras democráticas deveriam permitir. Como instrumento, este campo se vale de elementos discursivos ao redor do pânico moral para a construção de ameaças, como os riscos de "venezuelização" ou de "ameaças comunistas que querem destruir as famílias" (GAMBOA, 2019). A construção de agendas de securitização e militarização da vida pública parece estar sendo capaz de construir não apenas conteúdos programáticos internos, mas de juntar agendas domésticas e externas, e o faz em constante questionamento ao multilateralismo — ou "globalismo". O uso da violência e da força tem sido o principal conteúdo programático ao redor do qual novos e antigos projetos à direita estão se articulando.

(5) O aumento da participação dos militares na política:

Junto com o fortalecimento de um campo político de extrema-direita, vê-se que há um aumento substancial do número de militares em cargos públicos. No Brasil de Bolsonaro, nas eleições de 2018, 6.755 candidatos militares foram eleitos para cargos no país e "de 2018 a 2020 aumenta em cerca de 55% a presença de militares na administração federal" (NOZAKI, 2021, p. 11). No gabinete, as Forças Armadas deixaram de ocupar apenas os espaços onde tradicionalmente estão, como o Ministério da Defesa e o Gabinete de Segurança Institucional, mas passaram a estar em ministérios como o de Infraestrutura, de Minas e Energia, de Ciência, Tecnologia e Comunicação e de Saúde, por exemplo. Na Venezuela de Maduro, o número de oficiais-generais aumentou, assim como aumentou sua influência no governo (VELASCO, 2019). Isto se dá no cenário da já persistente "crise de identidade dos militares sul-americanos" após os processos de redemocratização na década de 1990 (FUCCILLE, 2003). Frente à ampliação da utilização das Forças Armadas em agendas de segurança pública em países como Brasil e Colômbia, a crise da identidade militar se amplia. Por fim, cabe notar, também, que as respostas à pandemia de covid-19 em diversos países na América Latina se deram, primordialmente, a partir de instrumentos militares (PASSOS; ACÁCIO, 2021)

(6) Ampliação de tensões fronteiriças:

Desde 2015, pode-se observar, também, o aumento de conflitos fronteiriços. Além da construção de muros, como aquele entre Argentina e Paraguai (Posadas-Encarnación),

which began to be built in 2015 and was stopped in 2017, it is worth mentioning the wall being built by Ecuador on its border with Peru (LONDOÑO, 2017). In 2017, in addition to the historic rivalry between Chile and Bolivia in the dispute over sea access, a tension on the border lasted for several months after the arrest of Bolivian customs officials in Chilean territory and the incursion of Chilean police officers into Bolivian territory. Since 2017, it has also been possible to see the construction of new Bolivian military bases on the border with Chile with the declared purpose of combating smuggling.

The tensest border region in South America is that between Colombia and Venezuela. In 2015, the situation in the city of Cúcuta turned into one of humanitarian collapse after the deportation of Colombian migrants by the Venezuelan government. Since the deepening of the crisis in Venezuela, one can also observe an increase in incursions by Venezuelan public security forces into Colombian territory, and vice versa. In 2017, the Colombian government denounced attacks and murders by the Guardia Nacional Venezolana in the department of La Guajira. In May 2021, Jesús Santrich, a FARC guerrilla dissident, was murdered by Colombian public security forces, and the Venezuelan government claims that this took place within its borders. Therefore, one can see that historical rivalries and border conflicts have been surfacing with greater emphasis since 2015, presenting new security risks for the subcontinent.

(7) There is, therefore, an intersection of several crises:

The militarization of America stems from the intensification of crises, such as those in Venezuela and Colombia, the renewal of border crises and historic rivalries, and the strengthening of a political camp that places military personnel in institutional positions and violence at the centre of their public agenda. All of this takes place against the backdrop of a dismantling of the institutional architecture that ensured regional cooperation. The dismantling of Latin American regionalism involves the use of weapons and the joining of defence and security agendas in terms of political enforcement.

POLICIES BEING ADOPTED: what is being done about it?

Given the current scenario, some policies are being established. In general:

(1) The region is no longer a priority to the foreign policy of South American governments. The centrality of the region in South American countries' foreign policies occurred in a context of expansion of South-South cooperation and of a search for the construction of a multipolar world. Today, however, the scenario is different: more traditional conceptions of foreign policy are once again hegemonic and, therefore, the global North is once again a priority for countries like Brazil, Chile and Argentina (during Mauricio Macri's administration).

(2) There is a proliferation of institutional regional forums, some of them with an ad-hoc character. In addition to the organizations already mentioned, such as Mercosur and

que começou a ser construído em 2015 e foi paralisado em 2017, pode-se destacar o muro que está sendo construído pelo Equador em sua fronteira com o Peru (LONDOÑO, 2017). Entre Chile e Bolívia, ademais da histórica rivalidade em função da disputa pelo mar, em 2017 uma tensão na fronteira se estendeu por vários meses após a detenção de funcionários alfandegários bolivianos em território chileno e da incursão de policiais chilenos dentro do território boliviano. Desde 2017, pode-se ver, também, a construção de novas bases militares bolivianas na fronteira com o Chile com o objetivo declarado de combater o contrabando.

A região fronteiriça mais tensa na América do Sul é aquela entre Colômbia e Venezuela. Em 2015, a situação na localidade de Cúcuta chegou à condição de colapso humanitário depois da deportação de migrantes colombianos por parte do governo venezuelano. Desde a acentuação da crise na Venezuela observa-se, também, um aumento das incursões por parte de forças de segurança pública venezuelanas em território colombiano e vice-versa. Em 2017, o governo colombiano denunciou agressões e assassinatos por parte da Guardia Nacional Venezolana no departamento de La Guajira. Em maio de 2021, Jesús Santrich, guerrilheiro dissidente das FARC, foi assassinato por forças de segurança pública colombianas, e o governo Venezuelano denuncia que isto tenha ocorrido em seu território nacional. Pode-se, ver, portanto, que rivalidades históricas e conflitos fronteiriços têm vindo à tona com mais ênfase desde 2015, apresentando novos riscos securitários para o subcontinente.

(7) Há, portanto, a intersecção de diversas crises:

A militarização da América passa pela intensificação de crises, como aquelas na Venezuela e na Colômbia, pela revitalização de crises fronteiriças e rivalidades históricas e pelo fortalecimento de um campo político que coloca militares em postos institucionais e a violência no centro de sua agenda pública. Tudo isto se dá em um cenário de desmonte da arquitetura institucional que garantia a cooperação regional. O desmonte do regionalismo latino-americano se dá pelas armas e pela junção das agendas de defesa e segurança em termos de execução política.

POLÍTICAS QUE ESTÃO SENDO ADOTADAS: o que está sendo feito a respeito?

Frente ao cenário atual, algumas políticas estão sendo estabelecidas. No geral:

(1) a região deixou de ser prioridade na política externa dos governos sul-americanos. A centralidade da região nas políticas externas dos países sul-americanos se deu em um contexto de expansão da cooperação sul-sul e da busca pela construção de um mundo multipolar. Hoje, no entanto, o cenário já é outro: concepções mais tradicionais de política externa voltaram a ser hegemônicas e, por isso, o norte global voltou a ser prioridade de países como Brasil, Chile e Argentina (sob o governo de Mauricio Macri).

(2) há uma proliferação de espaços regionais institucionais, alguns deles com caráter *ad hoc*, para além das organizações já mencionadas, como Mercosul e OEA; há diversos

the OAS, there are several other forums, such as the Andean Community, ALBA, CELAC, or even organizations whose profiles are more strictly linked to specific political camps, such as Prosul and the Puebla Group. Regionalization remained a reality in South America, Latin America and the American hemisphere, but in a less solid way, which generated an institutional multiplicity that is often uncoordinated. In other words, there are many local institutions, but they have little coordination capacity, because they are disconnected and do not ensure regional stability in the subcontinent.

(3) Institutional multiplicity leads to a *forum shopping* scenario (VELASCO, 2019, p.6) in which "state or non-state actors move through a wide variety of institutional mechanisms, favouring in each case or situation the one that best meets their concerns and interests".

(4) Even in the midst of regional institutional multiplicity, there are no organizations to think about security and/or defence cooperation. In this sense, the drafting of policies is the responsibility of national governments and, currently, the two agendas are often merged.

POLICY RECOMMENDATIONS: lessons from the South American context for regionalisms in crisis

Analysing the militarization context in South America is important not only for those who ponder about the subcontinent, but for all those interested in investigating regionalism. The South American experience of regional integration was one of the best structured throughout the 21st century, but from a different perspective than that adopted by the European Union, for example. While the EU initially progressed based on economic integration, South America, through UNASUR, did it on a basis of political and defence dialogue. Currently, it has already become evident that the South American process has gaps to be bridged. However, the lessons about the successes and, mainly, about what still needs to be done in South America are of great value for the other subcontinents. If South America must absorb and study the good practices of other regionalisms, the measures that must be adopted to avoid militarization are certainly of interest to the entire globe at a time of expansion of xenophobic and de-democratizing nationalisms. Some suggestions are presented below:

(1) Organizing an institutional architecture that ensures political cooperation among countries in the region:

Given the dismantling of UNASUR and the void in terms of regional cooperation and coordination, it is essential that there are multilateral forums for the peaceful settlement of disputes in South America. Therefore, it is urgent to reorganize an architecture that includes the entire subcontinent, as well as the various transnational political agendas. The multiplicity of organizations existing today in the subcontinent has not been able to resolve controversies or strengthen regionalisms. Hence the need for an umbrella structure to coordinate the various initiatives in order to build dialogue.

outros espaços, como a Comunidade Andina, a ALBA, a CELAC, ou mesmo organizações com perfis mais ligados a campos políticos específicos, como o Prosul e o Grupo de Puebla. Nota-se que a regionalização continuou a ser uma realidade na América do Sul, na América Latina e no hemisfério americano, mas de forma menos sólida, o que gerou uma multiplicidade institucional que, muitas vezes, é descoordenada. Ou seja, há muitas instituições localizadas, mas que são pouco coordenativas, já que desconectadas, e não garantem a estabilidade regional no subcontinente;

(3) a multiplicidade institucional traz um cenário de *forum shopping* (VELASCO, 2019, p. 6) em que "os atores estatais ou não estatais transitam por uma variedade ampla de mecanismos institucionais, privilegiando em cada caso ou situação aquele que melhor atende a seus anseios e interesses".

(4) mesmo em meio à multiplicidade institucional regional, não há organismos para pensar em cooperação securitária e/ou em defesa. A construção das políticas neste sentido fica a cargo dos governos nacionais e, atualmente, as duas agendas são frequentemente fundidas.

RECOMENDAÇÕES POLÍTICAS: lições do contexto sul-americano para regionalismos em crise

O estudo sobre o contexto de militarização na América do Sul é importante não apenas para aqueles que pensam o subcontinente, mas para todos aqueles interessados em pensar o regionalismo. A experiência sul-americana de integração regional foi uma das mais bem estruturadas ao longo do século XXI, mas tomando um ponto de partida diferente daquele adotado pela União Europeia, por exemplo. Enquanto esta caminhou, incialmente, a partir da integração econômica, a América do Sul, por meio da UNASUL, o fez a partir do diálogo político e de defesa. Atualmente, já se vê que o processo sul-americano tem buracos a serem preenchidos. No entanto, as lições sobre os sucessos e, principalmente, sobre o que ainda deve ser feito na América do Sul, são de grande valia para os outros subcontinentes. Se a América do Sul deve absorver e estudar as boas práticas de outros regionalismos, certamente as medidas que devem ser adotadas para evitar a militarização são de interesse de todo o globo em um momento de ampliação de nacionalismos xenofóbicos e de desdemocratização. Algumas sugestões são apresentadas abaixo:

(1) Organização de uma arquitetura institucional que garanta a cooperação políticaentre os países da região:

Frente ao desmonte da UNASUL e ao vazio em termos de cooperação e coordenação regional, é fundamental que haja, na América do Sul, espaços de solução pacífica de controvérsias que sejam multilaterais. Por isso, é urgente a reorganização de uma arquitetura que dê conta de todo o subcontinente e, junto com isto, dê conta das diversas agendas políticas transnacionais. A multiplicidade de organizações existentes hoje no subcontinente não foi capaz de resolver as controvérsias ou de solidificar regionalismos. Daí a necessidade de uma estrutura que funcione como guarda-chuva e coordenação entre as diversas iniciativas para a construção de diálogo.

(2) Expanding the debate on the meanings of regionalism:

The establishment of regional forums capable of promoting multilateralism depends on solid conceptions of regionalism. Which region are we talking about? What are the objectives of a regional political structure? How to enable the regional project to succeed in being transnational and, in this way, gather different political camps around itself? In South America, together with the weakening of UNASUR, the very concept of South America has been lost. As a result, other regionalisms gained more space, such as the Andean or the Hemispheric. Consequently, it is important to infuse political and ethical content to discussions on regionalism. In view of this, it is also important that political conceptions of regionalism always understand it as a tool for multilateralism — and not for exclusion. In a political context of increasing xenophobic nationalism, regionalism should be thought of as a way to promote dialogue and international cooperation. There is a fragile balance between nationalisms, regionalisms and multilateralism, but it is not only possible to do so: it is essential for peacekeeping.

(3) Developing differentiated policies for security and defence:

For the South America militarization process to be halted, it is necessary for the roles of the Armed Forces and the public security forces to be clearly defined and, therefore, that policies are developed with distinct parameters and objectives. After all, from the moment issues come to be understood as security agendas and seen as threats to national States and sovereignties, public policies related to them necessarily change — and, in this sense, they start to be seen as matters of defence. South America faces social issues that are transnational in nature and, therefore, shared by several countries, such as drug trafficking, organized crime and migration-related humanitarian crises. Hence, it is essential that South American social problems are faced as such, and not as security agendas. Therefore, it is crucial that 3.1) the security and defence agendas be separated. Furthermore, multilateral organizations 3.2) need organizations for the joint discussion of transnational social agendas within desecuritized scopes.

(4) Expanding and qualifying border policies:

Border-oriented policies must find room in regional multilateral organizations. Even though these are often bilateral issues, establishing rules and good practices makes the settlement of disputes easier. Furthermore, the presence of a mediator in border conflicts should be encouraged.

(5) Formulating and implementing foreign policy as public policy:

Finally, in a scenario of growing de-democratization in South America, it is essential to promote foreign policy profiles that are understood as public policies (MILANI; PINHEIRO, 2013). This should mean not only developing international policy strategies from the standpoint of different domestic public and social sectors, but also encouraging

(2) Ampliação do debate sobre os significados do regionalismo:

A construção de espaços regionais capazes de promover o multilateralismo depende de concepções sólidas de regionalismo. De qual região se está falando? Quais os objetivos almejados com a construção política regional? Como fazer com que o projeto regional consiga ser transnacional e, com isto, juntar diferentes campos políticos ao redor de si? Na América do Sul, junto com o esvaziamento da UNASUL, a própria concepção de América do Sul foi sendo perdida. Com isto, outros regionalismos foram tendo mais espaço, como o andino ou o hemisférico. Por isto, é importante dotar de conteúdo político e ético as discussões sobre o regionalismo. Frente a isto, é importante que as concepções políticas sobre o regionalismo sempre o entendam como instrumento de multilateralismo — e não de exclusão. Em um contexto político de aumento do nacionalismo xenofóbico, o regionalismo deve ser pensado como forma de promover diálogos e cooperação internacional. Há fragilidade no equilíbrio entre nacionalismos, regionalismos e multilateralismo, mas não só é possível fazê-lo: é essencial para a manutenção da paz.

(3) Construção de políticas diferenciadas para segurança e defesa:

Para que o processo de militarização da América do Sul seja paralisado, é necessário que as Forças Armadas e as forças de segurança pública tenham seus papéis bem definidos e, portanto, que sejam políticas construídas com forma e objetivos distintos. Afinal, a partir do momento em que temas passam a ser entendidos como agendas de segurança e vistos como ameaças aos Estados nacionais e às soberanias, necessariamente as políticas públicas a eles relacionadas se alteram — e, neste sentido, passam a ser encarados como assuntos de defesa. A América do Sul enfrenta questões sociais que são transnacionais e, portanto, compartilhadas por diversos países, como o tráfico de drogas, o crime organizado e as crises humanitárias em função de migrações. Neste sentido, é fundamental que os problemas sociais sul-americanos sejam encarados como tais, e não como agendas securitárias. Por isso, é crucial que 3.1) as agendas de segurança e defesa sejam separadas. Além disto, as organizações multilaterais 3.2) precisam de organismos para a discussão conjunta sobre agendas sociais transnacionais em escopos dessecuritizados.

(4) Ampliação e qualificação de políticas para fronteiras:

Políticas direcionadas às fronteiras devem ter espaços em organizações multilaterais regionais. Ainda que, muitas vezes, tratem-se de questões bilaterais, o estabelecimento de regras e de boas práticas facilita a solução de controvérsias. Além disso, a presença de um mediador nos conflitos fronteiriços deve ser estimulada.

(5) Formulação e implementação da política externa como política pública:

Por fim, em um cenário de crescente desdemocratização na América do Sul, é fundamental que haja a promoção de perfis de política externa que sejam compreendidos como políticas públicas (MILANI; PINHEIRO, 2013). Isto deve significar não apenas a construção de estratégias de política internacional a partir de diversos setores públicos

social participation in international agendas and in international organizations. The democratization of the international debate — still overly restricted to specific forums to which civil society has little access — is essential to prevent the remilitarization process from enduring. Peace is built constantly, day by day —therefore, it must be part of the daily life of civil society.

Sources:

BIROLI, Flavia. Gênero, "valores família" e democracia. In: BIROLI, Flavia. MACHADO, Maria. VAGGIONE, Juan. Gênero, neoconservadorismo e democracia. São Paulo: Boitempo, 2020.

CLOSS, Marília. Transformações na mobilização da violência na América do Sul: comparação de conjunturas críticas para o estudo de caso da crise na Venezuela. Rio de Janeiro, **Revista Sul Global,** v. 1, n. 1, 2020.

FUCCILLE, Luis. As forças armadas e a missão militar no governo FHC. Aracaju, **Revista TOMO**, v. 6, n. 1, 2003.

GAMBOA, Laura. El reajuste de la derecha colombiana. Bogotá, Colombia Internacional: v. 99, 2019.

LONDOÑO, Andrés. Fronteiras sul-americanas: reflexões sobre tensões e os conflitos recentes. Rio de Janeiro, Boletim OPSA, v. 12, n. 4, 2017.

MARTINEZ, Elias. LYRA, Mariana. O Processo de Dessecuritização do Narcotráfico na Unasul. Rio de Janeiro, **Contexto Internacional**, v. 37, n. 2, 2015.

MILANI, Carlos; PINHEIRO, Leticia. Política Externa Brasileira: Os Desafios de sua Caracterização como Política Pública. Rio de Janeiro, **Contexto Internacional**, vol. 35, n. 1, 2013.

NOZAKI, William. Militarização da Administração Pública no Brasil: projeto de nação ou projeto de poder? Caderno da Reforma Administrativa, Fórum Nacional Permanente de Carreiras Típicas de Estado (Fonacate), 2021.

PASSOS, Anais. ACÁCIO, Igor. A militarização das respostas à COVID-19 nas democracias Latino-americanas. São Paulo, **RAP**: Revista de Administração Pública, 2021.

SAINT-PIERRE, Héctor Luis. "Defesa" ou "Segurança"? Reflexões em Torno dos Conceitos e Ideologias. Rio de Janeiro, **Contexto Internacional**, vol. 33, n. 2, 2011.

SANAHUJA, José. Regionalismo post-liberal y multilateralismo en sudamérica: el caso de UNASUR. **Anuario de la integración regional de América Latina y el gran Caribe**. 2012.

VELASCO, Paulo. A falência das instituições regionais diante da crise venezuelana. Rio de Janeiro, Boletim OPSA, v. 14, n. 2, 2019.

e sociais domésticos, mas, também, a promoção de participação social em agendas internacionais e em organismos internacionais. A democratização do debate internacional — ainda tão restrito a espaços específicos de pouco acesso à sociedade civil — é fundamental para evitar que o processo de remilitarização tenha continuidade. A paz é construção constante e diária — e, portanto, deve fazer parte do cotidiano da sociedade civil.

Fontes:

BIROLI, Flavia. Gênero, "valores família" e democracia. In: BIROLI, Flavia. MACHADO, Maria. VAGGIONE, Juan. **Gênero, neoconservadorismo e democracia.** São Paulo: Boitempo, 2020.

CLOSS, Marília. Transformações na mobilização da violência na América do Sul: comparação de conjunturas críticas para o estudo de caso da crise na Venezuela. Rio de Janeiro, **Revista Sul Global**, v. 1, n. 1, 2020.

FUCCILLE, Luis. As forças armadas e a missão militar no governo FHC. Aracaju, **Revista TOMO**, v. 6, n. 1, 2003.

GAMBOA, Laura. El reajuste de la derecha colombiana. Bogotá, **Colombia Internacional**: v. 99, 2019.

LONDOÑO, Andrés. Fronteiras sul-americanas: reflexões sobre tensões e os conflitos recentes. Rio de Janeiro, Boletim OPSA, v. 12, n. 4, 2017.

MARTINEZ, Elias. LYRA, Mariana. O Processo de Dessecuritização do Narcotráfico na Unasul. Rio de Janeiro, **Contexto Internacional**, v. 37, n. 2, 2015.

MILANI, Carlos; PINHEIRO, Leticia. Política Externa Brasileira: Os Desafios de sua Caracterização como Política Pública. Rio de Janeiro, **Contexto Internacional**, vol. 35, n. 1, 2013.

NOZAKI, William. **Militarização da Administração Pública no Brasil:** projeto de nação ou projeto de poder? Caderno da Reforma Administrativa, Fórum Nacional Permanente de Carreiras Típicas de Estado (Fonacate), 2021.

PASSOS, Anais. ACÁCIO, Igor. A militarização das respostas à COVID-19 nas democracias Latino-americanas. São Paulo, **RAP**: Revista de Administração Pública, 2021.

SAINT-PIERRE, Héctor Luis. "Defesa" ou "Segurança"? Reflexões em Torno dos Conceitos e Ideologias. Rio de Janeiro, **Contexto Internacional**, vol. 33, n. 2, 2011.

SANAHUJA, José. Regionalismo post-liberal y multilateralismo en sudamérica: el caso de UNASUR. **Anuario de la integración regional de América Latina y el gran Caribe**. 2012.

VELASCO, Paulo. A falência das instituições regionais diante da crise venezuelana. Rio de Janeiro, **Boletim OPSA**, v. 14, n. 2, 2019.

Tássio Franchi

Tássio Franchi é Doutor em Desenvolvimento Sustentável (CDS-UnB), Mestre em História (UNESP/Franca) e Graduado em História (UEL).
É professor adjunto do Instituto Meira Mattos na Escola de Comando e Estado-Maior do Exército (IMM/ECEME).

Tássio Franchi has a Doctorate in Sustainable Development (CDS-UnB), a Master's degree in History (UNESP/Franca), and a Bachelor's degree in History (UEL). He is an adjunct professor at Meira Mattos Institute at the Brazilian Army Command and General Staff College (IMM/ECEME).

Guerras no século XXI: uma perspectiva a partir das fronteiras sul-americanas

Wars of the 21st century: a perspective from the south american borders

Tássio Franchi

SUMÁRIO EXECUTIVO

As guerras interestatais na América do Sul são historicamente subclassificadas pelas bases de classificação de conflitos, o que gera uma percepção, na comunidade internacional, de que o subcontinente é uma região pacífica e livre de conflitos.

Este *policy paper* vem discutir como, sob o manto de paz, escondem-se animosidades históricas e conflitos latentes que retornam quando as condições se tornam favoráveis. Feito isso, indicamos ações que podem colaborar para identificar tensões e promover a construção de bases mais sólidas para a estabilidade e a paz regional nas próximas das décadas.

INTRODUÇÃO

A ausência de guerras declaradas não significa a existência de paz. Essa é uma verdade que se aplica tanto a países que são *players* globais como a países com ação limitada aos seus contextos regionais. Durante décadas, sob o manto da paz, esconderam-se tensões e interesses que explodiram em conflitos violentos entre os países sul-americanos. A partir dessa constatação, impõe-se a necessidade de compreender os conflitos entre os países como o primeiro passo para tentar preveni-los.

EXECUTIVE SUMMARY

Interstate Wars in South America are historically under-classified in conflict classification bases, which leads the international community to perceive the subcontinent as a peaceful, conflict-free region.

This policy paper addresses how, under the cloak of peace, veiled historical animosities and latent conflicts emerge when conditions become favourable. Actions are then indicated that can help identify tensions and promote the construction of stronger foundations for regional stability and peace in the coming decades.

INTRODUCTION

The absence of declared wars does not mean the existence of peace. This dictum applies both to countries that are global players and to countries whose actions are limited to their regional contexts. For decades, under the guise of peace, tensions and interests that erupted into violent conflicts between South American countries were concealed. Based on this observation, the need arises to understand conflicts between countries as the first step in trying to prevent them.

There are two concepts under which to analyse peace and war in South America. "Long peace", which interprets the region as peaceful, without significant clashes between States; and "violent peace", which admits the existence of latent tensions, sometimes frozen, due to regional and international geopolitical pressures or due to the conjunctural inability of countries that, in spite of it, did not dismiss weapons as an alternative to action.

Considering the second concept as valid, it is necessary to reflect on how wars between South American countries have happened, to analyse which elements of tension remain latent and need to be monitored so those countries do not find themselves on the battlefield again. One way to do so is to review the taxonomies of interstate conflicts, confronting them with historical data and with the new regional and global contexts, in order to detect the false notes in the concert of South American nations.

TYPIFYING THE MONSTER

Carl von Clausewitz was dedicated to understanding the war between nation-states in its essence, overcoming the shackles of temporal and technological contexts. Some important Clausewitzian concepts are essential for us to continue. *(i) War as a limited act of violence* — war can be defined as a large-scale duel, in which one contender tries to impose his will on the other by the use of force (violence). Victory comes not only from the enemy's unconditional surrender, but also from the moment when one side loses the will to fight and begins to negotiate peace. In other words, war does not have to be an all-encompassing enterprise, it can be limited. *(ii) The primacy of politics* — war must be understood as a continuation of politics with other means. It is the political will that defines the objectives to be achieved in war, and it is up to the military, with strategies and the use of force, to achieve them (CLAUSEWITZ, 2010). Armies fight wars, political disputes make them and end them when their goals have been achieved or when they find themselves unable to reach them.

Hence war, understood as the use of force by political entities, can be classified in various different ways and we are interested in wars between States, particularly in the same continent. But how to differentiate a border incident from an act of war? How to classify a confrontation between two countries? To do so, we resort to the classifications of war. Three of the biggest conflict classification projects are: the Correlates of War (COW), at the University of Michigan in the USA; the Uppsala Conflict Data Programme (UCDP), at Uppsala University in Sweden; the Conflict Barometer (CB), at the Heidelberg Institute in Germany.

COW classified wars into nine different manifestations and into four categories that allow us to understand who the involved actors (State or non-State) are, and the location where the conflict takes place. In brief: "Interstate Wars"; "Extra-State Wars", fought in colonies, for example; "Intra-State Wars", such as civil wars; and "Non-State Wars".

Since the beginning of the COW project in the 1970s and until today, two of its basic criteria for identifying an interstate war have been: *(i)* a threshold of a minimum of 1,000 deaths associated with the set of battles fought between at least two actors; *(ii)*

Existem duas linhas de interpretações sobre a paz e a guerra na América do Sul. A "longa paz", que interpreta a região como pacífica, sem confrontos significativos entre os Estados e a "paz violenta", que admite a existência de tensões latentes, por vezes congeladas, devido a pressões geopolíticas regionais e internacionais ou a incapacidades conjunturais dos países que, apesar disso, não dispensaram as armas como alternativa de ação.

Considerando válida a segunda linha, é preciso refletir sobre como aconteceram as guerras entre os países sul-americanos, analisar quais elementos de tensão permanecem latentes e precisam ser monitorados para que os países não voltem a se encontrar nos campos de batalha. Para tanto, um caminho é rever as taxonomias dos conflitos interestatais, confrontando-as com dados históricos e com os novos contextos regionais e globais a fim de ouvir os ruídos no concerto das nações sul-americanas.

TIPIFICANDO O MONSTRO

Carl von Clausewitz se dedicou a compreender a guerra entre Estados nacionais em sua essência, vencendo as amarras dos contextos temporais e tecnológicos. Dele, extraímos alguns conceitos importantes para continuar. *(i) A guerra como um ato de violência limitado* — a guerra pode ser definida como um duelo em larga escala, em que um contendedor tenta impor, pelo uso da força (violência), sua vontade ao outro. A vitória não vem apenas da rendição incondicional do inimigo, mas também do momento em que um lado perde a vontade de lutar e passa a negociar a paz. Ou seja, a guerra não precisa ser um empreendimento total, ela pode ser limitada. *(ii) O primado da política* — a guerra deve ser compreendida como a continuação da política por outros meios. São as vontades políticas que definem os objetivos a serem alcançados na guerra, cabendo aos militares, por meio de estratégias e do emprego da força, alcançá-las (CLAUSEWITZ, 2010). Exércitos lutam as guerras, disputas políticas as fazem e as encerram quando veem satisfeitos seus interesses ou se descobrem incapazes de alcançá-los.

A guerra, entendida, então, como uso da força por entes políticos, tem diversas classificações possíveis e interessam-nos as guerras entre Estados, particularmente em um mesmo continente. Mas, como diferenciar um incidente fronteiriço de um ato de guerra? Como classificar o confronto entre dois países? Para tanto, recorre-se às classificações da guerra. Três dos maiores projetos de classificação de conflitos são: *Correlates of War* (COW), da Universidade de Michigan nos EUA; *Uppsala Conflict Data Program* da Universidade Uppsala, na Suécia; *Conflict Barometer* do Instituto Heidelberg, na Alemanha.

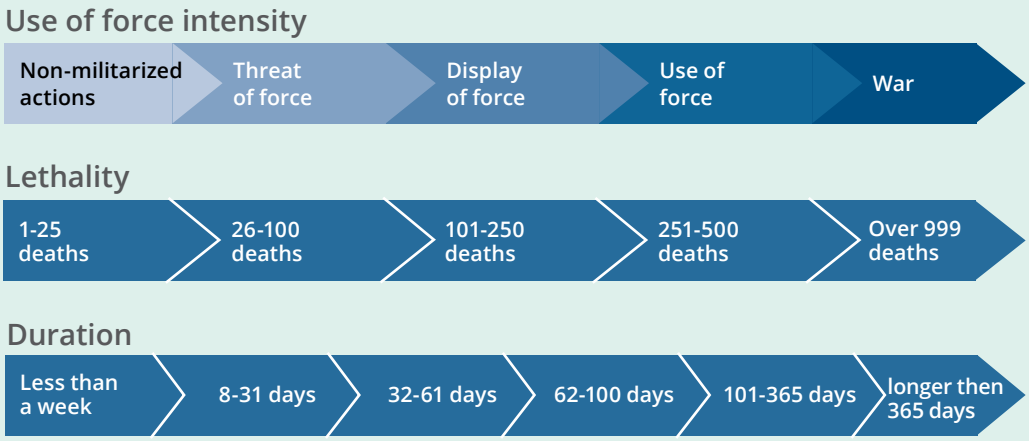
No COW, as guerras foram tipificadas em nove diferentes manifestações e em quatro categorias que permitem entender quem são os atores envolvidos (estatais ou não-estatais) e o espaço onde o conflito ocorre. Em síntese: "Guerra entre Estados"; "Guerras exteriores", lutadas em colônias, por exemplo; "Guerras internas", como guerras civis; e "Guerras com atores não-estatais".

Desde o início do projeto COW, na década de 1970, e até hoje, dois dos seus critérios básicos para identificar uma guerra interestatal permanecem: *(i)* um limite de, no mínimo, 1.000 mortes associadas ao conjunto de batalhas travadas entre, no mínimo,

the presence, on both sides, of organisations capable of conducting organised combat (armed forces).

> [...] inter-state wars are those that involve the armed forces of two or more members of the interstate system (states) in sustained combat. (...) Hostilities must also involve a minimum of 1,000 fatalities between or among the armed forces per year (or 12-month period), beginning with the start date of the war. (SARKEES and WAYMAN, 2010, p. 75)

Expanding the pre-existing bases in COW, the Militarised Interstate Dispute (MID) dataset used specific indicators of interstate wars seeking to understand the incidents that generated conflicts and measuring the use of force. The result was a classification ranging from non-militarised actions to war, which, in turn, has indicators such as: intensity, lethality and duration.



Source: Adapted from GHOSN, PALMER and BREMER, 2004, p. 142-143

The measurement is taken per "militarised incident", which can be summarised as: a threat of military action; a display of military strength; and the use of military force by one State against another (GHOSN, PALMER and BREMER, 2004). However, it is only when the use of force reaches a lethality rate of more than a thousand deaths that a "conflict" can be classified as "war".

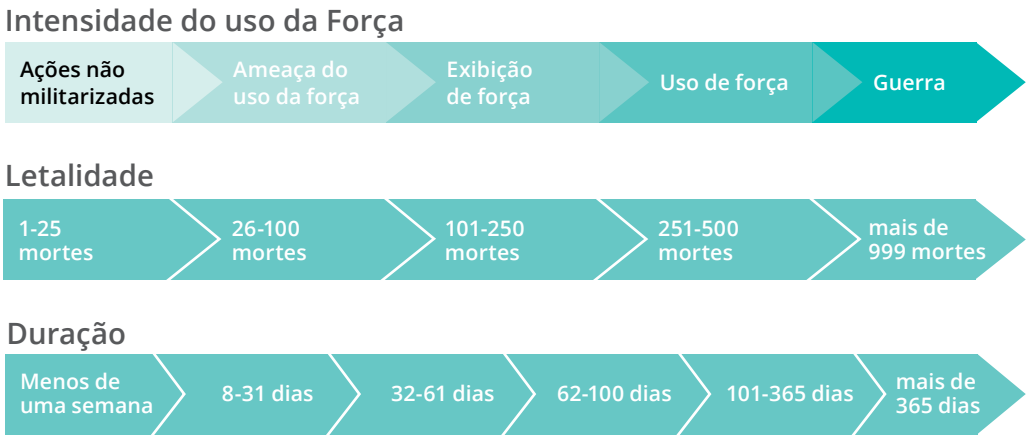
The UCDP has been dedicated to measuring conflict lethality rates and classifies wars into four types: "extra-systemic", "interstate", "intrastate", and "internationalised intrastate conflict" (at borders). However, unlike the MID, it only starts to consider a situation as a "conflict" after the first 25 deaths/year; between 25 and 999 deaths, the classification is a "minor conflict", for more than 1,000 deaths/year the classification is "war" (PETTERSON and WALLENSTEEN, 2015).

In turn, the CB classifies conflicts into five types: "Dispute", "Non-violent crisis", "Violent crisis", "Limited conflict", and "War", the first two being characterised by the absence of the use of force, whereas the last three, by its presence. The CB uses five indicators with up to three different levels of intensity for each of them, and its classification is obtained by adding up these variables. In addition to fatality, common to all previous indexes, the CB introduces the following variables: (i) the material used

dois atores; *(ii)* a presença, em ambos os lados, de organizações capazes de conduzir combates organizados (forças armadas).

> [...] guerras interestatais são aquelas que envolvem forças armadas de dois ou mais integrantes do sistema interestadual (estados) em combate sustentado. (...) As hostilidades também devem envolver um mínimo de 1.000 mortes entre as forças armadas por ano (ou período de 12 meses), começando com a data de início da guerra. (SARKEES e WAYMAN, 2010, p. 75)

Ampliando as bases preexistentes no COW, o projeto *Military Interstate Dataset* (MID) levantou indicadores específicos para as guerras interestatais buscando compreender os incidentes que geraram conflitos e mensurando o uso da força. O resultado foi uma classificação que vai de ações não militarizadas até a guerra, a qual, por sua vez, tem indicadores como: intensidade, letalidade e duração.



Fonte: adaptado de GHOSN, PALMER e BREMER, 2004, p. 142-143

A mensuração é feita por "incidentes militarizados", que podem ser sintetizados como: uma ameaça de ação militar; uma exibição de força militar; o uso da força militar por um Estado contra outro (GHOSN, PALMER e BREMER, 2004). Entretanto, somente quando o uso da força atinge letalidade de mais de mil mortes é que um "conflito" pode ser classificado como "guerra".

O *Uppsala Conflict Data Program* (UCDP) tem-se dedicado a medir os índices de letalidade dos conflitos e classifica as guerras em quatro tipos: "extrassistêmico", "interestatal", "interno" e "conflito interno internacionalizado" (nas fronteiras). Mas, diferente do MID, só começa a considerar uma situação como um "conflito" após as primeiras 25 mortes/ano; entre 25 e 999 mortes, classifica-a como um "conflito menor" e aquelas com mais de 1.000 mortes/ano, como "guerras" (PETTERSON e WALLENSTEEN, 2015).

Por sua vez, o *Conflict Barometer (CB)* classifica os conflitos em cinco tipos: "Disputa", "Crise não violenta", "Crise violenta", "Conflito limitado" e "Guerra", sendo os dois primeiros caracterizados pela ausência do uso de força e os três últimos, pela presença dela. O CB usa cinco indicadores com até três diferentes níveis de intensidade para cada uma delas, sendo sua classificação obtida pelo somatório destas variáveis. Além da mortalidade, comum a todos os índices anteriores, o CB apresenta como variáveis: (i) o material

(light or heavy); (ii) the military personnel involved; (iii) lethality; (iv) the destruction of basic infrastructure, cultural assets, homes, and the economy; (v) and the number of displaced people and refugees as a result of the conflict (WANCKE, 2015).

Classification of conflicts according to the *Conflict Barometer*

Intensity	Terminology	Level of violence	Intensity class
1	Dispute	Non-violent conflict	Low intensity
2	Non-violent crisis		
3	Violent	Violent conflict	Medium intensity
4	Limited conflict		High intensity
5	War		

Source: Wancke, 2015

Thus, conflict classification can start in phases prior to the use of force and with different intensities. However, only when it reaches high levels of violence can a "conflict" be classified as a "war". In this taxonomy, South American conflicts are under-classified again.

The systematisation efforts described have brought advances to the understanding of wars. Nevertheless, the fact that the starting point for reflection are countries that have been the scene of world wars may make analysts short-sighted in relation to wars on other continents that do not have a similar degree of industrialisation, demographic characteristics or military capacity. A war does not need hundreds of fatalities or to drag on for years with high destruction rates; a war needs motives (political will) and actions (use of violence) carried out in accordance with the capabilities of the fighters involved.

THERE ARE NO WARS IN THE TROPICAL PARADISE: LONG PEACE AND VIOLENT PEACE

Scholars maintain that South America is a region that is experiencing a long period of peace, without relevant wars between its States. In general, they support their studies with the databases cited here, or make comparisons with other conflicts of the 20th and 21st century, such as the Iraq Wars (1991 and 2003). According to Centeno, it can be said that "the last two centuries have not seen the level of war that was common to other regions. No matter how it is approached, South America appears remarkably peaceful" (2002, p. 37).

In fact, looking at indicators such as "duration" and "fatalities" (+1,000 deaths/year), in the entire 20th century, there would have been only one war on the continent, the Chaco War (1932-1935), the others taking place in the 21st century. All other conflicts would have been "minor conflicts". That is what the data in COW show. Between 1816 and 2007, 227 wars were recorded in the world, and only 8 in South America. Of these 8, only 3 in the 20th century, and neither the Cenepa War (1995) nor the Falkland Islands War (1982) meet the requirement of one thousand deaths per year.

empregado (leve ou pesado); (ii) os efetivos militares envolvidos; (iii) letalidade; (iv) a destruição de infraestrutura básica, bens culturais, casas e economia; (v) e o número de deslocados e refugiados oriundos do conflito (WANCKE, 2015).

Classificação de conflitos de acordo com *Conflict Barometer*

Intensidade	Terminologia	Nível de violência	Classe de intensidade
1	Disputa	Conflito não violento	Baixa intensidade
2	Crise não violenta		
3	Crise violenta	Conflito violento	Intensidade média
4	Conflito limitado		Alta intensidae
5	Guerra		

Fonte: Wancke, 2015

Com isso, a classificação de conflito pode ter início em fases anteriores ao uso da força e com intensidades diferentes. Entretanto, só quanto atinge níveis elevados de violência é que um "conflito" pode ser classificado como "guerra". Nesta taxonomia, os conflitos sul-americanos aparecem subclassificados novamente.

Os esforços de sistematização descritos trouxeram avanços na compreensão das guerras. Entretanto, o fato de serem pensados a partir de países que foram palcos de guerras mundiais pode torná-los míopes em relação à guerra em outros continentes que não têm índices semelhantes de industrialização, demografia ou capacidade militar. Uma guerra não precisa de centenas de mortos ou de se arrastar por anos, com altos índices de destruição; uma guerra precisa de motivos (vontades políticas) e ações (emprego da violência) executadas de acordo com as capacidades dos lutadores envolvidos.

NÃO EXISTEM GUERRAS NO PARAÍSO TROPICAL: A LONGA PAZ E A PAZ VIOLENTA

Estudiosos sustentam que a América do Sul é uma região que vive um longo período de paz, sem guerras relevantes entre seus Estados. No geral, apoiam seus estudos nas bases de dados apresentadas, ou fazem comparações com outros conflitos do século XX e XXI, como as Guerras do Iraque (1991 e 2003). Segundo Centeno, pode-se dizer que "os últimos dois séculos não viram o nível de guerra que era comum a outras regiões. Não importa como seja abordada, a América do Sul parece notavelmente pacífica" (2002, p. 37).

De fato, olhando indicadores como "duração" e "fatalidades" (+1.000 mortos/ano), em todo o século XX teria ocorrido apenas uma guerra no continente, a Guerra do Chaco (1932-1935), ficando as outras no século XIX. Todos os outros conflitos teriam sido "conflitos menores". Isso é o que dizem os dados em *Correlates of War* que, entre 1816 e 2007, contabilizam 227 guerras no mundo e apenas 8 na América do Sul. Destas 8, apenas 3 no século XX, sendo que nem a Guerra do Cenepa (1995), nem a Guerra das Malvinas/Falklands (1982) atendem ao quesito de mil mortes por ano.

Correlates of War - Wars in South America 1816–2007

Name	Century	Deaths	Classification
Cenepa War (1995)	XX	up to 400	Minor Conflict
Falkland Islands War (1982)		905	Minor Conflict
Chaco War (1932-1935)		80-100 thousand	War
Pacific War (1879-1883)	19th	25-30 thousand	War
Chincha Islands War (1865-1866)		1.000	War
War of the Triple Alliance (1864-1870)		440 thousand	War
Ecuadorian-Colombian War (1863)		1.500	War
Platine War (1851-1852)		1.800	War

Source: Correlates of War (SARKEES, WAYMAN, 2010).

But what were the means found by the countries in the region to build such a long-lasting peace? Summarizing some of the central arguments around the "long peace", we have: *(i)* explanations of an economic-liberal nature, which maintain that the search for development, economic interdependence and integration acted in favour of peaceful solutions to conflicts; *(ii)* satisfaction with the territorial *status quo* (KACOWICZ, 1998); *(iii)* wars occurred mainly over border disputes that lost momentum after 1945, being resolved diplomatically without producing armed conflicts (HUTH, 2009); *(iv)* the limitations of public spending on the defence sector would leave the Armed Forces unable to wage wars (BATTAGLINO 2008); and *(v)* the cooperation among South American armed forces in the recent period.

Economic interdependencies and regional integration are a strong argument for maintaining regional peace. The European Union and Mercosur are examples of this: since they were established, there have been no armed conflicts between their members.

However, one needs to remember that tensions in the La Plata River basin have already been high between Argentina, Brazil and Paraguay due to the use of water resources for energy generation. Diplomatic tensions and demonstrations of strength occurred since the announcement of the construction of the Itaipu Hydroelectric Dam and lasted until the signing of the Tripartite Itaipu-Corpus Agreement in 1979 (NETO, 2021). In 2023, the review of Annex C of the Treaty of Itaipu will take place, which will interfere in the prices and quantities of energy distributed. This situation may require a new rebalancing between countries.

It is also necessary to take into account the effect on interstate relations of the Covid-19 pandemic, which caused the closure of the borders of the Mercosur countries, and the disputes over the supplies to fight the disease, which may have shaken some relations and whose impacts are still being measured (LAURO et al, 2020).

Arguments regarding satisfaction with the territorial *status quo* and their disputes resolved by international arbitration are recurrent. Centeno synthesises this vision:

Correlates of War - Guerras na América do Sul 1816–2007

Nome	Século	Mortos	Classificação
Guerra do Cenepa (1995)	XX	até 400	Conflito Menor
Guerra das Malvinas/Falklands (1982)		905	Conflito Menor
Guerra do Chaco (1932-1935)		80-100 mil	Guerra
Guerra do Pacífico (1879-1883)	XIX	25-30 mil	Guerra
Guerra das ilhas Chincha (1865-1866)		1.000	Guerra
Guerra do Paraguai ou Tríplice Aliança (1864-1870)		440 mil	Guerra
Guerra Equatoriana-Colombiana (1863)		1.500	Guerra
Guerra do Prata (1851-1852)		1.800	Guerra

Fontes: Correlates of War (SARKEES, WAYMAN, 2010).

Mas quais seriam os meios encontrados pelos países da região para construir uma paz tão douradora? Sintetizando alguns dos argumentos centrais em torno da "longa paz", temos: *(i)* explicações de cunho econômico-liberal, que defendem que a busca pelo desenvolvimento, a interdependência econômica e a integração atuaram em prol de soluções pacíficas de conflitos; *(ii)* satisfação com o *status quo* territorial (KACOWICZ, 1998); *(iii)* as guerras ocorreram principalmente por questões territoriais que passaram a ter pouca importância pós-1945, sendo resolvidas diplomaticamente sem produzir conflitos armados (HUTH, 2009); *(iv)* as limitações dos gastos públicos com o setor de defesa deixariam as FFAA incapacitadas de travar guerras (BATTAGLINO 2008); e *(v)* a cooperação entre as Forças Armadas sul-americanas no período recente.

As interdependências econômicas e a integração regional são um forte argumento para a manutenção da paz regional. A União Europeia e o Mercosul são exemplos disto: desde que foram instituídos, não ocorreram conflitos armados entres seus membros.

Todavia, é preciso lembrar que as tensões na bacia do Prata já estiveram elevadas entre Argentina, Brasil e Paraguai devido ao uso dos recursos hídricos para a geração de energia. Tensões diplomáticas e demonstrações de força ocorreram desde o anúncio da construção da Usina Hidroelétrica de Itaipu até a assinatura do acordo tripartite Itaipu-Corpus em 1979 (NETO, 2021). Em 2023, vai ocorrer a revisão do Anexo C do Tratado de Itaipu, que vai interferir nos preços e nas quantidades de energia distribuídas e essa situação poderá exigir novo reequilíbrio entre os países.

É preciso ter em conta, também, o efeito nas relações interestatais da pandemia de Covid-19, que provocou o fechamento de fronteiras dos países do Mercosul, e as disputas em torno dos insumos para o combate à doença, que podem ter estremecido algumas relações e cujos impactos ainda estão sendo mensurados (LAURO et al, 2020).

Os argumentos em torno da satisfação com o *status quo* territorial e suas disputas resolvidas por arbitragens internacionais são recorrentes. Centeno sintetiza essa visão:

> Nowhere is the general peace of the continent more clearly seen than on a map. Examine a map of Latin America in 1840 and the general borders and country configurations look surprisingly like today's. While early units such as Gran Colombia, the Central American Republic, and the Peruvian-Bolivian Confederation have vanished, no politically recognised state has disappeared through conquest (CENTENO, 2002, p. 10).

When scrutinising the map of South America, the author did not consider, among other aspects, that: Bolivia had an exit to the sea; Ecuador had a border with Brazil (until 1941); Colombia, Chile, Brazil, Paraguay, and Peru increased their territories, that is, other countries lost territory (FRANCHI, et al. 2017). Such territorial losses were ratified by protocols of understanding and international mediation, but with troops still in the disputed areas, which ensured a more advantageous position in negotiations. Such was the case of Ecuador that, by signing the *Protocolo de Paz, Amistad y Límites* mediated by Brazilian chancellor Oswaldo Aranha, lost almost fifty percent of its territory in 1942. In fact, the border conflicts between Peru and Ecuador extend from 1829 to 1995, bringing the total to more than 150 years of alternation between moments of freezing, latency and wars (BARROSO, 2007).

The Falkland Islands War (1982) is another centuries-old conflict, in which a military operation was carried out as a way to secure advantages at the diplomatic negotiation table that would follow, although the dictates of war led Argentina to defeat (GÓMEZ, 2019). The dispute over the territory of Essequibo, between Venezuela and Guyana, has been going on since the mid-19th century, with disputed and undefined agreements between the parties. The discovery of oil fields in the region rekindled Venezuelan interests, which created a secured zone called the "Atlantic Façade", entering the Guyana territorial sea (YNFANTE, 2020).

We realise that diplomatic mediations have cooled down, but have not resolved the conflicts, which have survived fuelled by diplomatic disputes or through sporadic demonstrations of force, awaiting the time for more violent actions. Fundamentally, the trait of constant diplomatic contestation must be noted as a strange timbre in the harmony between nations.

Another type of interstate tension not linked to a territorial dispute, but to a feeling of loss of sovereignty at the borders, occurs when, in the fight against non-state actors, the territorial limits of countries are crossed. The "Angostura" incident (2008-2010) dragged Colombia, Ecuador and Venezuela into diplomatic clashes and mobilisation of troops on the borders of these countries because a Colombian military operation penetrated a few kilometres into Ecuadorian territory to attack a FARC camp (BUSTILLOS, BRAVO, 2019).

The inability of South American States and armed forces to wage wars, either because of budgetary constraints or organisational incompetence, is another argument for regional peace. "War requires basic organisational competence and access to resources that only certain states have. From this point of view, Latin America has been peaceful because the states in the region have never developed the political capacity to wage prolonged wars" (CENTENO, 2002, p. 91).

> *Nowhere is the general peace of the continent more clearly seen than on a map. Examine a map of Latin America in 1840 and the general borders and country configurations look surprisingly like today's. While early units such as Gran Colombia, the Central American Republic, and the Peruvian-Bolivian Confederation have vanished, no politically recognized state has disappeared through conquest* (CENTENO, 2002, p. 10).[1]

Ao observar o mapa da América do Sul, o autor não considerou, dentre outros aspectos, que: a Bolívia possuía uma saída para o mar; o Equador possuía fronteira com o Brasil (até 1941); Colômbia, Chile, Brasil, Paraguai e Peru aumentaram seus territórios, ou seja, outros países perderam territórios (FRANCHI, et al. 2017). Tais perdas territoriais foram ratificadas com protocolos de entendimentos e com mediação internacional, mas com tropas ainda no terreno disputado, o que garantia uma posição mais vantajosa nas negociações. Foi o caso do Equador que, ao assinar o *Protocolo de Paz, Amistad y Límites* mediado pelo chanceler brasileiro Oswaldo Aranha, perdeu quase cinquenta por cento do seu território, em 1942. De fato, os conflitos fronteiriços entre Peru e Equador se estendem desde 1829 até 1995, perfazendo mais de 150 anos de alternância entre momentos de congelamento, latência e guerras (BARROSO, 2007).

A Guerra das Malvinas/Falklands (1982) é outro litígio secular em que uma operação militar foi realizada como forma de obter vantagens na mesa de negociações diplomáticas que se seguiria, embora o acaso da guerra tenha levado a Argentina à derrota (GÓMEZ, 2019). O litígio pelo território do Essequibo, entre a Venezuela e a Guiana, se estende desde meados do século XIX, com acordos contestados e sem definição entre as partes. As descobertas de campos petrolíferos na região reacenderam os interesses venezuelanos, que criaram uma área de segurança chamada "Fachada Atlântica", adentrando o mar territorial da Guiana (YNFANTE, 2020).

Percebemos que as mediações diplomáticas esfriaram, mas não resolveram os conflitos, que sobreviveram alimentados com contestações diplomáticas ou através de demonstrações de força esporádicas, aguardando o momento de ações mais violentas. Fundamentalmente, o traço da contestação diplomática constante deve ser notado como um timbre estranho na harmonia entre as nações.

Outro tipo de tensão interestatal não ligada a uma disputa territorial, mas a um sentimento de perda de soberania nas fronteiras acontece quando, no combate a atores não estatais, atravessam-se os limites territoriais dos países. O incidente de "Angostura" (2008-2010) arrastou Colômbia, Equador e Venezuela para rusgas diplomáticas e mobilização de tropas nas fronteiras desses países porque uma operação militar colombiana penetrou alguns quilômetros no território equatoriano para atacar um acampamento das FARC (BUSTILLOS, BRAVO, 2019).

A incapacidade de os Estados e de as Forças Armadas sul-americanas travarem guerras,

[1] Em lugar algum a paz geral do continente é vista de modo mais claro do que em um mapa. Examine um mapa da América Latina em 1848 e as fronteiras gerais e a configuração dos países aparecem de modo surpreendentemente similar ao de hoje. Enquanto unidades antigas, como a Grã Colômbia, a República Central Americana e a Confederação Peru-Boliviana desapareceram, nenhum estado politicamente reconhecido desapareceu devido a conquista. (Nota do Revisor)

Wars do not require organisational competence, they require clear political objectives, armies and the will to fight. Competence, military efficiency and resources collaborate to decide the outcome of the conflict, not its outbreak. All of the American or Soviet military competence did not save them from defeats against less institutionally organised armies in Vietnam and Afghanistan. One can also note the wars between States on the African continent, whose armies do not have high standards of organisation (WILLIAMS, 2017).

From the standpoint of budgetary constraints, defence spending in South America has been below 2% of GDP in the last five years. The only exceptions are Colombia and Ecuador that have consistently spent more than 2% of their GDP on defence in the last 5 years.

Military expenditures in relation to GDP (%)

Country	1990	1995	2000	2005	2010	2015	2016	2017	2018	2019
Colombia	1,86	2,83	3,03	3,35	3,63	3,11	3,07	3,21	3,07	3,15
Ecuador	1,89	2,34	1,45	2,30	3,01	2,62	2,51	2,36	2,35	2,29
Chile	3,40	2,56	2,70	2,52	2,24	1,90	1,92	1,93	1,86	1,82
Uruguay	3,53	2,71	2,44	2,00	1,88	1,82	1,87	1,96	2,13	2,02
Bolivia	2,82	2,10	2,06	1,77	1,67	1,74	1,63	1,54	1,54	1,42
Guyana	0,91	0,92	1,77	1,41	1,38	1,45	1,48	1,64	1,60	1,65
Brazil	2,36	1,86	1,73	1,52	1,54	1,37	1,35	1,42	1,51	1,48
Peru	2,68	2,64	1,79	1,60	1,46	1,73	1,30	1,25	1,17	1,17
Paraguay	2,13	2,28	1,24	0,72	0,75	1,07	0,95	0,89	0,93	0,99
Argentina	1,45	1,47	1,15	0,85	0,81	0,85	0,81	0,86	0,75	0,71
Venezuela	1,52	1,55	1,53	1,83	1,01	0,94	0,45	0,49	0,00	0,00

Source: World Development Indicators database (25/05/2021) *No data available on Suriname

However, if we look at regional defence spending in the first decade of the 21st century, several investment peaks can be observed in different countries, which have led analysts to interpret it as a South American arms race (VILLA and VIGGIANO, 2012).

On the one hand, historically, Ecuador and Peru were at war in 1995 and this explains their high spending. Colombia was experiencing an upsurge in fighting against the FARC-EP and other paramilitary groups, which culminated in the peace agreement in 2016. On the other hand, Paraguay, Uruguay, Bolivia, and Chile were not at war. The explanation is that these countries were going through processes of modernisation of their armed forces as equipment and weapons systems reached the end of their useful lives (PAREDE, 2020), and it was necessary to revitalise them to ensure an acceptable level of deterrence. In this case, it is important to note that "deterrent modernisation" must come along with transparent defence documents and agendas so as not to be interpreted as an acquisition of offensive military advantages aimed at a regional power imbalance. Therefore, looking at budgets alone does not tell us whether a country is preparing for war or just investing to maintain its deterrent

seja por limitações orçamentárias, seja por incompetência organizacional, é outro argumento para a paz regional. "A guerra requer competência organizacional básica e acesso a recursos que apenas alguns Estados possuem. Deste ponto de vista, a América Latina tem sido pacífica porque os Estados da região nunca desenvolveram a capacidade política de ter guerras prolongadas" (CENTENO, 2002, p. 91).

Guerras não precisam de competência organizacional, precisam de objetivos políticos claros, exércitos e vontade de lutar. A competência, a eficiência militar e os recursos colaboram para decidir os resultados do confronto, não o seu início. Toda a competência militar norte-americana ou soviética não os salvou de derrotas frente a exércitos menos organizados institucionalmente no Vietnã e no Afeganistão. Ou, ainda, observem-se as guerras entre Estados no continente africano, cujos exércitos não têm altos padrões de organização (WILLIAMS, 2017).

Do ponto de vista das limitações orçamentárias, nos últimos cinco anos, os gastos com defesa na América do Sul ficaram abaixo dos 2% do PIB. Exceção feita apenas à Colômbia e ao Equador que, nos últimos 5 anos, têm gastado, de forma consistente, mais de 2% do PIB em defesa.

Gastos militares em relação ao PIB (%)

País	1990	1995	2000	2005	2010	2015	2016	2017	2018	2019
Colômbia	1,86	2,83	3,03	3,35	3,63	3,11	3,07	3,21	3,07	3,15
Equador	1,89	2,34	1,45	2,30	3,01	2,62	2,51	2,36	2,35	2,29
Chile	3,40	2,56	2,70	2,52	2,24	1,90	1,92	1,93	1,86	1,82
Uruguai	3,53	2,71	2,44	2,00	1,88	1,82	1,87	1,96	2,13	2,02
Bolívia	2,82	2,10	2,06	1,77	1,67	1,74	1,63	1,54	1,54	1,42
Guiana	0,91	0,92	1,77	1,41	1,38	1,45	1,48	1,64	1,60	1,65
Brasil	2,36	1,86	1,73	1,52	1,54	1,37	1,35	1,42	1,51	1,48
Peru	2,68	2,64	1,79	1,60	1,46	1,73	1,30	1,25	1,17	1,17
Paraguai	2,13	2,28	1,24	0,72	0,75	1,07	0,95	0,89	0,93	0,99
Argentina	1,45	1,47	1,15	0,85	0,81	0,85	0,81	0,86	0,75	0,71
Venezuela	1,52	1,55	1,53	1,83	1,01	0,94	0,45	0,49	0,00	0,00

Fonte: World Development Indicators database (25/05/2021) *Não existem dados disponíveis do Suriname

Entretanto, se olharmos para os gastos regionais com defesa na primeira década do século XXI, podem ser observados vários picos de investimentos em diferentes países, o que levou analistas a interpretarem-nos como uma corrida armamentista sul-americana (VILLA e VIGGIANO, 2012).

Por um lado, historicamente, Equador e Peru estavam em Guerra em 1995 e isso explica seus gastos elevados. A Colômbia vivia o recrudescimento dos combates contra as FARC-EP e outros grupos paramilitares, que culminou com os acordos de paz em 2016. Entretanto, por outro lado, Paraguai, Uruguai, Bolívia e Chile não estavam em guerra. A explicação é que estes países atravessavam processos de modernização de suas forças armadas à medida que equipamentos e sistemas de armas chegavam ao final de suas

status. One needs to understand whether the country's posture is transparent and cooperative or competitive.

Defence cooperation has several nuances that can contribute to regional stability, but which are not captured as indicators in the bases that map international conflicts because they are in stages prior to the deterioration of relations between countries. Activities such as military diplomacy; exchange of officers in internships and courses; facing common threats, such as drug trafficking; bilateral agreements; combined exercises; joint participation in UN peacekeeping missions; creation of common response forces, such as the *Fuerza de Paz Cruz Del Sur* between Argentina and Chile; common projects in industrial defence bases; and, finally, the establishment of multilateral forums to discuss regional defence, such as the South American Defence Council (CDS/UNASUR), foster regional stability.

Of these initiatives, multilateral defence forums are the most complete and complex resources to be operationalised in a lasting way (LEITE, 2015). The creation of the South American Defence Council (2008), within UNASUR, took place at a time when the political situation allowed it, but changes in this same situation weakened the entity from 2018, when Colombia, Argentina, Brazil, Bolivia, Chile, Ecuador, Uruguay, Paraguay, and Peru announced their withdrawal from the organisation.

On the other hand, other defence cooperation initiatives continue to take place in areas less prone to the fluctuations of political circumstances. Joint military operations and exercises are a positive indicator of cooperation when carried out in neutral territories — far from areas of latent tension or borders with neighbouring countries not invited to participate. An example is the Combined Humanitarian Logistics Exercise AmazonLog17, held in 2017 on the triple border (Brazil-Colombia-Peru), with the participation of troops from the three countries and military observers from nineteen other countries (COLOG, 2018).

The exchange of officers between countries in the region is another indicator of cooperation that, according to Martins (2016), helps to create a "transnational identity" among the region's military, which facilitates contacts and the search for understanding in times of crisis, in addition to fostering the development of autochthonous views and solutions for the region. An example of this can be seen in the 653 officers from friendly nations, of which 360 were from South America, that graduated from the Brazilian Army Command and General Staff College (ECEME – acronym in Portuguese) between 1968 and 2017.

Measuring these interactions among South American armies is a valid indicator of what the relationships between the military of these countries are like, because the prolonged absence of exchanges can be a negative sign in the relations among countries.

vidas úteis (PAREDE, 2020), sendo necessário revitalizá-los para garantir um nível de dissuasão aceitável. Neste caso, é importante notar que uma "modernização dissuasiva" deve ser seguida de documentos e de agendas de defesa transparentes a fim de não ser interpretada como aquisição de vantagens militares ofensivas visando a um desequilíbrio de poder regional. Assim, olhar somente os orçamentos não nos indica se um país está se preparando para uma guerra ou apenas investindo para manter seu *status* dissuasório. É preciso entender se sua postura é transparente e cooperativa ou competitiva.

A cooperação na área de defesa tem várias nuances que podem colaborar para a estabilidade regional, mas que não são captadas como indicadores nas bases que mapeiam os conflitos internacionais por estarem em estágios anteriores à deterioração das relações entre os países. Atividades como diplomacia militar; troca de oficiais em estágios e cursos; enfrentamento de ameaças comuns, como o narcotráfico; acordos bilaterais; exercícios combinados; participação conjunta em missões de paz da UN; criação de forças de resposta comuns, como a *Fuerza de Paz Cruz Del Sur* entre Argentina e Chile; projetos comuns nas bases industriais de defesa e, por fim, o estabelecimento de foros multilaterais para discutir a defesa regional, como o Conselho de Defesa Sul-Americano (CDS/UNASUL) fomentam a estabilidade regional.

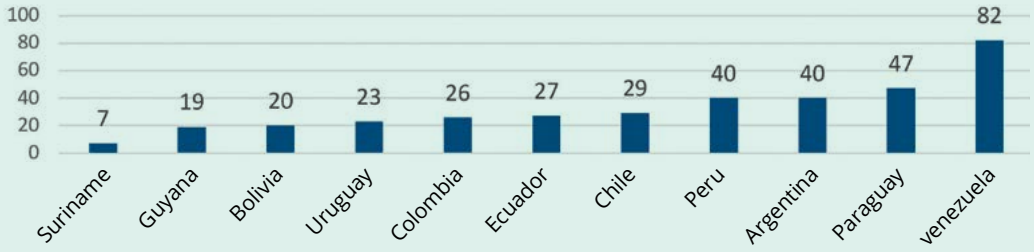
Destas iniciativas, os foros multilaterais de defesa são os recursos mais completos e complexos de serem operacionalizados de maneira durável (LEITE, 2015). A criação do Conselho de Defesa Sul-Americano (2008), dentro da UNASUL, ocorreu em um momento em que a conjuntura política a permitiu, mas as mudanças desta mesma conjuntura esvaziaram a entidade a partir de 2018, quando Colômbia, Argentina, Brasil, Bolívia, Chile, Equador, Uruguai, Paraguai e Peru anunciaram suas saídas do organismo.

Em contrapartida, outras iniciativas de cooperação em defesa seguem acontecendo em áreas menos propensas às flutuações das conjunturas políticas. Operações e exercícios militares conjuntos são um indicador positivo de cooperação quando realizados em territórios neutros – afastados de zonas de tensão latente ou de fronteiras com países vizinhos não convidados a participar. Um exemplo foi o Exercício Combinado de Logística Humanitária AmazonLog17, realizado em 2017 na tríplice fronteira (Brasil-Colômbia-Peru), com a participação de tropas dos três países e observadores militares de dezenove outros países (COLOG, 2018).

O intercâmbio de oficiais entre os países da região é um outro indicador de cooperação que, segundo Martins (2016), colabora para criar uma "identidade transnacional" entre os militares da região, o que facilita os contatos e a busca de entendimentos em momentos de crise, além de fomentar o desenvolvimento de olhares e soluções autóctones sobre a região. Um exemplo disto pode ser observado na Escola de Comando e Estado-Maior do Brasil (ECEME) onde, entre 1968 e 2017, formaram-se 653 oficiais de nações amigas, sendo que, destes, 360 eram oriundos da América do Sul.

Mensurar essas interações entre os exércitos sul-americanos é um indicador válido de como estão os relacionamentos entre os militares destes países porque a ausência prolongada de intercâmbios pode ser um sinal negativo nas relações entre os países.

Officers from South American friendly nations trained at ECEME



Source: Adapted from PAIM, 2019. p. 174

Considering what has been discussed here so far in theoretical terms, we can summarise some of the characteristics of conflicts in South America:

(i) they have **limited goals**, that is why the use of the armed forces is limited, aiming to obtain an advantageous position in the subsequent negotiation tables or to prevent it;

(ii) being limited, they are **brief and violent**, with a **low total number of victims and material loss**, but with the expectation of significant political gains;

(iii) **they occur in border regions** (land and sea), owing to historical disputes, to disputes related to natural resources or incidents involving the combat of regular troops against non-state actors;

(iv) diplomatic disputes go on for decades and there is a **refusal to accept the result of international mediations;** this non-acceptance of the *status quo* is a characteristic of disputes that can evolve into wars.

Throughout the 20th century, South American countries have used force as an option to achieve their political goals several times. In the 21st century, continuing tensions show that this option is not a closed-off path.

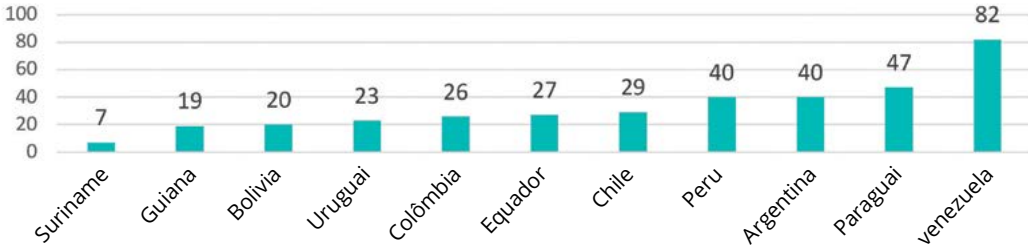
RECOMMENDATIONS FOR UNDERSTANDING WAR AND SEEKING PEACE

As we have tried to demonstrate, under the guise of South American peace, conflicts and unresolved issues lie dormant and linger on in diplomatic protests and periods of State violence. With this in mind, we list the following propositions:

(1) Fostering stable multilateral entities

Governments should seek to establish multilateral entities with a greater presence of career State personnel, such as diplomats, the military, academics, and other civil servants, who may be the key to building more stable entities less prone to the risk of extinction due to changes in the political situation. Otherwise, there is a risk that, with each change in the political situation, such entities will be weakened and new ones created in a cycle that will not allow real progress towards the construction of a common South American defence agenda.

Oficiais de Nações Amigas da América do Sul formados na ECEME



Fonte: Adaptado de PAIM, 2019. p. 174

Considerando o que já se desenhou teoricamente até aqui, podemos sintetizar algumas das características dos conflitos na América do Sul:

(i) têm o**bjetivos limitados**, por isso o emprego das Forças Armadas é limitado, visando a obter uma posição vantajosa nas mesas de negociações posteriores ou impedir isso;

(ii) sendo limitados, são **breves e violentos**, com um **baixo número total de vítimas e perda materiais**, mas com a expectativa de ganhos políticos significativos;

(iii) **ocorrem em regiões de fronteiras** (terrestres e marítimas), por disputas históricas, por disputas relacionadas a recursos naturais ou a incidentes envolvendo o combate de tropas regulares a atores não-estatais;

(iv) as disputas diplomáticas se prologam no tempo por décadas e existe a **recusa na aceitação do resultado de mediações internacionais;** essa não aceitação do *status quo* é uma característica das disputas que pode evoluir para guerras.

Durante o século XX, por diversas vezes, os países sul-americanos usaram a força como uma opção para atingirem seus objetivos políticos. No século XXI, a continuidade de tensões mostra que essa opção não é uma via extinta.

RECOMENDAÇÕES PARA ENTENDER A GUERRA E BUSCAR A PAZ

Como procuramos demonstrar, sob o manto da paz sul-americana, pulsam conflitos e questões ainda sem solução que se arrastam em contestações diplomáticas e momento de violência estatal. Neste sentido, elencamos as seguintes proposições:

(1) Fomentar entidades multilaterais estáveis

Os governos devem buscar estabelecer entidades multilaterais com uma maior presença de funcionários estatais de carreira, como: diplomatas, militares, acadêmicos e outros servidores afins, que podem ser a chave para construir entidades mais estáveis e menos propensas ao risco de extinção com mudanças na conjuntura política. Caso contrário, corre-se o risco de, à cada mudança na conjuntura política, as entidades serem esvaziadas e novas criadas em um ciclo que não permitirá avanços reais em prol da construção de uma agenda comum de defesa sul-americana.

(2) Monitoring of border tensions

Since most tensions are caused by border issues, monitoring diplomatic and military activities linked to national borders is essential to detect escalating tensions or preparations for a conflict. The countries in the region have limited strategic mobility, so any military action will be preceded by the concentration of shock troops in the region or on access roads, which can be easily detected. Additionally, since the use of violence is a path towards the negotiating table, diplomacy will play an active role in seeking international support and building a rationale for the escalation of the crisis into conflict.

(3) Encouraging regional research on war, peace, and the actors involved

Fostering South American associations and research programs aimed at studying war from autochthonous civilian and military perspectives, since these actors can think of and calibrate more solid regional indicators that point to the degree of cooperation or conflict thawing before they occur, rather than thinking of measuring them by the number of deaths or by their intensity after they have occurred.

(4) Developing regions in dispute in an integrated manner

Borders can also be the stage for solutions to prevent future conflicts. In the case of border regions involving disputes over natural resources, the promotion of public policies and projects that direct part of the *royalties* arising from the exploration of such resources for sustainable development initiatives on both sides of the border can collaborate to replace the feeling of "loss" with one of "partnership", providing strong foundations for the creation of stability.

To sum up, dialogue and the constant search for cooperation must be the path to be followed to maintain peace in South America. Discontent with the territorial *status quo* and resentment from previous territorial losses must be monitored and worked on in order to establish positive cooperation agendas.

Isolated nations cornered in their own regions by their own neighbours end up being driven to war. The maintenance of interstate peace is only possible with the constant interest and attention of nations to align their wills instead of putting them on collision courses.

(2) Monitoramento de tensões fronteiriças

Como a maior parte das tensões giram em torno de questões fronteiriças, monitorar atividades diplomáticas e militares ligadas às fronteiras nacionais é essencial para perceber escaladas de tensões ou de preparação para um conflito. Os países da região têm uma mobilidade estratégica limitada, por isso, qualquer ação militar vai ser precedida de concentração de forças de choque na região ou em vias de acesso, o que pode ser facilmente detectado. E, como o uso da violência é um caminho para a mesa de negociação, a diplomacia terá um papel ativo na busca de apoio internacional e construção de uma justificativa para a escalada da crise até o conflito.

(3) Incentivar pesquisas regionais sobre a guerra, a paz e seus atores

Fomentar associações e programas de pesquisa sul-americanos voltados a estudar a guerra a partir de olhares autóctones civis e militares, uma vez que esses atores podem pensar e calibrar indicadores regionais mais sólidos, que apontem para o grau de cooperação ou de descongelamento de conflitos antes que esses ocorram, ao invés de pensar em medi-los pelo número de mortos ou por sua intensidade depois que ocorreram.

(4) Desenvolver de forma integrada as regiões em litígio

As fronteiras também podem ser o palco de soluções para prevenir os conflitos futuros. No caso de regiões fronteiriças envolvendo disputas sobre recursos naturais, fomentar políticas públicas e projetos que direcionem parte dos *royalties* da exploração para iniciativas de desenvolvimento sustentáveis nos dois lados da fronteira pode colaborar para substituir a sensação de "perda" por outra de "parceria", criando uma estabilidade com bases sólidas.

Em síntese, na América do Sul, o caminho para a manutenção da paz deve ser o diálogo e a constante busca por cooperação. O descontentamento com o *status quo* territorial e os ressentimentos por perdas territoriais anteriores devem ser monitorados e trabalhados de forma a se estabelecerem agendas positivas de cooperação.

Nações isoladas e acuadas em suas próprias regiões por seus próprios vizinhos acabam conduzidas à guerra. A manutenção da paz interestatal só é possível com interesse e atenção constantes das nações para alinhar suas vontades ao invés de colocá-las em rotas de colisão.

REFERENCES

BARROSO, Mauro. **Cenepa, a última guerra sul-americana**. Rio de Janeiro: STAMPPA, 2007.

BATTAGLINO, Jorge M. Palabras mortales. Rearme y carrera armamentista en América del Sur. **Nueva Sociedad**. No. 15, pp. 23-34. 2008.

BUSTILLOS, Ramón Urbano, BRAVO, Kléver Antonio. ***Afectación a la soberanía, análisis comparativo: Angostura (2008) y San Lorenzo (2018), Ecuador.*** **Revista de Ciencias de Seguridad y Defensa.** Vol. IV, No. 4, 2019. pp.190-206

CENTENO, Miguel Angel. **Blood and debt: War and the nation-state in Latin America**. Penn State Press, 2002.

CLAUSEWITZ, Carl von. **Da Guerra**. São Paulo: Martins Fontes, 2010.

COLOG (Comando Logístico), **AMAZONLOG17 Relatório**. Brasília: Feb. 2018.

FRANCHI, Tássio; MIGON, Eduardo Xavier Ferreira Glaser; VILLARREAL, Roberto Xavier Jiménez. *Taxonomy of interstate conflicts: is South America a peaceful region?* **Brazilian Political Science Review**, v. 11, n. 2, 2017.

GHOSN, Faten; PALMER, Glenn; BREMER, Stuart A. The MID3 data set, 1993—2001*: Procedures, coding rules, and description*. **Conflict management and peace science**, v. 21, n. 2, p. 133-154, 2004.

GÓMEZ, Mariano Oscar; LUZURIAGA, Agustín. ***Malvinas, entre la niebla y la fricción***. **Military Review**. Segundo Trimestre. 2019. pp. 81-87.

HUTH, Paul K. **Standing your ground: Territorial disputes and international conflict**. University of Michigan Press, 2009.

KACOWICZ, Arie Marcelo. **Zones of peace in the Third World: South America and West Africa in comparative perspective.** SUNY Press, 1998.

LAURO, Adriano; CORRÊA, Claudio Rodrigues, HONÓRIO, Thiago Jacobino. *The potential impacts of COVID-19 pandemic on international defense and security.* **Revista da Escola de Guerra Naval.** Vol. 26, n. 3, 2020. pp. 579-608.

LEITE, Lucas Amaral Batista. *South America as security community: autonomous region and identity construction.* **Brazilian Journal of International Relations**, v. 4, n. 1, p. 92-110, 2015.

MARTÍN, Félix. **Militarist peace in South America: conditions for war and peace**. Springer, 2006.

NETO, Tomaz Espósito. **Itaipu e as Relações Brasileiro-Paraguaias de 1962 a 1979: Fronteira, Energia e Poder**. Editora Appris, 2021.

PAIM, Rodrigo de Almeida. ***A Diplomacia (Militar) nas Relações Internacionais.*** **Revista Brasileira de Estudos Estratégicos,** Rio de Janeiro. v. 10, n. 19, 2019. pp.157-178.

PETTERSSON, Thérèse; WALLENSTEEN, Peter. *Armed conflicts, 1946–2014*. **Journal of Peace Research**, v. 52, n. 4, p. 536-550, 2015.

SARKEES, Meredith Reid; WAYMAN, Frank. **Resort to war: 1816-2007. Correlates of War**. Washington DC: CQ Press. 2010.

REFERÊNCIAS

BARROSO, Mauro. **Cenepa, a última guerra sul-americana.** Rio de Janeiro: STAMPPA, 2007.

BATTAGLINO, Jorge M. Palabras mortales. Rearme y carrera armamentista en América del Sur. **Nueva Sociedad**. Nº 15, pp. 23-34. 2008.

BUSTILLOS, Ramón Urbano, BRAVO, Kléver Antonio. *Afectación a la soberanía, análisis comparativo: Angostura (2008) y San Lorenzo (2018), Ecuado*r. **Revista de Ciencias de Seguridad y Defensa**. Vol. IV, No. 4, 2019. pp.190-206

CENTENO, Miguel Angel. **Blood and debt: War and the nation-state in Latin America**. Penn State Press, 2002.

CLAUSEWITZ, Carl von. **Da Guerra**. São Paulo: Martins Fontes, 2010.

COLOG (Comando Logístico), **AMAZONLOG17 Relatóri**o. Brasília: fev. 2018.

FRANCHI, Tássio; MIGON, Eduardo Xavier Ferreira Glaser; VILLARREAL, Roberto Xavier Jiménez. *Taxonomy of interstate conflicts: is South America a peaceful region?* **Brazilian Political Science Review**, v. 11, n. 2, 2017.

GHOSN, Faten; PALMER, Glenn; BREMER, Stuart A. The MID3 data set, 1993—2001: *Procedures, coding rules, and description*. **Conflict management and peace science**, v. 21, n. 2, p. 133-154, 2004.

GÓMEZ, Mariano Oscar; LUZURIAGA, Agustín. *Malvinas, entre la niebla y la fricción*. **Military Review**. Segundo Trimestre. 2019. pp. 81-87.

HUTH, Paul K. **Standing your ground: Territorial disputes and international conflict**. University of Michigan Press, 2009.

KACOWICZ, Arie Marcelo. **Zones of peace in the Third World: South America and West Africa in comparative perspective**. SUNY Press, 1998.

LAURO, Adriano; CORRÊA, Claudio Rodrigues, HONÓRIO, Thiago Jacobino. *The potential impacts of COVID-19 pandemic on international defense and security*. **Revista da Escola de Guerra Naval**. Vol. 26, n. 3, 2020. pp. 579-608.

LEITE, Lucas Amaral Batista. *South America as security community: autonomous region and identity construction*. **Brazilian Journal of International Relations**, v. 4, n. 1, p. 92-110, 2015.

MARTÍN, Félix. **Militarist peace in South America: conditions for war and peace**. Springer, 2006.

NETO, Tomaz Espósito. **Itaipu e as Relações Brasileiro-Paraguaias de 1962 a 1979: Fronteira, Energia e Poder**. Editora Appris, 2021.

PAIM, Rodrigo de Almeida. *A Diplomacia (Militar) nas Relações Internacionais*. **Revista Brasileira de Estudos Estratégicos**, Rio de Janeiro. v. 10, n. 19, 2019. pp.157-178.

PETTERSSON, Thérèse; WALLENSTEEN, Peter. *Armed conflicts, 1946–2014*. **Journal of Peace Research,** v. 52, n. 4, p. 536-550, 2015.

SARKEES, Meredith Reid; WAYMAN, Frank. **Resort to war: 1816-2007. Correlates of War**. Washington DC: CQ Press. 2010.

PEDROSA, Fernando Gomes VELÔZO*. O Chile e as Demandas de Modernização do Exército Durante a Transição Democrática.* **Coleção Meira Mattos: revista das ciências militares**, v. 14, n. 49, p. 99-122, 21 Jan. 2020.

VILLA, Rafael Duarte; VIGGIANO, Juliana. *Trends in South American weapons purchases at the beginning of the new millennium.* **Revista Brasileira de Política Internacional**, v. 55, n. 2, p. 28-47, 2012.

WANCKE, Stella (Org). **Conflict barometer 2014***:* disputes, non-violent crises, violent crises, limited wars and wars. Heidelberg: HIIK 2015. 178 pp.

WILLIAMS, Paul D. *Continuity and change in war and conflict in Africa*. **Prism**, v. 6, n. 4, p. 32-45, 2017.

YNFANTE, Jesús E. Caldera. *El Esequibo es venezolano: El litigio estratégico de Venezuela contra Guyana en la Corte Internacional de Justicia*. **Opción: Revista de Ciencias Humanas y Sociales**, n. 93, p. 389-443, 2020.

PEDROSA, Fernando Gomes Velôzo. ***O Chile e as Demandas de Modernização do Exército Durante a Transição Democrática***. **Coleção Meira Mattos: revista das ciências militares**, v. 14, n. 49, p. 99-122, 21 jan. 2020.

VILLA, Rafael Duarte; VIGGIANO, Juliana. ***Trends in South American weapons purchases at the beginning of the new millennium***. **Revista Brasileira de Política Internacional**, v. 55, n. 2, p. 28-47, 2012.

WANCKE, Stella (Org). **Conflict barometer 2014**: disputes, non-violent crises, violent crises, limited wars and wars. Heidelberg: HIIK 2015. 178 pp.

WILLIAMS, Paul D. ***Continuity and change in war and conflict in Africa***. **Prism**, v. 6, n. 4, p. 32-45, 2017.

YNFANTE, Jesús E. Caldera. ***El Esequibo es venezolano: El litigio estratégico de Venezuela contra Guyana en la Corte Internacional de Justicia***. **Opción: Revista de Ciencias Humanas y Sociales**, n. 93, p. 389-443, 2020.

Ines Correa Gomes Cardinot

Mestranda em Ciências Aeroespaciais pelo (PPGCA) da Universidade da Força Aérea (UNIFA), Pesquisadora do Pró – Defesa IV - Rede CTID: Defesa Cibernética. Pesquisadora do Laboratório de Simulações e Cenários (LSC) na Escola de Guerra Naval (EGN). E-mail: inescgcardinot@gmail.com

Master's degree student in Aerospace Science under the Aerospace Science Graduate Programme (PPGCA) of the Air Force University (UNIFA), Researcher in the Pro - Defence IV - Defence Industry Technical Committee - CTID Network: Cyber Defence. Researcher at the Simulations and Scenarios Laboratory (LSC) at the Naval Warfare Academy (EGN). Email: inescgcardinot@gmail.com

Edival Dan Junior

Doutorando em Engenharia de Produção pela Universidade Federal do Rio de Janeiro (UFRJ). Gerente Setorial de Conteúdo Local na Petrobras - Petróleo Brasileiro S.A. E-mail: edivaldan@yahoo.com.br

PhD student in Production Engineering at the Federal University of Rio de Janeiro, UFRJ. Sector Manager for Local Content at Petrobras - Petróleo Brasileiro SA E-mail: edivaldan@yahoo.com.br

Crise na crise: Impacto nas infraestruturas críticas informacionais da administração pública em tempos de pandemia

A crisis within a crisis: impact on critical public administration information infrastructure during the pandemic

Ines Correa Gomes Cardinot
Edival Dan Junior

RESUMO:

Diante do alastro da covid-19, a migração dos empregados de atividades administrativas para o ambiente online se tornou uma necessidade, traduzida em acessos remotos em massa. Nem todas as empresas estavam preparadas para esse fenômeno, que gerou acessos a informações sensíveis sem qualquer segurança informacional aplicada. Desta forma, o presente artigo tem como objetivo investigar o impacto da migração do trabalho para a modalidade remota nos órgãos públicos da administração brasileira, o que se justifica pela fragilidade da segurança cibernética da administração pública brasileira após sofrer uma sequência de ataques cibernéticos no ano de 2020. Busca apresentar também as iniciativas para o combate aos crimes cibernéticos no mundo, analisando de forma qualitativa os impactos e medidas que foram implementados no Brasil.

Palavras-Chave:

Pandemia, Administração Pública, Segurança Cibernética, Infraestruturas críticas informacionais.

ABSTRACT:

Given the spread of COVID-19, it became essential for employees in office positions to migrate to working from home. This translated into a massive adoption of remote access. Not all companies were prepared to deal with this circumstance, which resulted in facilitating access to sensitive information without the implementation of any information security policy. This article aims at investigating the impacts of work migrating to the online mode in Brazilian government bodies, driven by the vulnerability of the Brazilian public administration's cyber security as revealed by a series of cyberattacks in 2020. It also seeks to present existing initiatives to fight cybercrime in the world and offers a qualitative analysis of their impacts and the measures implemented in Brazil.

Key words:

Pandemic, Public Administration, Cyber Security, Critical Information Infrastructure.

INTRODUCTION

Due to the pandemic generated by the spread of the Sars-CoV-2 virus, which causes Covid-19, sanitary measures had to be adopted to flatten the expected short-term contagion curve. Among these were social distancing and lockdown measures. Municipal decrees were issued banning commerce and companies from operating in presential formats. Both government and private companies were unexpectedly forced to adopt the practice of home office without having the time to devise rules, organise training, adapting or preparing change management for their employees, therefore not guaranteeing the soundness of their operations, as pointed out by Souza (2020).

As work migrated during the health crisis, massive cyberattacks were perpetrated on various institutions around the world, while companies tried to empirically organise employee access to corporate networks from home computers, according to Santos (2020). Cyberattacks were highly damaging on Brazilian public bodies, which host sensitive information directly affecting the operation of critical infrastructures nationwide, as stated by Figueiredo and Fiatkoski (2020).

This article carries out a qualitative methodological analysis of the 2020 cyberattacks and presents a review of the literature seeking to investigate whether cyber security vulnerability in government agencies at the time of the massive transition to the home office was the main driver for cyberattacks.

Context

Since the World Health Organization (WHO) declared Covid-19 a pandemic on March 11, 2020, the number of deaths has grown exponentially worldwide and authorities the world over have focused their efforts on implementing strict emergency measures to attempt to contain the spread of the virus, as pointed out by Satter *et al.* 2020. At that time, a scenario of chaos came about and opened the way for cyber criminals, whose attacks soared both in Brazil and around the world.

According to Alcântara and Vilar-Lopes (2020), during the quarantine, which led to more people going online and a massive use of the home office, there was an increase in data traffic with the result that access data were stolen through phishing and malware attacks, and numerous cyberattacks happened around the world.

Theoretical basis

The theoretical basis for this article has been obtained mostly from *Segurança e Defesa do Espaço Cibernético Brasileiro*[1] (2010), a published paper by Raphael Mandarino Junior that is his monograph, written under the Information and Communication Security Management Specialisation Programme. University of Brasília - UnB/Department of Computer Science - DCE: Brasília.

[1] Security and Defence of the Brazilian Cyberspace. (Translator's note,)

INTRODUÇÃO

Em virtude da pandemia gerada pelo alastramento do vírus Sars-CoV-2, causador da covid-19, medidas sanitárias precisaram ser adotadas, visando a redução da curva de contágio prevista em curto prazo, como o isolamento e o *lockdown*, com decretos municipais impedindo comércio e empresas de atuarem presencialmente. Empresas públicas e de capital privado precisaram migrar seus serviços do escritório para a modalidade *home office* de forma abrupta, sem quaisquer regras, treinamento, tempo de adaptação ou gestão da mudança para os empregados, não dando oportunidade para a garantia do bom andamento das operações, conforme apontado por Souza (2020)

Durante essa migração, em meio ao caos sanitário, ataques cibernéticos em massa foram sofridos por diferentes instituições ao redor do mundo, ao mesmo tempo que as empresas tentavam organizar, de forma empírica, o acesso dos empregados às redes corporativas com a utilização de redes domésticas, segundo Santos (2020). Ataques cibernéticos foram contundentes contra órgãos públicos brasileiros, detentores de informações sensíveis e que tinham relação direta com o funcionamento de infraestruturas críticas do país, conforme citado por Figueiredo e Fiatkoski (2020).

Voltado a uma análise metodológica qualitativa dos ataques cibernéticos sofridos em 2020, o presente artigo apresenta uma revisão bibliográfica, buscando investigar se a fragilidade da segurança cibernética dos órgãos governamentais no momento de transição em massa para o ambiente online doméstico foi o principal motivador para os ataques cibernéticos.

Contextualização

No momento da declaração da Organização Mundial de Saúde (OMS), em 11 de março de 2020, da existência da pandemia, no mundo todo se via um aumento exponencial do número de mortos, de tal forma que as autoridades internacionais redirecionaram seus esforços para ações rígidas e emergenciais na tentativa de conter a propagação do vírus, conforme apontado por Satter *et al.* (2020). Configura-se, naquele momento, um cenário de caos, propício para investidas de criminosos cibernéticos, cujos ataques aumentaram no Brasil e no mundo.

De acordo com Alcântara e Vilar-Lopes (2020), com o aumento do tráfego de dados durante a quarentena, que resultou em mais pessoas conectadas e da utilização em massa do *home office*, acessos foram roubados pela prática de *Phishing* (do inglês, pescagem) e ataques de *software* malicioso (*malware*) que resultaram em inúmeros ataques cibernéticos ao redor do mundo.

Fundamentação teórica

Para esse artigo, a fundamentação teórica foi baseada, em sua maioria, na obra publicada de Segurança e Defesa do Espaço Cibernético Brasileiro (2010), de Raphael Mandarino Junior, resultado de sua monografia aprovada no Curso de Especialização em Gestão da Segurança da Informação e Comunicações. Universidade de Brasília - UnB/ Departamento de Ciência da Computação - DCE: Brasília.

Cyber Security refers to the protection and guarantee of the use of strategic information assets, especially those in connection with critical information infrastructures (communication and computer networks and their IT systems), which control national critical infrastructures. It also includes the interaction with government and private bodies involved in the operation of national critical infrastructures, especially Federal Public Administration agencies (FPA) (p 18).

It is not the same as Cyber Defence, which refers to a set of defensive, exploratory and offensive actions in the context of military planning and is carried out in cyber space, aiming at protecting information systems, obtaining data for the production of intelligence and damaging the opponent's information systems (p 18).

It is also worth defining the concept of Information and Communication Security, which is a set of actions aiming at enabling and ensuring availability, integrity, reliability and authenticity of information (p 18).

Critical Infrastructure (CI) includes facilities, services, goods and systems that, if interrupted or destroyed, will cause serious social, economic, political, international damage or impact the security of the State and society (p.18).

For the theoretical basis of the terms in English, several authors have been used as reference.

According to Moraes (2018), phishing is a random attack technique in which emails are sent to the victim, containing various types of information, such as bank payment slips, product ads, false traffic tickets, false court cases, i.e., various methods seeking to entice curiosity or fear on the victim or simply to look trustworthy, so that the victim clicks on a link, causing a malware to be installed in the system, opening the way for other attacks. Clicking on the link causes the system to be redirected to fake sites, usually of well reputed established stores, so that the victim feels comfortable (p. 22).

Ransomware is malicious software that infects a computer and can block access to the system through encryption, and the victim is subjected to extortion, usually charged in cryptocurrencies, digital money, to regain access (NEVES, 2008).

As per Candido et al. (2018), malware is the combination of the English words malicious and software, i.e., malicious software. The software and its commands are made for various purposes: just infiltrating a computer or system, causing damage and deleting data, stealing information, publicizing services, etc.

Segurança Cibernética se refere à proteção e garantia de utilização de ativos de informação estratégicos, principalmente os ligados às infraestruturas críticas da informação (redes de comunicação e de computadores e seus sistemas informatizados) que controlam as infraestruturas críticas nacionais. Também abrange a interação com órgãos públicos e privados envolvidos no funcionamento das infraestruturas críticas nacionais, especialmente os órgãos da Administração Pública Federal (APF) (p. 18).

Difere de Defesa Cibernética, que se refere a um conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com a finalidade de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente (p. 18).

É importante pontuar também o conceito de Segurança da Informação e Comunicações, que é definido como o conjunto de ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações (p. 18).

Infraestruturas Críticas (IC), por sua vez, são as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade (p.18).

Para fundamentação teórica de termos em inglês, utilizam-se autores diversos.

De acordo com Moraes (2018), *phishing* é uma técnica de ataques aleatórios no qual e-mails são enviados à vítima, contendo vários tipos de informações, como boletos, anúncio de produto, multa de trânsito falsa, processo judicial falso, ou seja, vários métodos que buscam fazer com que a vítima, pela curiosidade, medo ou simplesmente confiança, clique em determinado link e, assim, instale algum tipo de software malicioso em sem sistema, abrindo portas para outros ataques. Esses links podem redirecionar a sites falsos que, na maioria das vezes, são de lojas consagradas e consolidadas, para que a vítima se sinta confortável (p. 22).

Ransomware é um software malicioso que infecta o computador, podendo restringir seu acesso ao sistema com o uso da criptografia, por meio da qual é feita uma extorsão que é cobrada, na maioria das vezes, em criptomoedas, "dinheiro digital", para que o acesso seja restabelecido (NEVES, 2008).

Para Candido et al. (2018), *malware* é a combinação das palavras inglesas *malicious* e *software*, ou seja, programas maliciosos. São programas e comandos feitos para diferentes propósitos: apenas infiltrar um computador ou sistema, causar danos e apagar dados, roubar informações, divulgar serviços etc.

Cyberattacks in the world in 2020

In the same month that the WHO declared the COVID-19 a pandemic, companies around the world were targeted by various types of ransomware attacks. Some examples were the American biotechnology company 10x Genomics, the University Hospital Brno, in the Czech Republic, the Hammersmith Medicines Research (HMR), in England, and the WHO itself. The cyberattacks varied from denial of service to malware encrypting files for data ransom, as pointed out by Gallagher apud Alcântara and Vilar-Lopes (2020).

Cyberattacks in Brazil in 2020

Brazil has also been the target of cyberattacks. According to Souza on the Canaltech website, Brazil recorded over 8.4 billion cyberattack attempts in 2020 alone.

In November of the same year, amidst the other cases mentioned, the most alarming moment for Brazil was most likely when government bodies were targeted by massive cyberattacks. Several services were interrupted and critical public records for the operation of public services to the population were put at risk. Editora JP. Filho (2021) highlights, *inter alia*, the following examples:

- **Superior Court of Justice** – The Superior Court of Justice's (STJ – acronym in Portuguese) files were encrypted, which blocked employees from accessing data, including the email accounts of the Court Justices. Backups were also encrypted. 12 thousand court cases. Hackers managed not only to paralyse all activities in the Supreme Court for 6 days, but also blocked telephone and internet connections as well as access to emails;

- **Ministry of Health** – A hacker attack exposed data of 243 million citizens registered in the Brazilian Universal Health System (SUS – acronym in Portuguese), as well as authorities' data, including the president of Brazil, Jair Bolsonaro, of the then speaker of the House of Representatives, Rodrigo Maia, and of Senator Davi Alcolumbre.

- **Secretary of State Office for the Capital, Brasilia** – This attack resulted in all servers being shut down. Blocked phone lines, disconnected servers, and difficulty in accessing documents and e-mails. Public officials were left without access to the internet and to the system files and were unable to perform their activities.

Analysis of the highest profile cyberattack in Brazil - Superior Court of Justice

One of the most common malwares is the so-called "backdoor trojan", which gives malicious users remote access to computers, allowing hackers to execute commands and gain access to user information. The DoublePulsar Backdoor was responsible for the Shadow Brokers leaks in March 2017, and was also used in the WannaCry attack in May 2017.

Ataques cibernéticos no mundo em 2020

No mesmo mês em que a OMS declarou a existência da pandemia, empresas em todo mundo sofreram ataques de diferentes *ransomwares*, como a empresa americana de biotecnologia *10x Genomics*, o Hospital Universitário de *Brno*, na República Tcheca, o centro de pesquisas *Hammersmith Medicines Research* (HMR) na Inglaterra e até mesmo a OMS, que sofreram desde ataques de negação de serviço a *malware* capaz de criptografar arquivos para cobrança de resgate pelos dados, conforme apontado por Gallagher *apud* Alcântara e Vilar-Lopes (2020).

Ataques cibernéticos no Brasil em 2020

O Brasil também tem sido alvo de ataques cibernéticos. De acordo com Souza, no site Canaltech, o país sofreu mais de 8,4 bilhões de tentativas de ataques cibernéticos apenas no ano de 2020.

Em novembro do mesmo ano, a despeito dos demais casos citados, o momento mais alarmante para o Brasil talvez tenha sido o ataque em massa aos órgãos públicos, que resultou na suspensão de diversos serviços e colocou em risco os registros únicos, fundamentais para o andamento das prestações de serviço à população. Dentre os ataques, a Editora JP. Filho (2021) destaca:

- **Superior Tribunal de Justiça** – Os arquivos da instituição foram criptografados, impedindo o acesso dos funcionários aos dados do Tribunal, inclusive às contas de e-mail dos Ministros da Corte. Os backups também foram criptografados. 12 mil processos. Os hackers não só paralisaram as atividades do STF por 6 dias como também bloquearam as conexões telefônicas, de internet e os acessos a e-mails;

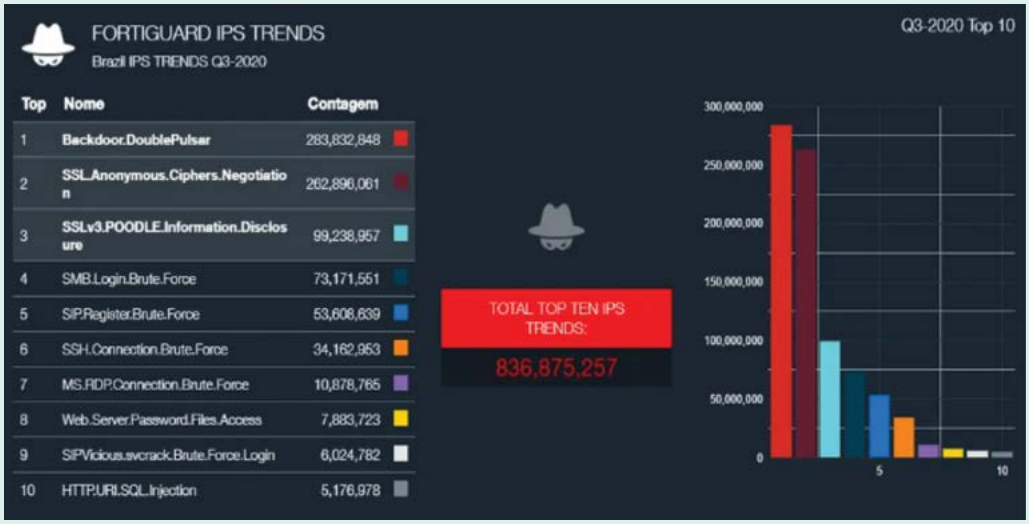
- **Ministério da Saúde** – Ataque *hacker* expôs dados de 243 milhões de cidadãos cadastrados no SUS, além de dados de autoridades, incluindo dados do presidente do Brasil, Jair Bolsonaro, do então presidente da Câmara dos Deputados, Rodrigo Maia, e os do Senador Davi Alcolumbre.

- **Secretaria de Governo do DF** – Ameaça de ataque resultou na retirada do ar de todos os servidores. Linhas telefônicas bloqueadas, servidores desligados e dificuldade de acesso a documentos e caixa de e-mails. Assim, os servidores ficaram sem acesso à internet e aos arquivos do sistema, sendo impossibilitados de realizar suas atividades.

Análise do ataque de maior repercussão no Brasil - STJ

Um dos tipos de *malware* mais comuns são os chamados "cavalos de tróia *backdoor*", que são responsáveis por dar acesso aos computadores remotamente, o que permite que os *hackers* executem comandos e tenham acesso a informações do usuário. O DoublePulsar Backdoor foi responsável pelos vazamentos do Shadow Brokers em março de 2017 e também foi utilizado no ataque à WannaCry, em maio de 2017.

Figure 1 - Fortiguard IPS Trends



Source: Copy/Fortinet (2020).

This ransomware is used in attacks that demand ransom in exchange for a key to recover encrypted data, as disclosed by @mindsec on the *Minuto da Segurança* website (2020), the same one used in the cyberattack on the STJ.

The attack on the STJ stands out. The court technicians described it:

> It was basically a ransomware attack. A Domain Admin account was exploited, which allowed the hacker to gain access to our servers, join virtual environment administration groups, and finally encrypt most of our virtual machines. (ESCOSTEGUY, 2020)

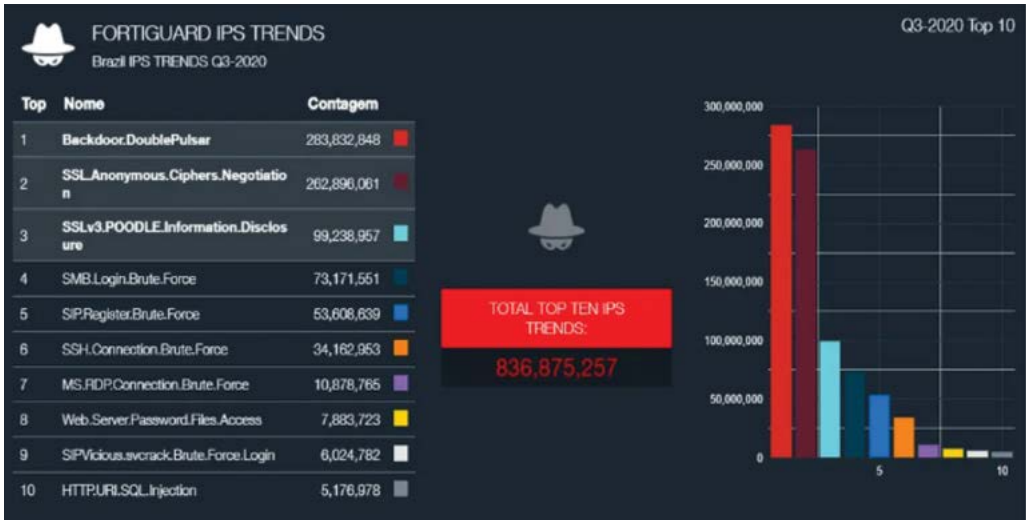
Access to the internet from home networks when individuals are working from home ends up mingling personal daily use information with corporate information leading to increased risks to the victims' hardware, which becomes a gateway for hackers to invade computers and get to the points of attack.

Actions taken in Brazil

The cyberattacks perpetrated on government institutions prompted new negotiations for information security at the Federal Administration level, notably to the publication of a government regulation that was already under review for approval by the National Congress, LAW No. 13.709/18 General Personal Data Protection Act (LGPD - acronym in Portuguese). The law aims at standardising personal data processing, including digital media, by individuals and companies, in order to protect basic freedom and privacy rights.

The LGPD was inspired by the General Data Protection Regulation 2016/679, the European law on privacy and personal data protection, that highlights careful treatment of personal data outside the European Union and the European Economic Area.

Figura 1 - Fortiguard IPS Trends



Fonte: Reprodução/Fortinet (2020).

Esse *ransomware* é utilizado em um tipo de ataque que pede resgate em troca da chave para recuperação dos dados criptografados, segundo divulgado por @mindsec no sítio Minuto da Segurança (2020), o mesmo utilizado no ataque cibernético do STJ.

Destaca-se o ataque ao STJ, cujos técnicos descreveram como:

> basicamente foi um ataque do tipo ransomware. Uma conta Domain Admin foi explorada, o que permitiu que o hacker tivesse acesso aos nossos servidores, se inserisse em grupos de administração do ambiente virtual e, por fim, criptografasse boa parte das nossas máquinas virtuais. (ESCOSTEGUY, 2020)

Acessos feitos em redes domésticas na modalidade *home office*, que divide informações pessoais de uso diário com as corporativas, gera maiores riscos às máquinas das vítimas, que se tornam um canal de invasão dos *hackers* para chegar aos pontos de ataques.

Ações adotadas no Brasil

Os ataques sofridos pelas instituições públicas impulsionaram novas tratativas para a segurança da informação, em nível Federal, destacadamente pela publicação da política pública que já estava em curso de aprovação no Congresso Nacional, como a LEI Nº 13.709/18 Lei Geral de Proteção de Dados Pessoais (LGPD), que visa normatizar o tratamento de dados pessoais, inclusive em meios digitais, por pessoas físicas e jurídicas, com o objetivo de proteger os direitos fundamentais da liberdade e da privacidade.

A LGPD foi inspirada no Regulamento Geral sobre a Proteção de Dados 2016/679, regulamento do direito europeu sobre privacidade e proteção de dados pessoais, destacando os cuidados no tratamento de dados pessoais para fora da União Europeia e do Espaço Econômico Europeu.

Due to the attacks in Brazil, the Federal Government identified the need to improve controls and increase investments in cyber defence. Progress towards the publication of Decree No. 10.222/20 National Cyber Security Strategy (E-Ciber – acronym in Portuguese) is also worth highlighting. It aims at putting the following strategic actions into practice:

1. Strengthening cyber governance actions
2. Establishing a centralised governance model at the national level
3. Fostering a participatory, collaborative, trustworthy and safe environment between the public sector, the private sector and society
4. Raising the level of government protection
5. Raising the level of protection of National Critical Infrastructures
6. Enhancing the legal framework on cyber security
7. Encouraging the creation of innovative cyber security solutions
8. Expanding Brazil's international cooperation in cyber security
9. Strengthening partnerships in cyber security, between the public sector, the private sector, academia and society
10. Raising society's maturity level in cyber security

The publication or review of other standards and guidelines was moved forward due to the new scenario that developed in 2020. One of them was the review of the National Cyber Security Policy and the creation of a Cyber Incident Management System.

Analysis result

Given all the elements introduced in this article, it becomes clear that companies and government institutions have sought to mitigate the impacts of the pandemic on their activities. The sudden need for massive access to corporate networks from personal computers did not prioritise critical issues such as information and communication security as there was no time to deal with the problem to the degree that was required.

It is true that some organisations had been testing home office practices before, but not to the extent seen in 2020. This resulted in access to newly adapted corporate networks by private accounts, without additional layers of cyber security and separation of environments in personal computers.

Therefore, this article suggests, based on the developments described above, that the lack of trained personnel and the lack of security in remote access computers can be considered two of the main causes driving cyberattacks, as the way individuals use their personal computers, which became hybrid environments in 2020, a fact that has been widely reported in global media, opens the way for hackers and other intruders to access personal data, making it possible for massive criminal attacks to succeed.

Devido aos ataques sofridos, o Governo Federal identificou a necessidade de aprimorar os controles e investimentos na defesa cibernética. Ressalta-se também os avanços para publicação do Decreto Nº 10.222/20 Estratégia Nacional de Segurança Cibernética (E-Ciber), que tem como objetivo colocar em prática as seguintes ações estratégicas:

1. Fortalecer as ações de governança cibernética
2. Estabelecer um modelo centralizado de governança no âmbito nacional
3. Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade
4. Elevar o nível de proteção do Governo
5. Elevar o nível de proteção das Infraestruturas Críticas Nacionais
6. Aprimorar o arcabouço legal sobre segurança cibernética
7. Incentivar a concepção de soluções inovadoras em segurança cibernética
8. Ampliar a cooperação internacional do Brasil em segurança cibernética
9. Ampliar a parceria em segurança cibernética, entre setor público, setor privado, academia e sociedade
10. Elevar o nível de maturidade da sociedade em segurança cibernética

Entre outras normas e diretrizes que tiveram sua publicação ou revisão antecipada diante do novo cenário desenhado no ano de 2020, tal como a revisão da Política Nacional de Segurança Cibernética e criação de um Sistema de Gestão de Incidentes Cibernéticos.

Resultado da análise

Perante tudo que foi exposto neste artigo, compreende-se que, diante do cenário de pandemia, as empresas e instituições buscaram mitigar os impactos em suas atividades. Dessa forma, a necessidade abrupta de acesso em massa às redes corporativas através de acessos domésticos deixou em segundo plano assuntos fundamentais como a segurança da informação e comunicação, que não tiveram tempo hábil para serem tratados na proporção demandada.

É verdade que já havia instituições testando os chamados *home offices*, mas não na escala realizada em 2020, que resultou em acessos a redes corporativas recém adaptadas por meio de contas particulares, sem adição de camadas extras de segurança cibernética e distinção dos ambientes em seus terminais.

Portanto, esse artigo aponta, perante tudo que foi anteriormente explanado, que a falta de treinamento de pessoal e a falta de segurança dos acessos remotos podem ser considerados como dois dos principais causadores e motivadores dos ataques cibernéticos, uma vez que a forma como as pessoas tratam terminais particulares — que, em 2020, se tornaram ambientes híbridos, o que foi noticiado em nível internacional — facilita o acesso de invasores *hackers* aos seus dados pessoais, dando oportunidade para que grandes investidas criminosas tenham sucesso.

CONCLUSION

In 2020, the pandemic led to an accelerated massive migration of employees from various organisations to working from home, which also meant massive access to corporate networks via home computers. This phenomenon "opened the doors" to the sensitive information of organisations to cybercrime.

With regard to the attacks targeting Brazilian public administration bodies, the case of the STJ stands out. It was widely reported on national and international media covering the investigation of the warning given by the court's IT team, according to which the invasion of the system was originated by an administrator account at a time when all employees were working from home, causing over one week of shutdown, according to an official statement issued by the STJ.

Cyberattacks on hospitals, research centres, laboratories and on a variety of institutions may cause severe impacts both on health and on the search for solutions to the pandemic, as well as on a wide range of services required by society as a whole.

Therefore, it can be concluded that, in addition to efforts to contain the spread of the pandemic, governments and companies must not neglect cyber security measures, as efforts may produce no effect, causing the loss of many lives, and largely postponing, or even rendering the solutions to contain the virus unworkable, in addition to causing billions in losses to the State.

Thus, it is essential to increase investments in information security of public bodies by hiring technical expertise and possibly by centralizing security and monitoring institutions. The information presented indicates firmly that, in addition to the health struggle against the coronavirus (Sars-CoV-2), it is critical to confront another challenge: the cybernetic one.

CONCLUSÃO

Em 2020, a pandemia resultou na migração acelerada e em massa de empregados das mais diferentes instituições para a realização de atividades via *home office*, refletindo no acesso, também em massa, às redes corporativas via terminais domésticos. Tal fenômeno "abriu as portas" para o acesso às informações sensíveis das instituições aos crimes cibernéticos.

Com ênfase nos ataques sofridos pelos órgãos da administração pública brasileira, destaca-se o caso do STJ, que foi amplamente noticiado em redes nacionais e internacionais, pela investigação do alerta dado pela equipe de TI da corte, que mencionou que a invasão ao sistema foi originada por uma conta de administrador em momento em que todos os funcionários trabalhavam de suas casas, gerando mais de uma semana de paralisação das atividades, segundo nota oficial do STJ.

Nesse sentido, os ataques cibernéticos a hospitais, centros de pesquisa, laboratórios e às mais diversas instituições podem gerar impactos catastróficos tanto na saúde e na busca de soluções para a pandemia, como para os mais diversos serviços necessários para toda a sociedade.

Conclui-se então que, além dos esforços para conter a pandemia, os governos e as empresas não podem se descuidar das iniciativas de segurança cibernéticas, pois, caso contrário, os esforços podem se tornar inócuos, causando a perda de muitas vidas e postergando sobremaneira, ou até inviabilizando, a solução para conter o vírus, além de gerar prejuízos bilionários aos cofres públicos.

Faz-se essencial, assim, o aumento de investimentos em segurança da informação junto aos órgãos públicos, com a contratação de técnicos e possivelmente com a centralização de segurança e monitoramento das instituições. Tais informações revelam que, paralelamente à luta travada pela saúde contra o coronavírus (Sars-CoV-2), há também a necessidade de posicionar-se frente a outro desafio: o cibernético.

BIBLIOGRAPHY

ALCÂNTARA, André, VILAR-LOPES, Gills. Overview dos casos de ataques cibernéticos durante a pandemia de COVID-19. RedeCTIDC. 2020. Available at: https://redectidc.com.br/rede-ctidc-covid-19-overview-dos-casos-de-ataques-ciberneticos-durante-a-pandemia.html Accessed on: Jun 05, 2021.

ALECRIM, Emerson. Ministério da Saúde expõe dados de 243 milhões de pessoas. 2020. Available at: https://tecnoblog.net/390237/ministerio-saude-expoe-dados-243-milhoes-pessoas/ Accessed on: June 06, 2021.

BRAZIL. Presidência da República. Decreto Nº 10.222 - Estratégia Nacional de Segurança Cibernética - E-Ciber. 2020. Available at: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Accessed on: June 06, 2021.

BRAZIL. Presidência da República. Decreto Nº 13.709/18 - Lei Geral de Proteção de Dados Pessoais. 2019. Available at: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm Accessed on: June 06, 2021.

CANDIDO, J.; BORGES, J. H.; FLORIAN, F. Segurança da informação com foco na propagação iminente de ransomware nas corporações. Simtec - Simpósio de Tecnologia da Fatec Taquaritinga, v. 4, n. 1, p. 13. 2018. Available at: https://simtec.fatectq.edu.br/index.php/simtec/article/view/270 Accessed on: June 27, 2021.

CASAL, MARCELLO. Ataque de hackers paralisa STJ pelo menos até segunda-feira (9). CUT. 2020. Available at: https://www.cut.org.br/noticias/ataque-de-hackers-paralisa-stj-pelo-menos-ate-segunda-feira-9-91a9 Accessed on: June 06, 2021.

ESCOSTEGUY, Diego. Hacker usou técnica simples para invadir STJ. 2020. Available at: https://obastidor.com.br/justica/hacker-usou-tecnica-simples-para-invadir-stj-21 Accessed on: June 06, 2021.

FILHO, JP. Editora. Ataques cibernéticos no Brasil ultrapassam 2,6 bilhões em 2020.2021. Available at: https://revistasegurototal.com.br/2021/01/15/ataques-ciberneticos-no-brasil-ultrapassam-26-bilhoes-em-2020/ Accessed on: June 06, 2021

MANDARINO JR., Raphael. Segurança e Defesa do Espaço Cibernético Brasileiro. UNB/Brasilia. 2010. Available at: https://sagres.org.br/artigos/nipe/seguranca_cibernetica.pdf. Accessed on: June 25, 2021.

MORAES, Ceia. Crimes cibernéticos e segurança da informação. 2018. Available at: https://app.uff.br/riuff/bitstream/1/8998/ Accessed on: June 27, 2021.

MINDSEC. 3,4 bilhões de ataques cibernéticos já atingiram o país em 2020. Blog Minuto da Segurança. 2020. Available at: https://minutodaseguranca.blog.br/34-bilhoes-de-tentativas-de-ataques-ciberneticos-ja-atingiram-o-pais-em-2020/ Accessed at: June 06, 2021.

NEVES.A. Como evitar se tornar uma vítima de ransomware? Samsung e Segurança. Available at: Accessed on: June 27, 2021.

GALLAGHER, Ryan. Hackers 'without conscience' target health-care providers, Bloomberg, 1 April, 2020. Available at:https://www.bloomberg.com/news/articles/2020-04-01/hackers-without-conscience-demand-ransom-from-health-providers. Accessed on: June 04, 2021.

REFERÊNCIAS

ALCÂNTARA, André, VILAR-LOPES, Gills. Overview dos casos de ataques cibernéticos durante a pandemia de COVID-19. RedeCTIDC. 2020. Disponível em: https://redectidc.com.br/rede-ctidc-covid-19-overview-dos-casos-de-ataques-ciberneticos-durante-a-pandemia.html Acesso em: 5 jun. 2021.

ALECRIM, Emerson. Ministério da Saúde expõe dados de 243 milhões de pessoas. 2020. Disponível em: https://tecnoblog.net/390237/ministerio-saude-expoe-dados-243-milhoes-pessoas/. Acesso em 6 jun. 2021.

BRASIL. Presidência da República. Decreto Nº 10.222 - Estratégia Nacional de Segurança Cibernética - E-Ciber. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em: 06 jun. 2021.

BRASIL. Presidência da República. Decreto Nº 13.709/18 - Lei Geral de Proteção de Dados Pessoais. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm Acesso em: 06 jun. 2021.

CANDIDO, J.; BORGES, J. H.; FLORIAN, F. Segurança da informação com foco na propagação iminente de ransomware nas corporações. Simtec - Simpósio de Tecnologia da Fatec Taquaritinga, v. 4, n. 1, p. 13. 2018. Disponível em: https://simtec.fatectq.edu.br/index.php/simtec/article/view/270 Acesso: 27 jun. 2021.

CASAL, MARCELLO. Ataque de hackers paralisa STJ pelo menos até segunda-feira (9). CUT. 2020. Disponível em: https://www.cut.org.br/noticias/ataque-de-hackers-paralisa-stj-pelo-menos-ate-segunda-feira-9-91a9 Acesso em: 06 jun. 2021.

ESCOSTEGUY, Diego. Hacker usou técnica simples para invadir STJ. 2020. Disponível em: https://obastidor.com.br/justica/hacker-usou-tecnica-simples-para-invadir-stj-21 Acesso em: 06 jun. 2021.

FILHO, JP. Editora. Ataques cibernéticos no Brasil ultrapassam 2,6 bilhões em 2020.2021. Disponível em: https://revistasegurototal.com.br/2021/01/15/ataques-ciberneticos-no-brasil-ultrapassam-26-bilhoes-em-2020/ Acesso em: 06 jun. 2021

MANDARINO JR., Raphael. Segurança e Defesa do Espaço Cibernético Brasileiro. UNB/Brasília. 2010. Disponível em: https://sagres.org.br/artigos/nipe/seguranca_cibernetica.pdf. Acesso em: 25 jun. 2021.

MORAES, Ceia. Crimes cibernéticos e segurança da informação. 2018. Disponível em: https://app.uff.br/riuff/bitstream/1/8998/ Acesso em: 27 jun. 2021.

MINDSEC. 3,4 bilhões de ataques cibernéticos já atingiram o país em 2020. Blog Minuto da Segurança. 2020. Disponível em: https://minutodaseguranca.blog.br/34-bilhoes-de-tentativas-de-ataques-ciberneticos-ja-atingiram-o-pais-em-2020/ Acesso em: 06 jun. 2021.

NEVES.A. Como evitar se tornar uma vítima de ransomware? Samsung e Segurança. Disponível em: Acesso em: 27 jun. 2021.

GALLAGHER, Ryan. Hackers 'without conscience' target health-care providers, Bloomberg, 1 abr. 2020. Disponível em:https://www.bloomberg.com/news/articles/2020-04-01/hackers-without-conscience-demand-ransom-from-health-providers. Acesso em: 4 jun. 2021.

HMR. Hammersmith Medicines Research. HMR visado por criminosos cibernéticos. 2020. Available at: https://www.hmrlondon.com/hmr-targeted-by-cyber-criminals Accessed on: June 06, 2021.

SANTOS, Ana L. Precisa se adaptar ao home office durante a pandemia? Descubra como. Correio Braziliense. 2020. Available at: https://www.correiobraziliense.com.br/app/noticia/eu-estudante/trabalho-e-formacao/2020/04/05/interna-trabalhoeformacao-2019,842584/precisa-se-adaptar-ao-home-office-durante-a-pandemia-descubra-como.shtml Accessed on: June 06, 2021.

SATTER, Raphael; STUBBS, Jack; BING, Christopher. Exclusive: Elite hackers target WHO as corona virus cyberattacks spike. Reuters. 2020. Available at: https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN Accessed on: June 06, 2021.

SOUZA, Ramon. Brasil sofreu mais de 8,4 bilhões de tentativas de ciberataques em 2020. Canaltech. 2021. Available at: https://canaltech.com.br/seguranca/brasil-sofreu-mais-de-8-4-bilhoes-de-tentativas-de-ciberataques-em-2020-179493/ Accessed on: June 06, 2021.

SOUZA, Ramon. Com home office, empresas descuidam de segurança e abrem brechas para hackers. Canaltech. 2020. Available at: https://canaltech.com.br/seguranca/com-home-office-empresas-descuidam-de-seguranca-e-abrem-brechas-para-hackers-172280/ Accessed on: June 06, 2021.

HMR. Hammersmith Medicines Research. HMR visado por criminosos cibernéticos. 2020. Disponível em: https://www.hmrlondon.com/hmr-targeted-by-cyber-criminals Acesso em: 6 jun 2021.

SANTOS, Ana L. Precisa se adaptar ao home office durante a pandemia? Descubra como. Correio Braziliense. 2020. Disponível em: https://www.correiobraziliense.com.br/app/noticia/eu-estudante/trabalho-e-formacao/2020/04/05/interna-trabalhoeformacao-2019,842584/precisa-se-adaptar-ao-home-office-durante-a-pandemia-descubra-como.shtml Acesso em: 06 jun. 2021.

SATTER, Raphael; STUBBS, Jack; BING, Christopher. Exclusivo: hackers de elite visam à OMS como um pico de ataques cibernéticos de coronavírus. Reuters. 2020. Disponível em: https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN Acesso em: 06 jun. 2021.

SOUZA, Ramon. Brasil sofreu mais de 8,4 bilhões de tentativas de ciberataques em 2020. Canaltech. 2021. Disponível em: https://canaltech.com.br/seguranca/brasil-sofreu-mais-de-8-4-bilhoes-de-tentativas-de-ciberataques-em-2020-179493/ Acesso em: 06 jun. 2021.

SOUZA, Ramos. Com home office, empresas descuidam de segurança e abrem brechas para hackers. Canaltech. 2020. Disponível em: https://canaltech.com.br/seguranca/com-home-office-empresas-descuidam-de-seguranca-e-abrem-brechas-para-hackers-172280/ Acesso em 06 jun 2021.

Louise Marie Hurel

Louise Marie Hurel lidera o Programa de Segurança Digital do Instituto Igarapé e é pesquisadora PhD em Data, Networks and Society no Departamento de Mídia e Comunicações da London School of Economics and Political Science. É membro do Advisory Board do Global Forum on Cyber Expertise (GFCE).

Louise Marie Hurel leads Igarapé Institute's Digital Security Program and pursues her PhD Research in Data, Networks and Society at the London School of Economics and Political Science's Department of Media and Communications. She is also an Advisory Board member of the Global Forum on Cyber Expertise (GFCE).

Gerindo Incidentes Cibernéticos: desafios e oportunidades para o Brasil e a UE

Governing Cyber Incidents: challenges and opportunities for Brazil and the EU

Louise Marie Hurel

Resumo Executivo

Este informe sobre políticas analisa (i) os mecanismos, políticas e/ou instrumentos que têm caracterizado a visão do Brasil e da UE em relação à cooperação nas respostas a incidentes cibernéticos e (ii) alguns dos desafios para sua operacionalização diante das mudanças no cenário de ameaças. Estes pontos serão desenvolvidos em três seções. A primeira apresenta uma visão geral da natureza muitas vezes debatida e complexa dos incidentes cibernéticos. A segunda oferece uma perspectiva profunda de como o Brasil e a UE têm tentado criar mecanismos políticos e institucionais para responder aos incidentes no contexto da regulamentação da proteção de dados e crescente preocupação com a defesa cibernética. Por último, o documento esboça recomendações políticas e sua importância para a governança da segurança cibernética tanto para o Brasil como para a UE.

Executive Summary

This policy brief looks at (i) the mechanisms, policies and/or tools that have characterised Brazil's and the EU's approach to cooperation in cyber incident response; and (ii) some of the challenges for their operationalisation vis-à-vis changes in the threat landscape. These points are unpacked in three sections. The first provides an overview of the complex and often-disputed nature of cyber incidents. The second provides an in-depth perspective of how Brazil and the EU have both sought to devise policy and institutional mechanisms to respond to incidents in the context of data protection regulations and growing concerns with cyber defence. Finally, the document outlines policy recommendations and their importance for both the EU and Brazil's cybersecurity governance.

Introduction

Throughout the last few years, several countries have been consistently pushing for greater digitalisation. Many have developed their own strategies and policies that set out expectations and actions for expanding the digitalisation of services and government systems — which include but is not restricted to the acquisition of new technologies, softwares and solutions as part of the common practice of the public sector to achieve such goals. While mottos such as the Silicon Valley's "move fast and break things" have served as a representation, part and parcel, of this driving force of innovation and transformation of sectors and services, security concerns often remained secondary, being neglected in the process of developing softwares and designing supply chains, for example. In addition, as these technologies reach into the most mundane aspects of how individuals go about their lives — from one's smartphone to digital identities as a requirement for citizens to access government services — they also expose users to risks of data theft and can serve to enable targeted activities against specific groups.[1]

However, cyberattacks to critical infrastructures, such as the Colonial Pipeline[2] ransomware that forced the American oil company to temporarily shut down its operations in May 2021 and the Solar Winds hack[3] that compromised multiple agencies of the US federal government, show that both governments and the private sector increasingly rely on a patchwork of technologies that are not always accompanied by strong cybersecurity protections. Thus, one of the consequences of the "moving fast and breaking things" motto — that is, an attempt to detach innovation from security concerns — is the expansion of the attack surface and landscape of action for malicious actors.[4] What is more, attacks such as these also highlight just how distributed and fragmented security provision is when it comes to the development of infrastructures and networked communications.

This "fragmentation of security provision"[5] not only provides a snapshot of the interdependencies present in cybersecurity politics but sheds light on three important dynamics: (i) it challenges the notion of the state as the traditional security provider[6]; (ii) it points to the pervasiveness of private governance of systems, infrastructures,

---

1 DEIBERT, Ronald. J. Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace. **Millennium**. 32, n. 3, p. 501-530. 2012. doi:10.1177/03058298030320030801

2 OSBORNE, Charlie. Colonial Pipeline attack: Everything you need to know. **ZDNet**. 13, March 2021. Available at: <https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/>.

3 BAKER, Pam. The SolarWinds hack timeline: Who knew what, and when? **CSO**. 4, June 2021. Available at: <https://www.csoonline.com/article/3613571/the-solarwinds-hack-timeline-who-knew-what-and-when.html>.

4 TAVERNISE, Sabrina. The Daily: Who is Hacking the US Economy? **The New York Times**. 08, June 2021. Available at: <https://www.nytimes.com/2021/06/08/podcasts/the-daily/colonial-pipeline-jbs-ransomware-attacks.html?action=click&module=audio-series-bar&region=header&pgtype=Article>

5 COLLIER, Jamie. Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision. **Politics and Governance**, 6, n. 2, p. 13-21. 2018.

6 KELLO, Lucas. **The Virtual Weapon and International Order**. New Haven, CT: Yale University Press. 2017.

Introdução

Ao longo dos últimos anos, os países têm pressionado de forma consistente por uma maior digitalização. Muitos desenvolveram suas próprias estratégias e políticas que criaram expectativas e ações para expandir a digitalização dos serviços e sistemas do governo — o que inclui, mas não se restringe às aquisições de novas tecnologias, softwares e soluções como parte da prática comum do setor público para alcançar esses objetivos. Enquanto lemas como o do Vale do Silício "mova-se rápido e quebre tudo" têm servido como uma representação fundamental dessa força motora da inovação e da transformação dos setores e dos serviços, as preocupações com a segurança em geral ficam em segundo plano, sendo negligenciadas no processo de desenvolvimento de softwares e no desenho de cadeias de fornecedores, por exemplo. Além do mais, na medida em que essas tecnologias atingem os aspectos mais corriqueiros da vida das pessoas — de um celular a identidades digitais como um pré-requisito para os cidadãos terem acesso a serviços do governo — elas também expõem os usuários ao risco de furto de dados e podem servir para permitir atividades direcionadas contra grupos específicos.[1]

No entanto, ataques cibernéticos com pedido de resgate (por ransomware) a infraestruturas críticas como a Colonial Pipeline[2], que forçou a empresa americana de petróleo a fechar temporariamente as operações em maio de 2021, e o ataque de hackers[3] à Solar Winds, que afetou diversas agências do governo federal dos EUA, mostram que tanto os governos como o setor privado confiam cada vez mais em uma colcha de retalhos tecnológica que nem sempre vem acompanhada de proteções de segurança cibernética robustas. Assim, uma das consequências do lema "mova-se rápido e quebre tudo" — isto é, a tentativa de separar inovação de preocupações com a segurança — é a expansão do campo de ataque e da área de ação de agentes mal intencionados.[4] E, além do mais, ataques como esses também chamam a atenção para como o fornecimento de segurança está distribuído e fragmentado quando se trata do desenvolvimento de infraestruturas e comunicações em rede.

Esta "fragmentação do fornecimento de segurança"[5] não oferece apenas uma imagem das interdependências presentes nas políticas de segurança cibernética, mas também esclarece três dinâmicas importantes: (i) desafia a noção de Estado como provedor tradicional de segurança[6]; (ii) assinala a generalizada governança privada dos sistemas,

---

1 DEIBERT, Ronald. J. Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace. **Millennium.** 32, n.3, p. 501-530. 2012. doi:10.1177/0305829803203003801

2 OSBORNE, Charlie. Colonial Pipeline attack: Everything you need to know. **ZDNet**. 13, March 2021. Disponível em: <https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/>.

3 BAKER, Pam. The SolarWinds hack timeline: Who knew what, and when? **CSO**. 4, June 2021. Disponível em: <https://www.csoonline.com/article/3613571/the-solarwinds-hack-timeline-who-knew-what-and-when.html>.

4 TAVERNISE, Sabrina. The Daily: Who is Hacking the US Economy? **The New York Times**. 08, June 2021. Disponível em: <https://www.nytimes.com/2021/06/08/podcasts/the-daily/colonial-pipeline-jbs-ransomware-attacks.html?action=click&module=audio-series-bar&region=header&pgtype=Article>

5 COLLIER, Jamie. Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision. **Politics and Governance,** 6, n.2, p. 13-21. 2018.

6 KELLO, Lucas. **The Virtual Weapon and International Order**. New Haven, CT: Yale University Press. 2017.

and networked communications[7]; and (iii) it sheds light on the complex landscape of actors involved in responding to a cyberattack.

These dynamics are the background of what has become a pressing question for cybersecurity governance: *How can governments effectively respond to cyberattacks? What mechanisms, policies and/or tools can enhance cooperation to identify, mitigate and address cyber incidents?*

Faced with the challenge of an effective, timely and evidence-based response, governments have devised a plethora of policies that seek to address the question of cooperation and coordination around cybersecurity threats at the national, regional, and international levels. These responses range from the development of national cybersecurity strategies and policies to discussions around international norms for the stability of cyberspace in spaces such as the United Nations Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG) on Cybersecurity. Private companies, on the other hand, encompass a wide range of actors that span from technology companies working in cybersecurity, the wider group of companies that acquire these solutions, to the growing cyber insurance market (to name a few).

This policy brief addresses those questions first, by providing an overview of the complex and often-disputed nature of cyber incidents. Second, it looks at how Brazil and the EU have both sought to devise policy and institutional mechanisms to respond to incidents. Third, it outlines policy recommendations and best practices from both cases.

The Challenge of Defining a Cyber Incident

Very few incidents make it to the media headlines, but they happen every day, continually. Cyber incidents can refer both to unintentional or intentional activities (malicious activities) that range from phishing and data leaks to botnets and more sophisticated ransomware attacks. According to Talos, Cisco's threat intelligence group, in 2018 there were more than 20 billion such attacks a day.[8] While figures may vary, numbers such as these serve to illustrate how vulnerabilities are part of the existence of infrastructures, networks, and systems. They require continuous maintenance, evaluation, and monitoring. Overall, vulnerabilities and incidents have become a pervasive condition of a digitised society.

However, the practice of determining what an incident/cyberattack is, who should respond, and how it should be addressed is far from an obvious process; it involves a complex enmeshment of technical, political, technological, and social considerations.

---

7 MUSIANI, Francesca; COGBURN, Derrick L.; DENARDIS, Laura; LEVINSON, Nanette. **The Turn to Infrastructure in Internet Governance**. London: Palgrave Macmillan. 2016. HUREL, Louise Marie & LOBATO, Luisa C. Unpacking cyber norms: private companies as norm entrepreneurs. **Journal of Cyber Policy**, 3, n. 1, p. 1-16. 2018.

8 BOTIFOLL, Jordi. This is the biggest threat to Latin America's Digital Transformation. **World Economic Forum**. 13, March 2018. Available at: <https://www.weforum.org/agenda/2018/03/this-is-the-biggest-threat-to-latin-america-s-digital-transformation/>

infraestruturas e comunicações em rede[7] e (iii) e ilumina o complexo cenário de agentes envolvidos na resposta a um ataque cibernético.

Estas dinâmicas são o pano de fundo do que passou a ser uma questão premente para a governança da segurança cibernética: *Como os governos podem responder efetivamente aos ataques cibernéticos? Que mecanismos, políticas e/ou instrumentos podem aumentar a cooperação para identificar, mitigar e lidar com os incidentes cibernéticos?*

Diante do desafio de uma resposta efetiva, oportuna e baseada em evidências, os governos elaboraram uma abundância de políticas que visa lidar com a questão da cooperação e coordenação em relação às ameaças à segurança cibernética no nível nacional, regional e internacional. Essas respostas vão desde o desenvolvimento de estratégias e políticas nacionais de segurança cibernética a discussões sobre normas internacionais para a estabilidade do espaço cibernético em espaços como o Grupo Governamental de Especialistas das Nações Unidas (UNGGE) e o Grupo de Trabalho Aberto (OEWG) sobre segurança cibernética. Empresas privadas, por outro lado, incluem uma ampla variedade de agentes, que vão de empresas de tecnologia que trabalham com segurança cibernética, o grupo mais amplo das empresas que compram essas soluções, até o crescente mercado de seguros cibernético (para mencionar alguns).

Este informe sobre políticas trata dessas questões, primeiro, ao oferecer uma visão geral da natureza frequentemente debatida e complexa dos incidentes cibernéticos. Em segundo lugar, analisa como o Brasil e a UE têm procurado criar mecanismos institucionais e políticos para responder a esses incidentes. Em terceiro lugar, esboça recomendações de políticas e de melhores práticas em ambos os casos.

O Desafio de Definir um Incidente Cibernético

São muito poucos os incidentes que chegam às manchetes dos meios de comunicação, mas acontecem todos os dias, de forma contínua. Os incidentes cibernéticos podem ser tanto atividades não intencionais como intencionais (atividades dolosas) que vão desde phishing e vazamento de dados de botnets e ataques mais sofisticados com pedido de resgate (por ransomware). De acordo com a Talos, o grupo de inteligência para ameaças da Cisco, em 2018, houve mais de 20 bilhões de ataques por dia.[8] Os números podem variar, mas cifras como essa servem como ilustração de como as vulnerabilidades fazem parte da existência das infraestruturas, redes e sistemas. Estes requerem manutenção constante, avaliação e monitoramento. Em geral, as vulnerabilidades e os incidentes se tornaram uma condição generalizada em uma sociedade digitalizada.

No entanto, o exercício de determinar o que é um incidente/ataque cibernético, quem deve responder e como deve ser tratado está longe de se um processo óbvio, pois envolve um emaranhado complexo de considerações técnicas, políticas, tecnológicas e sociais.

---

7 MUSIANI, Francesca; COGBURN, Derrick L.; DENARDIS, Laura; LEVINSON, Nanette. **The Turn to Infrastructure in Internet Governance**. London: Palgrave Macmillan. 2016. HUREL, Louise Marie & LOBATO, Luisa C. Unpacking cyber norms: private companies as norm entrepreneurs. Journal of Cyber Policy, 3, n.1, p. 1-16. 2018.

8 BOTIFOLL, Jordi. This is the biggest threat to Latin America's Digital Transformation. **World Economic Forum.** 13, March 2018. Disponível em: <https://www.weforum.org/agenda/2018/03/this-is-the-biggest-threat-to-latin-america-s-digital-transformation/>

Technologically, the identification of incidents involves a host of technologies and tools that are used to identify, communicate, share information about codes, threat indicators, network data and respond to incidents. These tools often range from the implementation of sensors (*honeypots*) across different networks — to gather information about network activities to support the process of investigation of a particular incident — to AI-driven solutions that seek to identify threat vectors, assemble vulnerability reports, and provide on-demand or continuous "threat intelligence". As is the case with other big data analytics solutions[9], while the delegation of threat detection to automated solutions can help streamline security activities and optimise response procedures, it can also result in less human supervision over the handling of an incident. The greater the delegation is, the lesser the control is over the interpretation and understanding of the incident response.

Politically, the identification of incidents can occur through state-led processes *of political attribution* whereby one state publicly declares that another actor (state or non-state) is involved and/or responsible for perpetrating an attack. In other words, attribution responds to the challenging question of identifying "who did it" — the perpetrator of an attack. One example of this practice was the Democratic National Committee hack in the US 2016 elections that was attributed to a group of state-sponsored Russian hackers called Fancy Bear or APT28 by an FBI and Department of Homeland Security joint report[10] — confirmed by the cybersecurity company CrowdStrike.[11] However, political attribution, in its broadest sense, can be considered beyond international state-state or state-sponsored cyberattacks and, when not followed by checks and balances and/or technical information, it can become a powerful political and rhetoric weapon to blame adversaries — be they domestic or international.

Technically, incidents are an integral part of the work of technical experts, network engineers, information security analysts, and so forth, that conduct incident response both in the public and private sector. Each country possesses a national focal point for incident response that has been called, since the 1980s, a Computer Security Incident Response Team (CSIRT). In Brazil, these national teams are the CERT.BR and CTIR Gov. The latter is responsible for coordinating incident response across the Federal Public Administration (APF), and the former focuses on the networks beyond the APF. These CSIRTs have established international and regional networks of collaboration and information sharing. Globally, the Forum on Incident Response Teams (FIRST) is the main space for teams to connect. There are also multiple regional networks such as the Latin America and Caribbean Network Information Centre (LACNIC) CSIRT group, Europe-based Task Force on Computer Security Incident Response Teams (TF-CERT) and the European Union Agency for Cybersecurity (ENISA).

9 KITCHIN, Robert. **The Data Revolution: Open Data, Data Infrastructures and Their Consequences.** London: SAGE. 2014.

10 SPRING, Tom. FBI-DHS Report Links Fancy Bear Gang to Election Hacks. **Threat Post**. Available at: <https://threatpost.com/fbi-dhs-report-links-fancy-bear-to-election-hacks/122802/>. Accessed: 27 Jun 2021.

11 CROWDSTRIKE'S work with the Democratic National Committee: Setting the record straight. **Crowdstrike.** 5, June 2020. Available at: <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>. **Accessed: 27 Jun 2021**.

Em termos tecnológicos, a identificação de incidentes envolve um conjunto de tecnologias e instrumentos que são usados para identificar, comunicar, compartilhar informações sobre códigos, indicadores de ameaças, dados de rede e resposta aos incidentes. Esses instrumentos podem ser desde a implementação de sensores (honeypots) em diversas redes — para obter informações sobre atividades de rede a fim de auxiliar no processo de investigação de um incidente específico — a soluções baseadas em IA que tentam identificar vetores de ameaças, reunir relatórios de vulnerabilidade e oferecer "inteligência sobre ameaças" contínua ou sob encomenda. De forma semelhante a outras soluções analíticas de big data[9], delegar a detecção de ameaças às soluções automáticas pode ajudar a agilizar as atividades de segurança e otimizar procedimentos de respostas, mas pode redundar também em menos supervisão humana ao lidar com um incidente. Quanto maior for a delegação, menor será o controle em relação à interpretação e compreensão da resposta ao incidente.

Em termos políticos, a identificação de incidentes pode ocorrer através de processos realizados pelo Estado *por atribuição política* por meio da qual um Estado declara publicamente que outro agente (Estado ou não Estado) está envolvido e/ou é responsável por realizar um ataque. Em outras palavras, a atribuição responde à questão desafiadora de identificar "quem foi" — o autor do ataque. Um exemplo dessa prática foi o ataque por hackers ao Comitê Nacional Democrático nas eleições presidenciais dos EUA em 2016, que foi atribuído a um grupo de hackers financiado pelo Estado russo, chamado Fancy Bear ou APT28, em um relatório[10] conjunto do FBI e do Departamento de Segurança Nacional — confirmado pela empresa de segurança cibernética CrowdStrike.[11] No entanto, a atribuição política, num sentido mais amplo, pode ser contemplada para além de ataques cibernéticos internacionais entre Estados ou financiados por Estados e, quando não acompanhada de mecanismos de freios e contrapesos e/ou informação técnica, pode ser uma poderosa arma política e retórica para culpar adversários — sejam eles internos ou externos.

Em termos técnicos, os incidentes são parte integrante do trabalho de especialistas técnicos, engenheiros de rede, analistas de segurança de informação, entre outros, que lideram a resposta ao incidente tanto no setor público quanto no privado. Cada país tem um ponto focal para resposta a incidentes que se denomina, desde os anos 80, uma Equipe de Resposta a Incidente de Segurança Computacional (CSIRT). No Brasil, essas equipes nacionais são os CERT.BR e os CTIR Gov. Este último é responsável por coordenar a resposta a incidentes em toda a Administração Pública Federal (APF), enquanto o anterior se dedica às redes além da APF. Estes CSIRTs criaram redes regionais e internacionais de colaboração e compartilhamento de informação. Internacionalmente, o Fórum Global de Resposta a Incidentes e Equipes de Segurança (FIRST) é o principal espaço para as equipes se conectarem. Existem, também, diversas redes regionais,

[9] KITCHIN, Robert. **The Data Revolution: Open Data, Data Infrastructures and Their Consequences**. Londres: SAGE. 2014.

[10] SPRING, Tom. FBI-DHS Report Links Fancy Bear Gang to Election Hacks. **Threat Post**. Disponível em: <https://threatpost.com/fbi-dhs-report-links-fancy-bear-to-election-hacks/122802/>. Acessado em: 27 Jun 2021.

[11] CROWDSTRIKE'S work with the Democratic National Committee: Setting the record straight. **Crowdstrike.** 5, June 2020. Disponível em: <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>. Acessado em: 27 jun. 2021.

However, more than mere technical vulnerabilities, incidents are socially constructed within a national environment with specific policies, norms, and collective understandings of cyber risks. As the section shows, the understanding of an incident is embedded in complex socio-technical dynamics that assemble technologies, actors, and political intention together. What is more, it highlights that incident response is composed by a continuum of practices that go from informal collaboration networks among technical experts to corporate solutions and political attribution.

Governing cyber incidents: a complex landscape in Brazil and the EU

There are multiple definitions of incidents across all sectors, but growing attention from governments to cybersecurity threats throughout the past decades has led to the development and proliferation of institutions related to incident handling. While responses to cyber incidents have been initially associated with computer and information security and, more specifically, with technical professionals working in CERTs, the emergence of national cybersecurity centres, cyber commands, and other institutions, as well as regulations targeting cybersecurity and data protection have all contributed to the reconfiguration and dispersion of the governance of cyber incidents across government agencies.

Brazil's Challenge: cyber incident, data security incident or both?

Brazil's *Information Security Glossary,* developed by the Institutional Security Office of the Presidency *(Gabinete de Segurança Institucional)*, provides two definitions to cyber incidents: incident (*incidente*) and security incident (*incidente de segurança*). The former refers to the event, action or omission that has or can enable unauthorised access, interruption, or changes to protected information. The latter qualifies the incident as a confirmed or suspected event related to the security of computer systems or networks. Such definitions are in line with Brazil's broader understanding of information security[12] — the actions and measures taken to ensure the confidentiality, integrity, and availability of information — as the general framing that encompasses cybersecurity practices — the actions directed towards the protection and security of operations and information systems.

However, according to the Brazilian Data Protection Law (LGPD) a *security incident* refers to the protection of personal data from non-authorised access and from accidental or illegal situations that involve the destruction, loss, alteration, communication, or any other form of inadequate or illicit treatment of the data (Art. 46). In early 2021, the Data Protection Authority (DPA) opened a call for public comments on security incident notifications, which has, in turn, resurfaced concerns over how reporting mechanisms will make sure that organisations know who to contact and what to report in each case.

[12] HUREL, L. M. Cibersegurança no Brasil: Uma Análise da Estratégia Nacional. **Instituto Igarapé**. 2021. Disponível em: https://ciberseguranca.igarape.org.br/estrategia/. Accessed: 27 Jun 2021.

como o Registro de Endereçamento da Internet para a América Latina e o Caribe (LACNIC), o grupo CSIRT, a Força Tarefa com base na Europa de Equipes de Resposta a Incidentes de Segurança Computacional (TF-CERT) e a Agência da União Europeia de Segurança Cibernética (ENISA).

Contudo, mais do que meras vulnerabilidades técnicas, os incidentes são socialmente construídos dentro de um ambiente nacional com políticas específicas, normas e uma compreensão coletiva do risco cibernético. Como esta seção demonstra, a compreensão de um incidente está repleta de dinâmicas técnico-sociais complexas que reúnem tecnologias, agentes e intenções políticas. E, ainda mais, enfatiza que a resposta a um incidente é composta por uma continuidade de práticas que vai desde redes informais de colaboração entre especialistas técnicos a soluções corporativas e atribuições políticas.

Gerindo incidentes cibernéticos: um cenário complexo no Brasil e na UE

Existem muitas definições de incidentes em diversos setores, mas a atenção crescente dos governos a ameaças à segurança cibernética ao longo das últimas décadas levou ao desenvolvimento e à proliferação de muitas instituições relacionadas a lidar com essas ameaças. Embora, de início, respostas a incidentes cibernéticos tenham sido associadas a computadores e segurança da informação, mais especificamente a profissionais técnicos que trabalham em CERTs[12], o surgimento de centros nacionais de segurança cibernética, comandos cibernéticos e outras instituições, assim como a regulamentação que tem como objetivo a segurança cibernética e a proteção de dados, todos contribuíram para a reconfiguração e a distribuição da governança dos incidentes cibernéticos a diversas agências governamentais.

O desafio do Brasil: incidente cibernético, segurança de dados ou ambos?

O *Glossário de Segurança da Informação* do Brasil, desenvolvido pelo Gabinete de Segurança Institucional, apresenta duas definições para incidentes cibernéticos: *incidente e incidente de segurança*. A primeira se refere ao evento, ação ou omissão que tenha permitido ou possa permitir acesso não autorizado, interrupção ou modificações em informações protegidas. A segunda qualifica o incidente como um evento suspeito ou confirmado relacionado à segurança dos sistemas de computação ou às redes. Estas definições estão de acordo com uma compreensão mais ampla sobre segurança da informação[13] no Brasil — as ações e medidas tomadas para garantir a confidencialidade, integridade e disponibilidade da informação — como um marco geral que inclui as práticas de segurança cibernética — as ações dirigidas à proteção e à segurança dos sistemas de operação e de informação.

No entanto, de acordo com a Lei Geral de Proteção de Dados do Brasil (LGPD), um *incidente de segurança* se refere à proteção de dados pessoais por alguém não autorizado e

[12] Centros de Estudos de Resposta e Tratamento de Incidentes em Computadores. (Nota do Revisor.)

[13] HUREL, L.M. Cibersegurança no Brasil: Uma Análise da Estratégia Nacional. Instituto Igarapé. 2021. Disponível em: https://ciberseguranca.igarape.org.br/estrategia/. Acessado em: 27 jun. 2021.

In line with other data protection regulations, Brazil's data protection law specifies (Art. 48) that the data controller should communicate to the DPA any security incident (*incidente de segurança*) that might pose a risk or harm to the subject's data. In these cases, the DPA is also responsible for verifying the severity of the incident and can require from the controller the adoption of measures that include (i) the public communication of the incident and/or (ii) measures to revert or mitigate the effect of the incident (Art. 28 §2).

Table: Data protection and cybersecurity approaches to incidents

	Data Protection (LGPD)	Cybersecurity/ Network Security
Scope	Protection of natural persons with regard to the processing of personal data	No single regulation or policy for cybersecurity incidents.
Target	Applies to any person or entity processing personal data (Art. 3).	Policies can apply to: >APF (ETIR networks) >Sectorial regulations (Banking and Telecom, for example)
Highlights	Clear designation of roles and responsibilities for notification processes within the LGPD – the ANPD, in this case. Rights and principles-based regulation that foresees greater transparency for subjects in cases of data security incidents.	Both APF agencies and sectorial regulations have included specific provisions on incident handling and notification. Some examples are: >Banking (CMN Resolution 4.893/2021) >Telecom (Anatel Resolution 760/2020) >National Justice Council (CNJ Resolution 396/2021)
Notification Requirements	The controller should communicate to the national authority and the data subject security incidents that could lead to risk or relevant harm to subject. Notification should be made in a 'reasonable' timeframe (Art. 48 §1).	>Institute and implement teams for the prevention, treatment and response to cyber incidents within the APF. Coordinated by CTIR Gov (Decree 9.637/2018) >Implement mechanisms for immediate communication of vulnerabilities or security incidents (Decree 9.637/2018).
Penalties	Multiple types of administrative sanctions (Art. 52)	Not specified

However, the challenge for Brazil is to understand how these different notification avenues — one through the DPA and another, more technical, through the national CERT, in this case, CTIR Gov for APF agencies — are to work in tandem; and not to assume that public agencies necessarily have a clear understanding of the difference between both types of incidents. Attacks can include both incident dimensions (data and system). Recognizing these blurry lines can help these

por situações acidentais e ilegais que envolvam a destruição, perda, alteração, divulgação, ou qualquer outra forma de tratamento inadequado ou ilícito dos dados (Art. 46). No início de 2021, a Autoridade Nacional de Proteção de Dados (ANPD) convocou uma audiência pública para comentários sobre notificações de incidentes de segurança que fez com que preocupações já existentes voltassem à tona em relação ao modo como os mecanismos de notificação podem garantir que as organizações saibam quem contatar e o que informar em cada caso.

De forma semelhante a outras regulamentações sobre proteção de dados, a Lei Geral de Proteção de Dados (LGPD) do Brasil especifica (Art. 48) que um responsável pelos dados deve comunicar à ANDP qualquer *incidente de segurança* que possa representar um risco ou dano aos dados submetidos. Nesses casos, a ANDP também é responsável por verificar a gravidade do incidente e pode requerer do responsável a adoção de medidas que incluam (i) um comunicado público do incidente e/ou (ii) medidas para reverter ou mitigar o efeito do incidente (Art. 28 §2).

Tabela: Abordagem de proteção de dados e segurança cibernética dos incidentes

	Proteção de Dados (LGPD)	**Segurança cibernética e Segurança de Redes**
Escopo	Proteção de pessoas naturais em relação ao processamento de dados pessoais	Não há uma única regulamentação ou política sobre incidentes de segurança cibernética.
Objetivo	Aplica-se a qualquer pessoa ou entidade que processe dados pessoais (Art. 3).	Políticas podem ser aplicadas a: >APF (ETIR redes) >Regulamentações Setoriais (Bancos e Telecomunicações, por exemplo)
Destaques	Atribuição clara dos papéis e responsabilidades pelo processo de notificação dentro da LGPD – no caso, a ANPD. Regulamentação baseada em direitos e princípios que preveem mais transparência para os sujeitos em caso de incidentes de segurança de dados.	Ambas agências da APF e regulamentações setoriais incluíram disposições específicas sobre o manejo de incidentes e notificações. Alguns exemplos são: >Setor bancário (CMN Resolução 4.893/2021) >Telecom (Anatel Resolução 760/2020) >Conselho Nacional de Justiça (CNJ Resolução 396/2021)
Requisitos para Notificação	O responsável deve comunicar à autoridade nacional os dados sujeitos a incidentes de segurança que possam levar a um risco ou dano relevante ao sujeito. A notificação deve ser feita em um prazo "razoável" (Art. 48 §1).	>Institui e implementa equipes para a prevenção, tratamento e resposta a incidentes cibernéticos dentro do escopo da APF. Coordenado pelo CTIR Gov (Decreto 9.637/2018) >Implementa mecanismos para a comunicação imediata de vulnerabilidades ou incidentes de segurança (Decreto 9.637/2018).
Sanções	Diversos tipos de sanções administrativas (Art. 52)	Não especificado

agencies reassess the notification process and establish adequate procedures for sharing or passing on information to the relevant body whenever a notification needs to be redirected.

While the LGPD provides a clearer pathway to notification processes for data breaches (even if still under construction), there is no single policy that governs incident reporting when it comes to network security and cybersecurity. The latter often includes a host of activities such as informal technical information exchange among CERTs and across the APF, submission of notifications from different organisations in the APF to the development of sectorial policies that place regulators as key points for notification of "relevant incidents". Going forward, the government will need to ensure that there is a plan for equalizing data protection and cybersecurity provisions across the APF — enhancing the existing best practices and strengthening a principles and rights-based approach to network and cybersecurity.

The EU: Harmonizing the institutional and regulatory complex

Throughout the years, the EU has developed a robust approach to emerging cybersecurity challenges that range from directives to new institutional developments, cyberdiplomacy toolkits and joint frameworks for dealing with cyber threats across member states. The EU's cybersecurity strategy and other documents such as the European Agenda on Security, the Digital Single Market strategy and the EU's global strategy have all contributed to the formation of a multidimensional view of cybersecurity from different angles (economic, security, international engagement). More recently, the EU has begun to reassess its previous documents. This, in turn, has led to the approval of the Cybersecurity Act (2019), a new Cybersecurity Strategy (2020), and the development of the second version of the NIS Directive. However, key challenges remain[13] as to how to harmonise existing mechanisms, national policies, and approaches to cybersecurity[14], in general, and incident response, in particular.

In regulatory terms, the EU's NIS Directive, approved in 2016 — and officially nationally transposed in 2018 by member states — has significantly contributed to building a common guideline for cybersecurity across the region. The Directive incorporates both data security and network security as part of the specifications of cyber incidents. On the one hand, the Directive defines *incidents* as "any event having an actual adverse effect on the security of network and information systems" (Art. 4). It also requires member states to have a designated CERT or competent authority to receive incident notifications (Art. 9), defines specific factors for determining the disruptiveness of a particular incident (Art. 6), establishes a CSIRT Network among member states (Art. 12), and outlines notification requirements

[13] ALUNGE, Rogers. Breach of security vs personal data breach: effect on EU data subject notification requirements. **International Data Privacy Law**. 2020. Available at: <https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaa021/5921790?login=true>. Accessed: 27 Jun 2021.

[14] ŚWIĄTKOWSKA, Joanna. Harmonised Approach to Cybersecurity – The Holy Grail of the European Union. **EU Cyber Direct. 2019. Available at**: < https://eucyberdirect.eu/wp-content/uploads/2019/12/swiatkowska_pif.pdf>. Accessed: 27 Jun 2021.

No entanto, o desafio para o Brasil é entender como esses diversos sistemas de notificação, um deles através do ANDP — e outro, mais técnico, através do CERT nacional, neste caso, o CTIR Gov para agências APF — devem trabalhar em conjunto; também considerando que nem todos os órgãos públicos têm necessariamente uma compreensão da diferença entre os dois tipos de incidentes. Ataques podem incluir ambas dimensões (dados e sistemas). Reconhecer essas linhas tênues pode ajudar esses órgãos a reavaliar o processo de notificação e estabelecer procedimentos adequados para compartilhar ou passar informações ao órgão competente sempre que uma notificação precisar ser redirecionada.

Embora a LGPD apresente um caminho mais claro em relação aos processos de notificação em casos de violações de dados (mesmo que ainda em construção), não há uma política única que determine a comunicação de incidentes quando se refere à segurança de rede e à segurança cibernética. Esta última, com frequência, inclui uma gama de atividades como o intercâmbio informal de informações técnicas entre CERTs e ao longo da APF, o envio de notificações de diferentes organizações na APF para o desenvolvimento de políticas setoriais que coloca os reguladores como pontos chave para notificações de "incidentes relevantes". Indo além, o governo irá precisar garantir que existe um plano para equalizar as provisões de proteção de dados e segurança cibernética em toda a APF — aprimorando as boas práticas já existentes e fortalecendo uma abordagem às redes e à segurança cibernética baseada em direitos e princípios.

A UE: Harmonizando o conjunto regulatório e institucional

Ao longo dos anos, a UE desenvolveu um método robusto diante dos novos desafios de segurança cibernética que inclui desde diretrizes a novos desenvolvimentos institucionais, diplomacia cibernética, conjunto de instrumentos e estruturas conjuntas para lidar com ameaças cibernéticas nos Estados Membro. A Estratégia da UE para Cibersegurança e outros documentos, tais como a Agenda Europeia sobre Segurança, a Estratégia do Mercado Único Digital e a Estratégia Global da UE contribuíram para a formação de uma visão multidimensional da segurança cibernética a partir de diferentes ângulos (econômico, segurança e participação internacional). Mais recentemente, a UE começou a revisar os documentos anteriores. Isto, por sua vez, levou à aprovação da Lei de Segurança Cibernética (2019), a uma nova Estratégia de Nacional de Segurança Cibernética (2020) e ao desenvolvimento da segunda versão da Diretriz NIS. No entanto, desafios importantes permanecem[14] a respeito de como harmonizar os mecanismos existentes, as políticas nacionais e as abordagens relacionadas à segurança cibernética[15], em geral, e resposta a incidentes, em particular.

Em termos regulatórios, a Diretriz NIS da UE, aprovada em 2016 — e oficialmente adotada em nível nacional em 2018 pelos Estados Membro — contribuiu significativamente para a construção de uma diretriz comum sobre segurança cibernética em toda a região.

[14] ALUNGE, Rogers. Breach of security vs personal data breach: effect on EU data subject notification requirements. **International Data Privacy Law**. 2020. Disponível em: <https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaa021/5921790?login=true>. Acessado em: 27 Jun 2021.

[15] ŚWIĄTKOWSKA, Joanna. Harmonised Approach to Cybersecurity – The Holy Grail of the European Union. **EU Cyber Direct**. 2019. Disponível em: < https://eucyberdirect.eu/wp-content/uploads/2019/12/swiatkowska_pif.pdf>. Acessado em: 27 Jun 2021.

for operators of essential services and digital service providers (Art. 14, 16) — to name a few. On the other hand, and beyond the work conducted by national CERTs, the Directive specifies that "competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents." As the table above shows, the GDPR and the NIS Directive complement each other in establishing an EU approach to the governance of cyber incidents.

Table: Data protection & cybersecurity approaches to incidents

(Source: ECA, 2019)[15]

	Data Protection (GDPR)	Cybersecurity/Network Security (NIS Directive)
Scope	Personal Data Security – Protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.	Network Security – Achievement of high level of security of network and information systems within the Union so as to improve the functioning of the internal market.
Target	Applies to any person or entity processing personal data related to the offering of goods and services or to the monitoring of their behaviour.	Security and notification requirements apply to operators of essential services and digital service providers.
Highlights	Rights of the data subject. Obligations of data controllers. Rules for transferring personal data.	>Obligation for Member States to define: a national strategy and to designate competent authorities, single points of contact and CSIRTs. >Establishment of Cooperation Group and CSIRTs Network.
Notification Requirements	Report breaches to supervisory authority without delay. In some cases, the data subjects (individuals) need to be informed too.	Incident reporting to the Competent Authority by: >Operators of essential services (energy, transport, banking, health, water, digital infrastructure); and >Providers of digital services (online market places, online search engines, cloud computing services).
Penalties	Up to €20 million or 4% of annual global turnover.	Member States shall set penalties that are effective, proportionate, and dissuasive.

[15] CHALLENGES to effective EU cybersecurity policy: Briefing Paper. **European Court of Auditors**. 2019. Available at: <https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf>. Accessed: 27 Jun 2021.

A Diretriz incorpora tanto a segurança de dados quanto a segurança de redes como parte das especificações dos incidentes cibernéticos. Por um lado, a Diretriz define *incidentes* como "qualquer evento que tenha um efeito adverso real na segurança da rede e nos sistemas de informação" (Art. 4). Também exige que os Estados Membro designem um CERT ou autoridade competente para receber notificações de incidentes (Art. 9), define fatores específicos para a determinação da gravidade de um incidente em particular (Art. 6), estabelece uma Rede CSIRT entre os Estados Membro (Art. 12) e estabelece requisitos de notificação para operadores de serviços essenciais e provedores digitais (Art. 14,16) — para mencionar apenas alguns. Por outro lado, e além do trabalho realizado pelos CERTs nacionais, a Diretriz especifica que as "autoridades competentes e autoridades de proteção de dados devem cooperar e trocar informação sobre todos os assuntos relevantes para solucionar qualquer violação de dados pessoais causada por incidentes." Como mostra a tabela abaixo, a GDPR e a Diretriz NIS se complementam no estabelecimento de uma abordagem de governança de incidentes cibernéticos pela UE.

Tabela: Abordagem de Proteção de Dados & segurança cibernética em incidentes (Fonte: ECA, 2019)[16]

	Proteção de Dados (GDPR)	Segurança Cibernética /Segurança de Redes (Diretriz/ Norma NIS)
Escopo	Segurança de Dados Pessoais – Proteção de pessoas naturais em relação ao processamento de dados pessoais e regras relacionadas ao movimento livre dos dados pessoais.	Segurança de Redes – Alcançar um alto nível de segurança de rede e de sistemas de informação dentro da União para melhorar o funcionamento do mercado interno.
Objetivo	Aplica-se a qualquer pessoa ou entidade que processe dados pessoais relacionados à oferta de bens e serviços ou ao monitoramento do seu comportamento.	Segurança e requisitos de notificação se aplicam aos operadores de serviços essenciais e fornecedores de serviços digitais.
Destaques	Direitos do sujeito dos dados Obrigações dos gestores de dados. Regras para compartilhamento de dados pessoais.	>Obrigação dos Estados Membro definir uma estratégia nacional e designar autoridades competentes, pontos únicos de contatos e CSIRTs. >Estabelecer Grupos de Cooperação e Redes de CSIRTs.
Requisitos para Notificação	Comunicar violações à autoridade supervisora o quanto antes. Em alguns casos os sujeitos dos dados (indivíduos) precisam ser informados.	Comunicação de Incidentes à Autoridade Competente por: >Operadores de serviços essenciais (energia, transporte, bancos, saúde, água, infraestrutura digital); e >Provedores de serviços digitais (mercado online, buscadores online, serviços de computação na nuvem).
Sanções	Até €20 milhões ou 4% do faturamento anual global.	Estados Membro devem estabelecer penalidades que sejam efetivas, proporcionais e dissuasivas.

[16] CHANLLENGES to effective EU cybersecurity policy: Briefing Paper. **European Court of Auditors**. 2019. Disponível em: <https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf>. Acessado em: 27 Jun 2021.

In addition to the regulatory steps to promote policy alignment between data protection and cybersecurity in the region, the EU has also sought to institutionally enhance their operational cooperation in cybersecurity. One of the key bodies in the EU's cybersecurity governance has been ENISA, which has, since its establishment in 2004, developed an important role in research, incident response cooperation across sectors and member states and supported governments across the region in enhancing their cybersecurity capacities through training, guidance on policy development and expansion of operational coordination across CERTs (CSIRT Network).

However, on 23 June 2021, the Commission launched a proposal for a Joint Cyber Unit to respond to cyberattacks[16], creating yet another space for information sharing and response beyond the CSIRT Network and other technical avenues for cooperation that were already in place (e.g., EC3 and the Blueprint for a Coordinated Response to Large Scale Cybersecurity Incidents and Crises). While ENISA would serve as the secretariat for the Joint Cyber Unit, the proposal highlights a stronger commitment from the EU in pushing towards what could be a more active and coordinated response to threat detection and response. As the Council Recommendation notes[17]

> [A] mechanism for harnessing existing resources and providing mutual assistance across the cyber communities responsible for network and information systems security, for combating cybercrime, for conducting cyber-diplomacy, and, where appropriate, for cyber-defence in the event of a crisis does not yet exist.

In the attempt to enhance coordination, the creation of the Joint Cyber Unit reintroduces the challenge of institutional complexity across the EU's activities in cybersecurity. What is more, the Unit sheds light on the transformation of technical cooperation in a time of growing ransomware attacks and their association with state-linked actors — such as the case of Solar Winds. The Commission's response goes beyond information sharing for the purposes of incident response and emphasises the need for threat intelligence gathering across Security Operations Centres.

The EU's case highlights the challenges involved in adapting institutional and policy responses to an evolving threat landscape. While regulatory measures have ensured some sort of complementarity, institutionally there are still many questions regarding "response" activities, the actors involved in doing so, the objectives and expected outcomes of what seems to be a more proactive approach to cyber threat mitigation.

---

[16] EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents. **European Commission.** 23 June 2021. Available at: < https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3088>. Accessed: 27 June 2021.

[17] RECOMMENDATION on building a Joint Cyber Unit. European Commission. 2021. Available at: <https://digital-strategy.ec.europa.eu/en/library/recommendation-building-joint-cyber-unit>.

Além das medidas regulatórias para promover um alinhamento político entre a proteção de dados e a segurança cibernética na região, a UE também tem buscado aumentar institucionalmente sua cooperação operacional em segurança cibernética. Um dos principais órgãos de governança de segurança cibernética da UE tem sido a ENISA, que, desde que foi criada em 2004, tem desenvolvido um importante papel na pesquisa e cooperação entre diversos setores e Estados Membro em resposta a incidentes e apoiado governos em toda a região para melhorar suas capacidades em segurança cibernética por meio de treinamento, orientação no desenvolvimento de políticas e na expansão da coordenação operacional entre todos os CERTs (Rede CSIRT).

Contudo, no dia 23 de junho de 2021, a Comissão lançou uma proposta de uma Unidade Cibernética Conjunta para responder a ataques cibernéticos[17], criando ainda mais um espaço para compartilhar informações e respostas além da Rede CSIRT e outras vias técnicas de cooperação que já existem (p. ex., EC3 e a Cartilha para uma Resposta Coordenada a Crises e Incidentes de Segurança Cibernética de Larga Escala). Enquanto a ENISA seria a secretaria para a Unidade Cibernética Conjunta, a proposta enfatiza um compromisso mais forte da UE em avançar rumo ao que poderia ser uma detecção e resposta a ameaças mais ativas e coordenadas. Como diz a Recomendação do Conselho[18]:

> [Um] mecanismo para aproveitar os recursos existentes e prestar assistência mútua entre as comunidades cibernéticas responsáveis pela segurança de sistemas de redes e de informação para combater o crime cibernético e para conduzir a diplomacia cibernética e, quando adequado, pela defesa cibernética no caso de uma crise, ainda não existe.

Na tentativa de melhorar a coordenação, a criação da Unidade Cibernética Conjunta reintroduz o desafio da complexidade institucional em todas as atividades de segurança cibernética da UE. Aliás, a Unidade ajuda a esclarecer a transformação da cooperação técnica em um momento de aumento de ataques com pedido de resgate (por ransomware) e sua associação a agentes vinculados a Estados — como o caso da Solar Winds. A resposta da Comissão vai além do compartilhamento de informações com o objetivo de responder a um incidente e enfatiza a necessidade de coletar informações sobre ameaças que conjugando todos os Centros Operacionais de Segurança.

O caso da UE chama a atenção para os desafios envolvidos na adaptação de respostas institucionais e políticas a um cenário de ameaças em constante evolução. Embora medidas regulatórias tenham garantido algum tipo de complementariedade, institucionalmente ainda há muitas questões relacionadas às atividades de "resposta", aos agentes responsáveis por elas, aos objetivos e resultados esperados do que parece ser uma abordagem mais proativa em relação à mitigação de ameaças cibernéticas.

---

[17] EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents. European Commission. 23 June 2021. Disponível em: < https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3088>. Acessado em: 27 June 2021.

[18] RECOMMENDATION on building a Joint Cyber Unit. European Commission. 2021. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/recommendation-building-joint-cyber-unit>.

Policy Recommendations

- **Governments should have a proactive approach to harmonizing data protection and cybersecurity frameworks.** In Brazil's case, the challenge is one of ensuring that this cross-pollination of efforts goes beyond the debate on developing a notification form and becomes a continuous dialogue between the ANPD and CERTs that fulfil a coordinating function (e.g.: CAIS-RNP, CERT BR, CTIR Gov), and regulatory agencies that perform a coordinating role in terms of incident information gathering (e.g., Anatel and Central Bank). The EU will also need to further understand existing incident response and information sharing activities coordinated by ENISA (and CSIRT network).

- When developing regulations and/or mechanisms associated with incident handling and response, **governments should assume gaps of knowledge across the targeted sectors.** Varying levels of capacity both in terms of data protection and cybersecurity have a direct impact on the notification process. It is not always the case that the notifier has a clear perspective on who (which body) to notify, especially in contexts of more complex incidents.

- To avoid the duplication of efforts, **governments should ensure that there are open avenues of collaboration between incident response teams and the DPA** — as the EU's case shows. This is particularly important for the operation and effectiveness of the ANPD going forward.

- While there has been much emphasis on the regulatory and institutional development of incident response capacities, these discussions should be accompanied by careful consideration of automated threat detection solutions. Even though useful for ensuring the timeliness of incident response activities, greater delegation to AI means less human supervision over identification processes. In this regard, **government agencies in Brazil and the EU should continue to foster a critical reflection on best practices for incorporating and acquiring AI solutions for cybersecurity into national incident response, offensive actions (cyber defence), and law enforcement activities.**

Recomendações de Políticas

- **Os governos devem adotar uma abordagem proativa para harmonizar as estruturas de proteção de dados e segurança cibernética.** No caso do Brasil, o desafio é garantir que esta polinização cruzada de esforços vá além do debate sobre desenvolver uma forma de notificação e se torne um diálogo contínuo entre a ANPD e CERTs, que preenchem uma função de coordenação (p. ex., CAIS-RNP, CERT BR, CTIR Gov), e agências reguladoras que desempenham um papel de coordenação da coleta de informações sobre um incidente (p. ex., Anatel e o Banco Central). A UE também precisará entender melhor como funcionam as atividades existentes de resposta a incidentes e de compartilhamento de informações coordenadas pela ENISA (e a rede CSIRT).

- Ao desenvolver regulamentações e/ou mecanismos associados ao manejo e resposta a incidentes, **governos devem supor lacunas de conhecimento em todos os setores importantes**. Níveis variáveis de capacidade, tanto em termos de proteção de dados quanto de segurança cibernética, têm um impacto direto no processo de notificação. Nem sempre acontece que quem notifica saiba a quem notificar (que órgão), especialmente em um contexto de incidentes mais complexos.

- Para evitar a duplicidade de esforços, **os governos devem garantir que há caminhos abertos de colaboração entre as equipes de resposta a incidentes e a ANDP** – como mostra o caso da UE. Isto é particularmente importante para que a operação e a efetividade da ANPD possam avançar.

- Embora tenha havido muita ênfase no desenvolvimento regulatório e institucional das capacidades de resposta a incidentes, essas discussões devem ser acompanhadas de considerações cuidadosas em relação a soluções de detecção automáticas de ameaças. Apesar de úteis para garantir a precisão das atividades de resposta a incidentes, delegar em maior medida à IA significa menos supervisão humana nos processos de identificação. Neste sentido, **as agências governamentais no Brasil e na UE devem continuar a promover a reflexão crítica sobre as melhores práticas para incorporar e adquirir soluções de IA para a segurança cibernética em respostas nacionais a incidentes, ações ofensivas (defesa cibernética) e atividades de aplicação da lei.**

Gills Vilar Lopes

Coordenador do Programa de Pós-Graduação em Ciências Aeroespaciais da Universidade da Força Aérea. Doutor em Ciência Política (UFPE). *Specialized Course* em *Cybersecurity* (NDU). Conselheiro Editorial da RBI/ABIN. Pesquisador Pró-Defesa IV.

Coordinator of the Postgraduate Program in Aerospace Science at the Brazilian Air Force University. PhD in Political Science (UFPE). Specialised Course in Cybersecurity (NDU).
Editorial Advisor at RBI/ABIN. Pró-Defesa IV Researcher.

Intersecções entre os domínios espacial e cibernético: implicações para o Poder Aeroespacial brasileiro

Intersections Between Space and Cyber Domains: implications for Brazilian Aerospace Power

Gills Vilar Lopes*

Sumário Executivo

A nova corrida espacial atual traz consigo antigos e novos atores, inclusive não estatais, para competir por zonas de influência, novas tecnologias e, portanto, poder no quarto domínio estratégico. Como assegurar o desenvolvimento soberano dos programas espaciais (nacionais e regionais) diante de um crescente cenário de militarização — e *weaponization* — do espaço exterior, altamente potencializado pelas ameaças cibernéticas? O presente trabalho contextualiza e analisa os principais desafios estratégicos para a chamada segurança espacial, ao mesmo tempo em que direciona suas preocupações e *cases* para as ameaças cibernéticas, tendo como foco o novo papel desempenhado e a ser desempenhado pelas forças aéreas em compreender e operar na intersecção entre os domínios espacial e cibernético. Ao final, realizam-se quatro recomendações no sentido de fortalecer e assegurar um olhar mais estratégico para esses dois domínios, especialmente no contexto europeu e latino-americano, em que pesem os novos desafios postos à força área do Brasil.

* As opiniões expressas neste trabalho são exclusivamente do seu autor e não refletem necessariamente a posição e visão das instituições a que o autor está vinculado.

Executive summary

Today, the new space race has old and new actors, including non-state actors, who compete for areas of influence, new technologies, and power in the fourth strategic domain. How to ensure the sovereign development of national and regional space programs in the face of a growing scenario of militarisation — and *weaponisation* — of outer space, which is greatly amplified by cyber threats? This article contextualises and analyses the main strategic challenges for so-called space security. It also directs concerns and cases towards cyber threats, focusing on the new role air forces play now and will play in the future in order to understand and operate at the intersection between the space and cyber domains. At the end of the article, four recommendations are made to reinforce and ensure a more strategic perspective for these two domains, especially in the European and Latin American context, considering the new challenges posed to the Brazilian Air Force.

* The opinions expressed in this article are exclusively those of the author and do not necessarily reflect the position or vision of the institutions to which the author is linked.

Introduction

The *final frontier* for the analysis and prospection of international security in the 21st certainly lies at the intersection of the space and cyber domains. Outer space[1] is constantly invaded not only by hardware — such as rockets, satellites and space stations — but also by software. Even though some assets have systems embedded in their payload, international relations and specialised literature provide evidence that there is no 100% safe system or power vacuum, not even in space. Therefore, one must think strategically about the cyber risks and vulnerabilities of space critical assets, aiming at a balance between sovereignty and national development, whether in the context of Latin American or European countries.

The issue of the *intersection* between these two war domains relates to the warning that, "Despite substantial interest in issues of cyber security and space security, too little attention has been paid to the combination of the two. And yet there are clear and critical points of *intersection*" (CHATHAM HOUSE, 2021, emphasis added). Thus, this paper seeks to describe the main findings about this intersection, contextualising them within the reality of most Latin American countries, especially Brazil, in line with the challenges faced by cybernetic and space powers, such as the United States of America (USA) and the European Union (EU).

Inversely proportional to the opportunities that present themselves with the exploration of outer space are the risks and threats inherent to this new venture *towards the stars*. Over the past five years, the geopolitics and geostrategy of the great powers have faced a second space race — also known as *New Space* —, which brings in new objectives and actors (UNAL, 2019, p. 4). This new scenario, in which great powers are fostering a veritable arms race, the security dilemma seems to bring about deep transformations in the space capacities available to State actors' strategy.

How has this militarisation of outer space impacted the art and science of war, especially for the Brazilian Air Force (FAB – acronym in Portuguese), which is responsible for developing the strategic space sector? In the Information Age, however, this question can only be fully answered if it is intertwined with the cyber domain. In this sense, this paper analyses how Latin American countries — in general, highly dependent on foreign technologies — can learn security lessons from new paradigms and cases in which great powers improve their doctrines and strategies in order to enter into "combat" and protect themselves cybernetically in outer space.

This paper is divided into three parts. The first part contextualises the problem of cyber threats that prevents States from reaching their objectives in outer space in the light of the Theory of Spacepower, of the National Defence University (NDU)[2], and the Clausewitzian concept of *Information Power*, as proposed by Lonsdale (1999). To some extent, we can see that such theorisations have found echo in command and

[1] The terms outer space, cosmic space, extra-atmospheric space, and space are synonyms. There are several definitions (KLEIN, 2006, p. 6), but we choose outer space, found in the glossaries of the Brazilian Ministry of Defence and the Brazilian Air Force, to designate the space outside the Earth's atmosphere.

[2] Academic branch of the Department of Defence (DoD) of the USA.

Introdução

A segurança internacional do século XXI certamente encontrou na intersecção dos domínios espacial e cibernético sua *fronteira final* de análise e prospecção. O espaço exterior[1] é constantemente tocado não só por *hardware* — tais como foguetes, satélites e estações espaciais —, mas também por *software*. Por mais que alguns ativos tenham sistemas embarcados em sua carga útil, as relações internacionais e a literatura especializada fornecem provas de que não existe sistema 100% seguro nem mesmo vácuo de poder, inclusive no espaço. Portanto, há que se pensar estrategicamente sobre os riscos e vulnerabilidades cibernéticos dos ativos críticos espaciais, visando ao equilíbrio entre soberania e desenvolvimento nacional, seja no contexto de países latino-americanos, seja de europeus.

A questão da *intersecção* entre esses dois domínios da guerra diz respeito ao alerta de que, "Despite substantial interest in the issues of cyber security and space security, too little attention has been paid to the combination of the two. And yet there are clear and critical points of *intersection*"3[2] (CHATHAM HOUSE, 2021, grifo nosso). Assim, busca-se aqui desvelar os principais achados dessa intersecção, contextualizando-os à realidade da maioria dos países latino-americanos, especialmente do Brasil, em consonância com os desafios enfrentados por potências cibernéticas e espaciais, como Estados Unidos da América (EUA) e União Europeia (UE).

Em uma relação inversamente proporcional às oportunidades que se apresentam com a exploração do espaço exterior, há também crescentes riscos e ameaças embutidos nessa nova empreitada *rumo às estrelas*. Nos últimos cinco anos, a geopolítica e a geoestratégia das grandes potências se defrontaram com uma segunda corrida espacial — também conhecida como *New Space* — que agrega novos objetivos e atores (UNAL, 2019, p. 4). Nesse novo cenário, em que grandes potências fomentam uma verdadeira corrida armamentista, o dilema de segurança parece produzir profundas transformações nas capacidades espaciais a serviço da Estratégia dos atores estatais.

Como essa militarização do espaço exterior tem impactado a arte e ciência da guerra, especialmente para a Força Aérea Brasileira (FA), responsável pelo desenvolvimento do setor estratégico espacial? Na Era da Informação, todavia, essa pergunta só pode ser plenamente respondida se estiver entrelaçada com o domínio cibernético. Nesse sentido, analisa-se como os países latino-americanos — em geral, altamente dependentes de tecnologias estrangeiras — podem extrair ensinamentos securitários a partir de novos paradigmas e casos em que grandes potências aperfeiçoam suas doutrinas e estratégias para "combater" e proteger-se ciberneticamente no espaço exterior.

Para tanto, este texto se subdivide em três partes. Na primeira, contextualiza-se a

[1] Os termos espaço exterior, espaço cósmico, espaço extra-atmosférico e espaço são sinônimos. Apesar de haver várias definições (KLEIN, 2006, p. 6), opta-se, aqui, por espaço cósmico, utilizado nos glossários do Ministério da Defesa e da Aeronáutica brasileiros, para designar o espaço situado fora da atmosfera terrestre.

[2] Apesar do substancial interesse pelas questões de cibersegurança e segurança especial, pouca atenção tem sido dada à combinação das duas. E, no entanto, há pontos claros e críticos de intersecção. (Tradução do Revisor)

control (C2) and strategic communications (StratCom) guidelines and operations of countries that are part of the EU and the North Atlantic Treaty Organisation (NATO), in addition to multi-domain operations around the world. The second part analyses the main political, strategic, and doctrinal landmarks of the Brazilian Aerospace Power, correlating them with what has been known, domestically, as Cybernetic and Space Strategic Sectors since 2008. Finally, the third part suggests ways to strengthen the intersection between these domains, emphasising the role of strategic bodies and documents, as well as international cooperation.

On the intersection between cybernetic and spatial domains

The maxim that there is no power vacuum in international relations also applies to outer space and cyberspace. To this end, cases are analysed in the light of the Theory of Spacepower, which raises concerns about "the ability to use space to influence others, events, or the environment to achieve one's purposes or goals. [...] spacepower manifests itself in various ways as sociocultural, economic, i*nformation, and security power*" (LUTES; HAYS, 2011, p. xiv, emphasis added). This theory draws from neoinstitutionalist Nye Jr (2011) who helps to understand contemporary international security through the various ways in which a state can use its — *hard, soft, smart,* and *cyber* — power in the 21st century.

The intersection between domains tends to further increase the fogginess of today's war, under which the most diffused interests and actors hover. Many examples of this can be seen in the creation of space forces and their strategies centred in Cyber Defence; attempts by International Space Law and the United Nations Committee on the Peaceful Uses of Outer Space (COPUOS) to legally limit cyberattacks against space assets and the development of cyber weapons as veritable space countermeasures (WEEDEN; SAMSON, 2020, p. 126-1134). Should we link these actions to traditional anti-satellite missiles (ASAT), and we would have at least an idea of the threats and risks that involve the armed forces and, in particular, the air forces.

In this perspective, outer space is the fourth strategic domain of warfare, and cyberspace, the fifth (LONSDALE, 1999). The intrinsic relationship between them (CHATHAM HOUSE, 2021) becomes increasingly visible as the 21st century progresses, especially after years of a certain lack of space prominence, with the end of the space race between Americans and Soviets, the discontinuity of important projects in this area, such as the American space shuttle, accidents with serious repercussions, and severe restrictions on national space programs. The fact is that, during this period, the great powers — such as China, the USA, and Russia — did not stop thinking strategically and putting into practice new ways of using outer space — especially the low Earth orbit (LEO)3 — to keep their national interests alive. The difference is that satellite assets now contain not only traditional intelligence, surveillance, and recognition (ISR) systems, but also logical and analogue devices against their enemy

[3] LEO comprises altitudes around 100 km and 1,200 km. However, there are other markings. Depending on the distance, the tactics to control, sabotage or destroy an orbiting space asset are different, but virtually all of them can be accessed via cyberspace.

problemática das ameaças cibernéticas para o atingimento de objetivos estatais no espaço exterior, à luz da Teoria do Poder Espacial, proveniente da *National Defense University* (NDU)[3], e do conceito clausewitziano de *Information Power*, proposto por Lonsdale (1999). Em certa medida, vê-se que tais teorizações têm encontrado eco em diretrizes e operações de comando e controle (C2) e comunicações estratégicas (StratCom) de países que fazem parte da UE e da Organização do Tratado do Atlântico Norte (OTAN), além de operações multidomínios mundo afora. Na segunda parte, analisam-se os principais marcos políticos, estratégicos e doutrinários do Poder Aeroespacial brasileiro, correlacionando-os com aquilo que, no País, se conhece, desde 2008, por Setores Estratégicos Cibernético e Espacial. Por fim, sugerem-se caminhos para fortalecer a intersecção entre esses domínios, enfatizando o papel de órgãos e documentos estratégicos, bem como a cooperação internacional.

Da Intersecção entre os domínios cibernético e espacial

A máxima de que não existe vácuo de poder nas relações internacionais também se aplica aos espaços cibernético e exterior. Para tanto, analisam-se *cases* à luz da Teoria do Poder Espacial, que lança preocupação sobre "the ability to use space to influence others, events, or the environment to achieve one's purposes or goals. [...] spacepower manifests itself in various ways as sociocultural, economic, *information, and security power*"[4] (LUTES; HAYS, 2011, p. xiv, grifo nosso). Tal teoria bebe da fonte neoinstitucionalista de Nye Jr (2011), que auxilia na compreensão da segurança internacional contemporânea por meio das diversas formas que um Estado pode utilizar seu poder – *hard, soft, smart e cyber* – no século XXI.

Nesse ponto, a intersecção entre domínios tende a aumentar ainda mais a névoa da guerra hodierna, sob a qual pairam os mais difusos interesses e atores. Exemplos disso não faltam e podem ser vislumbrados, por exemplo, com a criação de forças espaciais e suas estratégias centradas em Defesa Cibernética; tentativas de o Direito Espacial Internacional e o Committee on the Peaceful Uses of Outer Space (COPUOS) das Nações Unidas limitarem legalmente ataques cibernéticos contra ativos espaciais e desenvolvimento de armas cibernéticas como verdadeiras contramedidas espaciais (WEEDEN; SAMSON, 2020, p. 126-134). Atrelem-se essas ações aos já tradicionais mísseis antissatélites (ASAT) e teremos, pelo menos, uma noção das ameaças e riscos que envolvem as forças armadas e, em particular, as forças áreas.

Nesse prisma, o espaço exterior se configura como o quarto domínio estratégico da guerra, e o cibernético, o quinto (LONSDALE, 1999). A relação intrínseca entre eles (CHARTHAM HOUSE, 2021) fica cada vez mais visível com o passar do século XXI, especialmente após anos de certa falta de protagonismo espacial, com o fim do acirramento espacial entre norte-americanos e soviéticos, da descontinuidade de projetos importantes nessa área como o ônibus espacial americano (*space shuttle*), desastres de

[3] Braço acadêmico do Ministério da Defesa (DoD) dos Estados Unidos da América (EUA).

[4] A habilidade de usar o espaço para influenciar outros, eventos, ou o meio para atingir os próprios fins ou metas. [...] o poder espacial se manifesta de várias formas como poder sociocultural, econômico, de informação e de segurança. (Tradução do Revisor)

counterparts (UNITED STATES OF AMERICA, 2018, p. 22; 2021, p. 8), in addition to the regular concerns of ensuring the physical and logical integrity of their land, air, link, and user segments. In the literature, this state of affairs has been called *weaponisation* of space (LUTES; HAYS, 2011; SMITH, 2002), that is, a stage of animosity and disputes, above militarisation, in which powers test new weapons and tactics to control and destroy enemy space assets.

Our emphasis here is precisely on how this situation, combined with the strategic-military use of cyberspace, increasingly advances national and international security. However, this does not mean that kinetic energy weapons are no longer part of the strategic calculation. On the contrary, tests such as the explosion of China's proprietary satellites in 2007 (DOLMAN; COOPER JR, 2011, p. 106; SANGER, 2009, p. 375-378), and those of India in 2019 (WEEDEN; SAMSON, 2020, p. xvi, 5-2) have made countries begin to question the security of the main assets responsible for the interconnectivity of their space systems. Likewise, developing countries, such as Brazil, should exercise caution. Despite just having a single geostationary satellite and the best location for space launches in the world, Brazil needs to protect itself, both technically and legally, to seek its own national development.

It is in this scenario that assets in orbit, such as satellites and space stations, came to be equipped not only with defensive capacities, but also offensive ones, both to monitor and collect information (ancillary activities of space power) and to control/destroy (core activity) other critical assets (UNITED STATES OF AMERICA, 2018; UNAL, 2019, p. 6). Therefore, the *how to,* that is, the strategy to achieve this political intent (BEAUFRE, 1998), was also adapted to the space domain, but is now linked to the cybernetic component with its own intrinsic risks and threats.

The intersection between these two domains, however, has brought about profound changes in the military branch of political power, serving as a warning and fostering debate in developing countries, such as Brazil.

The Brazilian Aerospace Power at the intersection of the fourth and fifth strategic domains

Some of the most modern air forces in the world have incorporated the space and information domains in the pursuit of their political objectives and in the implementation of their (major) strategies, such as the *US Space Force*, the French *Armée de l'air et de l'espace*, and the Israeli *Air and Space Arm*. However, this debate will only make sense for countries that have not yet fully mastered these technologies if it includes the perspective of cyber security and defence of their space assets. Unlike the approach taken by major players, the outlook suggested here is a more defensive, protective, and prospective perspective on these assets, shielded, of course, against measures and soft power based on diplomacy, such as the Outer Space Treaty, ratified by the Brazilian government in 1969.

grande repercussão e fortes contingenciamentos nos programas espaciais nacionais. O fato é que, nesse período, grandes potências — como China, EUA e Rússia — não deixaram de pensar estrategicamente e pôr em prática novas formas de utilizar o espaço exterior — especialmente a órbita terrestre baixa (LEO)[5] — para manter seus interesses nacionais vivos. A diferença é que, agora, ativos satelitais passam a abrigar não apenas os tradicionais sistemas de inteligência, vigilância e reconhecimento (ISR), como também dispositivos lógicos e analógicos contra seus pares inimigos (ESTADOS UNIDOS DA AMÉRICA, 2018, p. 22; 2021, p. 8), somadas às tradicionais preocupações de assegurar a integridade física e lógica de seus segmentos terrestres, aéreos, de *link* e de usuário. A esse estado de coisas a literatura tem chamado de *weaponization* do espaço (LUTES; HAYS, 2011; SMITH, 2002), ou seja, um estágio de animosidade e disputas, superior à militarização, em que potências testam novas armas e táticas de controle e destruição de ativos espaciais do inimigo.

Nossa ênfase aqui é justamente como essa situação conjugada ao uso estratégico-militar do espaço cibernético potencializa cada vez mais a segurança nacional e internacional. Todavia, não quer dizer que armas de efeito cinético deixaram de fazer parte do cálculo estratégico. Pelo contrário, testes como a explosão de satélites próprios da China em 2007 (DOLMAN; COOPER JR, 2011, p. 106; SANGER, 2009, p. 375-378) e da Índia em 2019 (WEEDEN; SAMSON, 2020, p. xvi, 5-2) têm chamado a atenção de países que passaram a questionar o quão seguros estariam seus principais ativos responsáveis pela interconectividade de seus sistemas espaciais. Da mesma forma, devem ficar cautelosos países em desenvolvimento, a exemplo do Brasil, que, embora possua um único satélite geoestacionário e a melhor localização para lançamentos espaciais do mundo, necessita de igual proteção, seja ela técnica, seja jurídica para buscar o seu próprio desenvolvimento nacional.

É nesse cenário que ativos em órbita, como satélites e estações espaciais, passam a ser equipados com capacidades não mais somente defensivas, como também ofensivas, tanto para vigiar e coletar informações (atividade-meio do poder espacial) quanto para controlar/destruir (atividade-fim) outros ativos críticos (ESTADOS UNIDOS DA AMÉRICA, 2018; UNAL, 2019, p. 6). Portanto, o *como fazer*, ou seja, a Estratégia para atingir esse intento político (BEAUFRE, 1998), também foi adaptado ao domínio espacial, só que agora atrelado à componente cibernética que já traz seus próprios riscos e ameaças.

A intersecção entre esses dois domínios, no entanto, tem provocado profundas transformações no braço armado do poder político, servindo de alerta, inclusive, para o debate em países em desenvolvimento, como o Brasil.

[5] LEO compreende altitudes em torno de 100 km e 1.200 km. Porém, há outras marcações. A depender da distância, as táticas para controlar, sabotar ou destruir um ativo espacial em órbita são diferentes, embora em praticamente todas seja possível acessar via espaço cibernético.

Unlike other armed forces, Brazil chose to intertwine the domains of Air and Space, amalgamating them into the Aerospace Power, understood as:

> [...] the projection of National Power resulting from the integration of the National resources available to use airspace and outer space, either as an instrument of political and military action, or as a factor of economic and social development, aiming at achieving and maintaining National goals. (BRAZIL, 2020a, p. 11-12)

In addition to the FAB itself, other elements constitute the Brazilian Aerospace Power, such as aerospace infrastructure, civil aviation, the aerospace and defence industry, and the human resources specialised in aerospace activity (BRAZIL, 2020a, p. 29-30). Therefore, the Aerospace Military Power is the military part of this greater power, leaving certain areas and responsibilities to other bodies, including those outside the Ministry of Defence, such as the Brazilian Space Agency (AEB – acronym in Portuguese), responsible for the Brazilian Space Program (PEB - acronym in Portuguese), and the Brazilian Institutional Security Cabinet (GSI - acronym in Portuguese), responsible for coordinating Cyber Security in Brazil. Consequently, because of its dual nature, the development of space activities in the country also involves the FAB, especially when the space assets involved concern the safeguarding of national sovereignty and integrity.

Since 2008, when the nuclear, cybernetic, and space strategic sectors were created, the FAB has been responsible for developing the Space Sector (BRAZIL, 2016, p. 30). In the past decade, there have been significant changes regarding the Preparation and Employment of Force, taking into account new space actors, the natural reformulation of the doctrine that now emphasises the intersection between cyber and outer spaces, and the creation of the Military Cyber Defence System (SMDC - acronym in Portuguese) and the Strategic Space Systems Program (PESE - acronym in Portuguese).

Although the Army is responsible for coordinating the strategic cyber sector, the other armed forces have their own inherent capabilities in this area. Cyberattack, exploitation, and protective actions (BRAZIL, 2014, p. 23-24, 30) are coordinated at the strategic level by the Cyber Defence Command (ComDCiber - acronym in Portuguese). The Air Force Cyber Defence Centre (CDCAer - acronym in Portuguese) is soon to become operational. On it lay the main expectations around the strategic intersection of the cyber and space domains in Brazil. These expectations are due to the expertise acquired by the Space Operations Centre (COPE - acronym in Portuguese), which is responsible for the cyber protection of the Geostationary Defence and Strategic Communications Satellite (SGDC - acronym in Portuguese).

It is also important to mention the role of the GSI as the coordinating body for Cyber Security policies and Intelligence Activity in Brazil. The GSI acts at the political level, but its documents and policies guide activities essential to the security of Brazilian society and State are consistent with our concerns, as they touch on the country's critical space assets. This is the case of the National Cybersecurity Strategy (E-Ciber - acronym in Portuguese), the first of five modules that make up the National Information Security

O Poder Aeroespacial brasileiro frente à intersecção dos quarto e quinto domínios estratégicos

Algumas das mais modernas forças aéreas do mundo têm incorporado os domínios espacial e informacional na busca por seus objetivos políticos e na consecução de suas (grandes) estratégias, a exemplo da *US Space Force*, da *Armée de l'air et de l'espace* francesa e da *Air and Space Arm* israelense. Mas tal discussão só fará sentido para países que não detêm o domínio completo dessas tecnologias se for envolta na perspectiva da Segurança e da Defesa Cibernéticas dos seus ativos espaciais. Logo, ao contrário da atuação de grandes *players*, a posição aqui levantada é pela perspectiva defensiva, protetiva e prospectiva desses ativos, resguardadas logicamente contra medidas e *soft power* baseados na diplomacia, como o Tratado do Espaço Cósmico, ratificado pelo governo brasileiro em 1969.

Diferentemente de outras forças armadas, o Brasil opta por entrelaçar o domínio do Ar e do Espaço, amalgamando-os no chamado Poder Aeroespacial, entendido como:

> [...] a projeção do Poder Nacional resultante da integração dos recursos de que a Nação dispõe para a utilização do espaço aéreo e do espaço exterior, quer como instrumento de ação política e militar, quer como fator de desenvolvimento econômico e social, visando conquistar e manter os objetivos nacionais. (BRASIL, 2020a, p. 11-12)

Além da própria FAB, outros elementos constituem o Poder Aeroespacial brasileiro, como a infraestrutura aeroespacial, a aviação civil, a indústria aeroespacial e de defesa e os recursos humanos especializados na atividade aeroespacial (BRASIL, 2020a, p. 29-30). Portanto, o Poder Militar Aeroespacial compreende a parte militar desse poder maior, deixando áreas e responsabilidades para outros órgãos, inclusive fora da administração do Ministério da Defesa, como é o caso da Agência Espacial Brasileira (AEB), responsável pelo Programa Espacial Brasileiro (PEB), e do Gabinete de Segurança Institucional da Presidência da República (GSI), responsável pela coordenação da Segurança Cibernética no Brasil. Assim, devido à sua natureza dual, o desenvolvimento das atividades espaciais no País passa também pela FAB, sobretudo quando os ativos espaciais envolvidos disserem respeito à salvaguarda da soberania e integridade nacional.

Com a criação em 2008 dos Setores Estratégicos — nuclear, cibernético e espacial —, coube à FAB o desenvolvimento do Setor Espacial (BRASIL, 2016, p. 30). Deste então, houve mudanças significativas em relação ao Preparo e Emprego da Força, levando em conta a inclusão de novos atores espaciais, a natural reformulação da doutrina que passou a enfatizar a intersecção entre espaços cibernético e exterior e a criação do Sistema Militar de Defesa Cibernética (SMDC) e do Programa Estratégico de Sistemas Espaciais (PESE).

Apesar de o Exército ser o responsável por coordenar o Setor Estratégico Cibernético, as demais Forças possuem suas próprias e inerentes capacidades nessa área. Não obstante as ações cibernéticas de ataque, exploração e proteção (BRASIL, 2014, p. 23-24, 30) serem coordenadas no nível estratégico pelo Comando de Defesa Cibernética (ComDCiber), aguarda-se a ativação do Centro de Defesa Cibernética da Aeronáutica (CDCAer), em que residirão as principais expectativas em torno da intersecção estratégica dos domínios cibernético e espacial no Brasil, haja vista a expertise já adquirida

Strategy (ENSI - acronym in Portuguese). Another two modules are still to be created for Cyber Defence and the security of critical infrastructures.

As stated, the human resources specialised in aerospace activities are also part of the Brazilian Aerospace Power (BRAZIL, 2020a, p. 30). When the Cybernetic and Space Strategic Sectors are analysed jointly, three options seem to point to the Triple Helix of innovation: education (university), training (government) and acquisition (business) of specialised human resources. In addition to the events and courses coordinated by ComDCiber, by the National School of Cyber Defence (ENaDCiber - acronym in Portuguese) and by the GSI, we would like to highlight the latest actions by Embraer Defence & Security, which plays a key role in these two domains and provides the FAB with modern aircraft, such as the KC-390, and with products and services aimed at ISR, C2, and space systems (EMBRAER, 2021). Therefore, it is not surprising to see Embraer join the Cyber Security sector, taking over Tempest, a leading company in the sector in Brazil, and investing R$ 20 million in Kryptus, a provider of encryption solutions for the Brazilian armed forces, as Gielow (2020) points out. He also emphasises the inter-domain relationship highlighted in this paper by stating that the space market "[...] goes hand in hand with the cybersecurity market [...]. After all, everything goes through satellites".

Final Considerations and Recommendations

As much as Latin American and European states are committed to defending peace and the peaceful solution of conflicts, the fact is that the military use of cyber and outer spaces brings security concerns driven by cyber threats. Therefore, it is essential to examine both domains from an intersectional perspective in order to better situate the new strategic concerns of current air forces.

Cyberspace challenges are related not only to the security of the few critical assets that developing countries possess, but also to the correct advancement of space projects by developed countries, as seen respectively in Latin American and European scenarios. So, finding out about what *really* happens in the world — or rather, above it — seems to be a new topic on the current international security agenda. Those who do not promote studies and debates at the intersection of these environments will certainly be failing to open a window of opportunity to exercise their space power.

From what has been seen so far, it becomes evident that apparently isolated cases, such as ASAT missile tests or cyberattacks against space assets, should be understood as part of a bigger picture that allows for more accurate decision-making concerning what is currently found in international security. And this is not done only by technicians and tactics, but also by interdisciplinary teams that can dispel the fog of war to the fullest degree and bring to light the many variables that make up the new battlefields. Accordingly, today, a comprehensive definition of space power permeates other areas and centres of gravity that are not exclusively military barracks. They include strategic domains no longer in isolation, but that intersect, as suggested here.

pelo Centro de Operações Espaciais (COPE), por meio da proteção cibernética do Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC).

Merece menção também o papel do GSI enquanto órgão coordenador das políticas de Segurança Cibernética e da Atividade de Inteligência no Brasil. Embora atue no nível político, seus documentos e políticas norteadoras de atividades essenciais à segurança da sociedade e Estado brasileiros se mostram condizentes com nossas preocupações, pois tocam os ativos críticos espaciais do País. É o caso da Estratégia Nacional de Segurança Cibernética (E-Ciber), primeiro de cinco módulos que compõem a Estratégia Nacional de Segurança da Informação (ENSI), no que se destacam aqui os módulos ainda a serem criados da Defesa Cibernética e da segurança das infraestruturas críticas.

Como dito, os recursos humanos especializados na atividade aeroespacial são também partes integrantes do Poder Aeroespacial brasileiro (BRASIL, 2020a, p. 30). Nesse prisma, quando analisamos conjuntamente os Setores Estratégicos Cibernético e Espacial, três opções parecem apontar para Tríplice Hélice da inovação: formação (universidade), capacitação (governo) e aquisição (empresa) de recursos humanos especializados. Ademais dos eventos e cursos coordenados pelo ComDCiber, pela Escola Nacional de Defesa Cibernética (ENaDCiber) e pelo GSI, destacamos aqui as últimas ações da Embraer Defesa & Segurança, que, por sinal, desempenha papel fulcral nesses dois domínios e fornece à FAB, além de modernos aviões como o KC-390, produtos e serviços voltados a ISR, C2 e sistemas espaciais (EMBRAER, 2021). Diante disso, não surpreende a recente entrada da Embraer no setor de Segurança Cibernética, passando a controlar a Tempest, empresa líder no segmento no País, e investindo R$ 20 milhões na Kryptus, fornecedora de soluções de criptografia para as forças armadas brasileiras, como aponta Gielow (2020), o qual, inclusive, reforça a relação interdomínios enfatizada neste *paper* ao afirmar que o mercado espacial "[...] anda de mãos dadas ao de cibersegurança [...]. Afinal de contas, tudo passa por satélites".

Se tudo passa por satélites, então nada mais óbvio do que buscar fortalecer capacidades e habilidades que podem pôr em risco o desenvolvimento das atividades espaciais, especialmente em contexto de superação de dependências por meio de cooperação internacional e parcerias estratégicas, como se vê a seguir.

Considerações Finais e Recomendações

Por mais que Estados latino-americanos e europeus estejam compromissados com a defesa da paz e a solução pacífica dos conflitos, o fato é que o uso militar dos espaços cibernético e cósmico traz consigo preocupações securitárias impulsionadas pelas ameaças cibernéticas. Portanto, um olhar interseccional entre ambos os domínios se faz (e se mostra) imprescindível para melhor situar as novas preocupações estratégicas das atuais forças aéreas.

Os desafios ciberespaciais, por assim dizer, estão relacionados não apenas à segurança dos poucos ativos críticos de que dispõem países em desenvolvimento, como também ao correto andamento de projetos espaciais por parte de países desenvolvidos, realidades latino-americana e europeia, respectivamente. Assim, inteirar-se acerca do que

From a Latin American standpoint, thinking about the domains of war in an increasingly combined way seems to be a path already outlined by the FAB in the latest update of its military doctrine in 2020 (BAPTISTA JUNIOR, 2021, p. 6), so that CDCAer can finally consolidate this perspective. It is clear to EU Member States, which have a very competitive space agency, that space *weaponisation* is more of a threat than an opportunity. Strengthening this position with the United Nations and NATO is inevitable, as is strengthening ties with friendly nations to allow speaking with one voice.

Given the evidence provided so far, some recommendations can be proposed, aiming at an effective intersection between the cyber and space domains:

1. *educating, training, and acquiring human resources*: key elements to develop the two domains, which must work in tandem; an emphasis is placed on interdisciplinary training. Exchanges with other institutions with more expertise would accelerate this process. For Latin American governments, and in particular Brazil, the NATO Centres of Excellence — especially the CCDCOE — are certainly a starting point. There should also be incentives and academic exchange via specific topics in Government calls for research proposals to promote technological and political research, such as Pró-Defesa, PROCAD-Defesa and Pró-Estratégia;

2. *strengthening international cooperation in defence*: literature and case analysis alone will not lead to expertise in the area. Therefore, it is recommended that ties be strengthened with air forces — and space forces, such as the USSF — that possess state-of-the-art cybernetics and space technology and that have already deployed them on the battlefield. This becomes an interfering variable for both Latin American and European countries. We understand that reinforcing these aspects would be the first step towards the stars. In Brazil, this step would come at the most opportune moment possible for the FAB, with the CDCAer becoming operational in the future;

3. *reviewing the current Brazilian E-Ciber and reinforcing the emphasis on the intersection of the two strategic domains in the future National Cyber Defence Strategy*: this task — which seems to be the least difficult one — falls on the already broad shoulders of the GSI and aims at including critical space assets in its infrastructure protection scope and at capturing the spirit of the New Space and militarisation of space. There is also a special provision or section on the need for research in grey areas of the two domains to serve as a legal parameter for future strategic programs and call for research proposals; and

4. *strengthening a position against space weaponisation*: certainly, UNCOPOUS is the most suitable forum for each State to be represented in, with the purpose of promoting this issue. For developing countries such as Brazil, this action would legally safeguard their few space assets in orbit and those to come — such as the Catarina and Lessônia constellations — from foreign interference. For developed countries, such as EU countries, it would allow for further development of their space projects, thus guaranteeing a larger share in the New Space market, as it is no coincidence

realmente ocorre no mundo — ou melhor, acima dele —, parece constituir-se como um novo tópico da agenda da segurança internacional atual. Quem não iniciar estudos e debates na intersecção desses ambientes, certamente, estará deixando de abrir uma janela de oportunidades para exercitar seu poder espacial.

Pelo que foi exposto até aqui, fica evidente que os casos aparentemente isolados, como testes de mísseis ASAT ou ataques cibernéticos contra ativos espaciais, devem ser postos em um quadro maior que possibilite tomadas de decisão mais precisas em relação ao que se observa atualmente na segurança internacional. E isso não é feito apenas por técnicos e táticas, mas também com uma equipe interdisciplinar que consiga afastar, ao máximo, a névoa da guerra e trazer à tona as diversas variáveis que compõem os novos campos de batalha. Assim, a definição abrangente de poder espacial perpassa, hoje, por áreas e centros de gravidade outros que não são exclusivamente a caserna e que abarcam os domínios estratégicos não mais de forma isolada, e sim interseccional, como se defende aqui.

Do ponto de vista latino-americano, pensar os domínios da guerra cada vez de forma mais combinada parece ser um caminho já esboçado pela FAB na última atualização de sua doutrina militar em 2020, nas palavras de seu Comandante (BAPTISTA JUNIOR, 2021, p. 6) para que o CDCAer possa, enfim, consolidar tal perspectiva. Aos Estados-membros da UE, que, por sinal, possuem uma agência espacial bastante competitiva, fica patente como a *weaponization* do espaço é mais uma ameaça do que oportunidade, tornando-se inevitável o fortalecimento dessa posição junto às Nações Unidas e à OTAN, bem como o fortalecimento de laços com nações amigas para unir vozes.

Diante das evidências levantadas até aqui, algumas recomendações podem ser vislumbradas, visando a uma efetiva intersecção entre os domínios cibernético e espacial:

1. *formar, capacitar e adquirir recursos humanos:* elementos-chave para o desenvolvimento dos dois domínios, mas que devem ser pensados em harmonia, não isolados; assim, a ênfase recai sobre uma formação interdisciplinar, na qual o intercâmbio com outras instituições com mais expertise aceleraria tal processo. Para os governos latino-americanos, e em especial o Brasil, certamente, os Centros de Excelência da OTAN — especialmente o CCDCOE — são um ponto de partida, bem como o incentivo e intercâmbio acadêmico por meio de tópicos específicos em Editais de fomento à pesquisa tecnológica e política, como Pró-Defesa, PROCAD-Defesa e Pró-Estratégia;

2. *fortalecer a cooperação internacional em defesa*: não há como obter expertise nessa área apenas por meio da literatura e análise da casuística. Assim, recomenda-se fortalecer laços com forças aéreas — e espaciais, como a USSF – que detêm o estado da arte cibernética e espacial e que já o empregaram no campo de batalha. Isso se torna uma variável interveniente tanto para países latino-americanos quanto europeus. Entende-se que o fortalecimento desses aspectos seria o primeiro passo rumo às estrelas de forma segura. No Brasil, esse passo viria no momento mais oportuno possível para FAB, com a futura ativação do CDCAer;

3. *revisar a atual E-Ciber brasileira* e *reforçar a ênfase na intersecção dos dois domínios estratégicos na futura Estratégia Nacional de Defesa Cibernética*: essa tarefa — que, a nosso ver, parece ser a menos difícil — recai sob os ombros já largos do GSI e vem no

that outer space is already considered the "new economic centre of gravity" (CAHAN; SADAT, 2021, p. 11). Hence the need to strengthen Brazilian smart power both in the military and in the diplomatic sectors, aiming also at the economic level, but always in the light of the Nation's political objectives.

Therefore, at the intersection of space and cyberspace, air forces find risks and threats consistent with the magnitude of the geopolitical, economic, and military relevance involved in these strategic domains. In order to fight them better, we need to anticipate their actions.

AD ASTRA ET ULTRA!

References

BAPTISTA JUNIOR, Carlos de A. **Diretriz do Comandante da Aeronáutica 2021-2022**. Brasília, DF: COMAER, 2021. Available at: http://issuu.com/portalfab/docs/diretriz_do_comandante_2021_2022. Accessed: 9 Jun. 2021.

BEAUFRE, André. **Introdução à estratégia.** Translated by: Luiz de A. Araripe. Rio de Janeiro: Biblioteca do Exército, 1998. (Coleção General Benício, v. 336).

BRAZIL. Comando da Aeronáutica. **DCA 1-1**: Doutrina básica da Força Aérea Brasileira. Brasília, DF: EMAER, 2020a. v. I.

BRAZIL. Ministério da Defesa. **MD31-M-08:** Doutrina Militar de Defesa Cibernética. Brasília, DF: EMCFA, 2014. Available at: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31a_ma_08a_defesaa_ciberneticaa_1a_2014.pdf. Accessed: 17 May 2021.

BRAZIL. Ministério da Defesa. **Política Nacional de Defesa / Estratégia Nacional de Defesa**. 2. ed. Brasília, DF: Ministério da Defesa, 2016. Available at: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/PNDeEND_V.MD.10VersoencaminhadaaoCongressoNacionalem24Nov16.pdf. Accessed: 26 May 2021.

CAHAN, Bruce; SADAT, Mir H. **Space policies for the New Space Age: competing on the final economic frontier.** Albuquerque, NM: NewSpace New Mexico, 2019. Available at: https://www.newspacenm.org/wp-content/uploads/2021/01/US-Space-Policies-for-the-New-Space-Age-Competing-on-the-Final-Economic-Frontier-010621-final.pdf. Accessed: 24 May 2021.

CHATHAM HOUSE. Cyber and space security. 2021. Available at: https://www.chathamhouse.org/about-us/our-departments/international-security-programme/cyber-and-space-security. Accessed: 30 May 2021.

DOLMAN, Everett C.; COOPER JR, Henry. Increasing the military uses of space. In: LUTES, Charles D.; HAYS, Peter L. (ed.). **Toward a theory of spacepower:** selected essays. Washington, DC: NDU Press, 2011. cap. 5, p. 97-117.

EMBRAER. Defesa & segurança. 2021. Available at: https://www.embraer.com/br/pt/defesa-e-seguranca. Accessed: 14 May 2021.

sentido de incluir tanto os ativos críticos espaciais em seu escopo de proteção infraestrutural quanto para captar o espírito do tempo do New Space e da militarização do espaço. Cabendo também um dispositivo ou seção especial sobre a necessidade de pesquisas em zonas cinzentas dos dois domínios, para servir de parâmetro legal a futuros programas estratégicos e editais de fomento; e

4. *fortalecer o posicionamento contra a weaponization do espaço:* certamente o fórum mais adequado para este pleito seria junto à representação de cada Estado no UNCOPOUS. Aos países em desenvolvimento, como o Brasil, esta ação salvaguardaria legalmente seus poucos ativos espaciais em órbita e aqueles vindouros — como as constelações Catarina e Lessônia — de interferências estrangeiras. E, aos países desenvolvidos, como os da UE, possibilitaria desenvolver ainda mais seus projetos espaciais, no sentido de garantir uma fatia maior no mercado do New Space, pois não é à toa que o espaço exterior já é considerado o "new economic center of gravity" da atualidade (CAHAN; SADAT, 2021, p. 11). Daí a necessidade de fortalecimento do *smart power* brasileiro tanto no setor militar quanto diplomático, visando, inclusive, o econômico, mas sempre à luz dos objetivos políticos da Nação.

Como se vê, as forças aéreas encontram na intersecção dos espaços espacial e cibernético riscos e ameaças condizentes com o tamanho da importância geopolítica, econômica e militar que envolvem tais domínios estratégicos. Para melhor combatê-los, é preciso antevê-los.

AD ASTRA ET ULTRA!

Referências

BAPTISTA JUNIOR, Carlos de A. **Diretriz do Comandante da Aeronáutica 2021-2022**. Brasília, DF: COMAER, 2021. Disponível em: http://issuu.com/portalfab/docs/diretriz_do_comandante_2021_2022. Acesso em: 9 jun. 2021.

BEAUFRE, André. **Introdução à estratégia**. Tradução: Luiz de A. Araripe. Rio de Janeiro: Biblioteca do Exército, 1998. (Coleção General Benício, v. 336).

BRASIL. Comando da Aeronáutica. **DCA 1-1:** Doutrina básica da Força Aérea Brasileira. Brasília, DF: EMAER, 2020a. v. I.

BRASIL. Ministério da Defesa. **MD31-M-08:** Doutrina Militar de Defesa Cibernética. Brasília, DF: EMCFA, 2014. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31a_ma_08a_defesaa_ciberneticaa_1a_2014.pdf. Acesso em: 17 maio 2021.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa / Estratégia Nacional de Defesa**. 2. ed. Brasília, DF: Ministério da Defesa, 2016. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/PNDeEND_V.MD.10VersoencaminhadaaoCongressoNacionalem24Nov16.pdf.
Acesso em: 26 maio 2021.

GIELOW, Igor. Embraer diversifica e entra no mercado de segurança cibernética. Folha de S. Paulo, 30 jun. 2020. Mercado. Available at: https://www1.folha.uol.com.br/mercado/2020/06/embraer-diversifica-e-entra-no-mercado-de-seguranca-cibernetica.shtml. Accessed: 27 May 2021.

KLEIN, John J. **Space warfare:** strategy, principles and policy. London: Routledge, 2006. (Space power and politics, 1).

LONSDALE, David J. Information power: strategy, geopolitics, and the fifth dimension. **Journal of Strategic Studies**, v. 22, n. 2-3, p. 137-157, 1999. Available at: http://dx.doi.org/10.1080/01402399908437758. Accessed: 18 May 2021.

LUTES, Charles D.; HAYS, Peter L. (ed.). **Toward a theory of spacepower**: selected essays. Washington, DC: NDU Press, 2011.

NYE JR, Joseph S. **The future of power**. New York: Public Affairs, 2011.

SANGER, David E. **The inheritance:** the world Obama confronts and the challenges to American power. Nova York, Harmony Books, 2009.

SMITH, M. V. **Ten propositions regarding spacepower.** Alabama: Air University Press, 2002.

UNAL, Beyza. Cybersecurity of NATO's space-based strategic assets. **Chatham House Research Paper**, London, July 2019. Available at: https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf. Accessed: 29 May 2021.

UNITED STATES OF AMERICA. Director of National Intelligence. **Annual Threat Assessment of the Intelligence Community**. Washington, DC: DNI, 2021. Available at: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf. Accessed: 14 May 2021.

UNITED STATES OF AMERICA. U.S. Air Force. **Competing in space.** Dayton, OH: National Air and Space Intelligence Center Public Affairs, 2018. Available at: https://media.defense.gov/2019/Jan/16/2002080386/-1/-1/1/190115-F-NV711-0002.PDF. Accessed: 30 May 2021.

WEEDEN, Brian; SAMSON, Victoria (ed.). **Global Counterspace and capabilities: an open source assessment**. Broomfield, CO: Secure World Foundation, 2020. Available at: https://swfound.org/media/206970/swf_counterspace2020_electronic_final.pdf. Accessed: 22 May 2021.

CAHAN, Bruce; SADAT, Mir H. **Space policies for the New Space Age: competing on the final economic frontier.** Albuquerque, NM: NewSpace New Mexico, 2019. Disponível em: https://www.newspacenm.org/wp-content/uploads/2021/01/US-Space-Policies-for-the-New-Space-Age-Competing-on-the-Final-Economic-Frontier-010621-final.pdf. Acesso em: 24 maio 2021.

CHATHAM HOUSE. Cyber and space security. 2021. Disponível em: https://www.chathamhouse.org/about-us/our-departments/international-security-programme/cyber-and-space-security. Acesso em: 30 maio 2021.

DOLMAN, Everett C.; COOPER JR, Henry. Increasing the military uses of space. In: LUTES, Charles D.; HAYS, Peter L. (ed.). **Toward a theory of spacepower:** selected essays. Washington, DC: NDU Press, 2011. cap. 5, p. 97-117.

EMBRAER. Defesa & segurança. 2021. Disponível em: https://www.embraer.com/br/pt/defesa-e-seguranca. Acesso em: 14 maio 2021.

ESTADOS UNIDOS DA AMÉRICA. Director of National Intelligence. **Annual Threat Assessment of the Intelligence Community.** Washington, DC: DNI, 2021. Disponível em: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf. Acesso em: 14 maio 2021.

ESTADOS UNIDOS DA AMÉRICA. U.S. Air Force. **Competing in space.** Dayton, OH: National Air and Space Intelligence Center Public Affairs, 2018. Disponível em: https://media.defense.gov/2019/Jan/16/2002080386/-1/-1/1/190115-F-NV711-0002.PDF. Acesso em: 30 maio 2021.

GIELOW, Igor. Embraer diversifica e entra no mercado de segurança cibernética. Folha de S. Paulo, 30 jun. 2020. Mercado. Disponível em: https://www1.folha.uol.com.br/mercado/2020/06/embraer-diversifica-e-entra-no-mercado-de-seguranca-cibernetica.shtml. Acesso em: 27 maio 2021.

KLEIN, John J. **Space warfare:** strategy, principles and policy. Londres: Routledge, 2006. (Space power and politics, 1).

LONSDALE, David J. Information power: strategy, geopolitics, and the fifth dimension. **Journal of Strategic Studies**, v. 22, n. 2-3, p. 137-157, 1999. Disponível em: http://dx.doi.org/10.1080/01402399908437758. Acesso em: 18 maio 2021.

LUTES, Charles D.; HAYS, Peter L. (ed.). **Toward a theory of spacepower:** selected essays. Washington, DC: NDU Press, 2011.

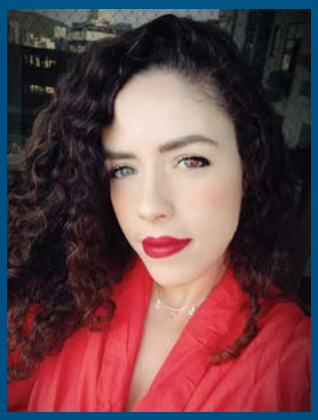
NYE JR, Joseph S. **The future of power.** New York: Public Affairs, 2011.

SANGER, David E. **The inheritance:** the world Obama confronts and the challenges to American power. Nova York, Harmony Books, 2009.

SMITH, M. V. **Ten propositions regarding spacepower.** Alabama: Air University Press, 2002.

UNAL, Beyza. Cybersecurity of NATO's space-based strategic assets. **Chatham House Research Paper**, Londres, jul. 2019. Disponível em: https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf. Acesso em: 29 maio 2021.

WEEDEN, Brian; SAMSON, Victoria (ed.). **Global Counterspace and capabilities: an open source assessment.** Broomfield, CO: Secure World Foundation, 2020. Disponível em: https://swfound.org/media/206970/swf_counterspace2020_electronic_final.pdf. Acesso em: 22 maio 2021.



Bruna Jaeger

Doutora em Economia Política Internacional (UFRJ), mestre em Estudos Estratégicos Internacionais (UFRGS) e professora do curso de Relações Internacionais (UniLaSalle-RJ). É pesquisadora-associada do Instituto Sul-Americano de Política e Estratégia (ISAPE). Contato: brunacjaeger@gmail.com

PhD in International Political Economy (UFRJ), MA in International Strategic Studies (UFRGS), and Lecturer in the International Relations undergraduate course (UniLaSalle-RJ). Research Associate at the South American Institute for Policy and Strategy (ISAPE) Contact: brunacjaeger@gmail.com

Conectividade estratégica através de cabos de fibra óptica: uma análise securitária sul-americana

Strategic Connectivity through Fibre Optic Cables: a South American Security Analysis

Bruna Coelho Jaeger

Sumário Executivo

O presente *policy paper* tem como tema as tecnologias de informação e comunicação (TICs) na América do Sul, com enfoque na questão securitária da rede de cabos de fibra óptica no subcontinente. O objetivo central, portanto, é discutir as vulnerabilidades, desafios e perspectivas de cooperação que se abrem a partir da conectividade estratégica sul-americana. O tema encontra justificativa no papel fulcral das TICs a partir da crescente digitalização da segurança internacional e da sua imprescindibilidade ao planejamento estratégico. A América do Sul apresenta 33 cabos submarinos que conectam a comunicação digital da região com o resto do mundo. Destes, 31 passam pelos EUA e apenas dois pela Europa. Assim, há uma centralidade do controle das telecomunicações sul-americanas a partir de empresas extrarregionais.

Como alternativa aos desafios gerados por essa dependência, em 2012, foi lançado no âmbito da União de Nações Sul-Americanas (UNASUL) o projeto "Anel Óptico Sul-Americano", uma rede de mais de 10.000 km de cabos terrestres de fibra óptica,

Executive Summary

The theme of this policy paper is information and communication technologies (ICTs) in South America with a special focus on the security of the subcontinent's fibre optic cable network. Therefore, its main objective is to discuss the cooperation vulnerabilities, challenges and perspectives that stem from South American strategic connectivity. The rationale behind the theme is the pivotal role of ICTs in the growing digitization of international security and its indispensability for strategic planning. South America has 33 submarine cables that connect the region's digital communication with the rest of the world. Thirty-one of these cables pass through the USA and only two through Europe. Thus, the control of South American telecommunications is centred in extra-regional companies.

As an alternative to the challenges brought by this dependence, the "South American Optical Ring" (2021) project was launched within the scope of the Union of South American Nations (UNASUR). The ring is comprised of a network of more than 10,000 km of terrestrial fibre optic cables

that aims at autonomously connecting the region's broadband internet. However, the project has made little progress. The UNASUR crisis and the role of the Brazilian regional leadership are at the heart of the problem. Therefore, it is important to discuss the current state of strategic connectivity from fibre optic cables in South America, its vulnerabilities, and possibilities for cooperation. This paper proposes an institutional reorganization of South American integration as an indispensable resolution, as well as the reduction of the dependence on the USA by fostering interconnection with other regions, especially Europe.

Context and importance of the problem: dependence and vulnerability of South American telecommunications

Since the inception of the Initiative for the Integration of Regional Infrastructure in South America (IIRSA) in 2000, ICTs have been defined as one of the fundamental strategic objectives of regional physical integration, together with transport and energy (IIRSA, 2004). However, the telecommunications sector has always been under-represented in annual plans. In IIRSA's last portfolio (2010), there were nine projects in this area, corresponding to 1.7% of the portfolio and 4.6% of total investments. Approximately 90% of these were fibre optic projects. In 2011, with the new organizational structure of the South American Infrastructure and Planning Council (COSIPLAN) and within the scope of UNASUR, the Working Group on Telecommunications was created. In COSIPLAN's Strategic Action Plan (2012-2022), objective 5 is to "Foster intensive Information and Communication Technology use, in order to overcome geographic and operational barriers in the region", and specific objective 5.3 is to "Stimulate projects to promote regional integration in South America through the use of Information and Communication Technology (ICT) tools" (COSIPLAN, 2011, p. 10).

South America is characterized by a wide disparity in the access to technologies. The countries with the highest number of personal computers in the region are Uruguay, Argentina and Chile, those being present in 67%, 62% and 60% of homes, respectively (WEF, 2016). In more populous countries, such as Brazil, this number is 38%. Currently, there is a complex network of 244 submarine fibre optic cables connecting the entire world. The Atlantis-2 is the main cable between South America and Europe. Brazil is developing other four cable systems: South Atlantic Express (SAEx), South Atlantic Cable System (SACS), Cameroon-Brazil Cable System (CBCS), and EllaLink. The latter is being developed with Europe and will be presented later. The map below shows the seven main submarine fibre optic networks connecting South America.

com o objetivo de conectar a internet banda larga da região de forma autônoma. No entanto, o projeto teve poucos avanços. A crise da UNASUL e do papel da liderança regional brasileira encontram-se no centro do problema. Nesse sentido, discute-se o atual estado da conectividade estratégica a partir de cabos de fibra óptica na América do Sul, suas vulnerabilidades e possibilidades de cooperação. Frente a isto, este paper propõe a reorganização institucional da integração sul-americana como resolução indispensável, bem como a redução da dependência dos EUA a partir do fomento da interconexão com outras regiões, especialmente a Europa.

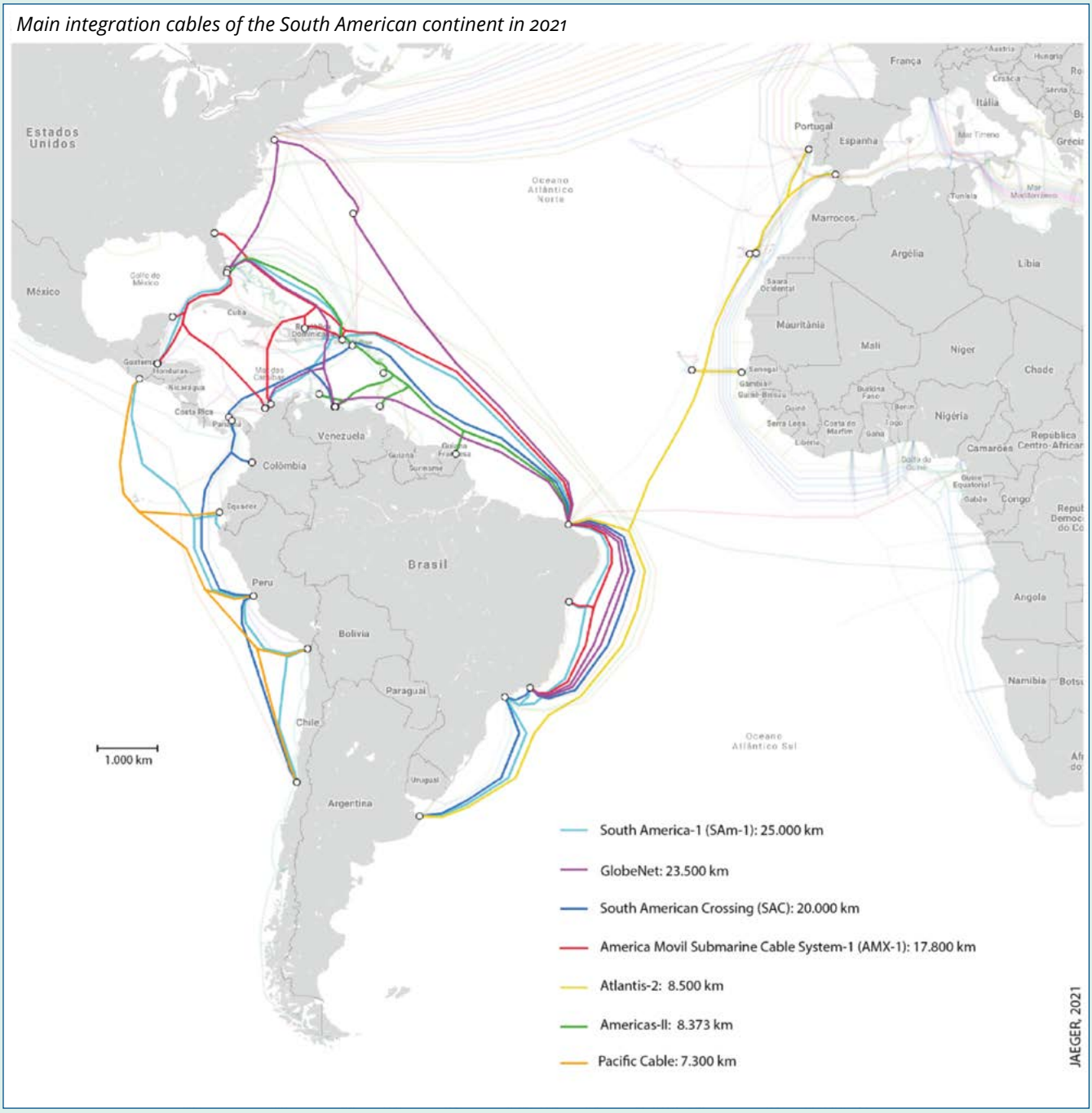
Contexto e importância do problema: dependência e vulnerabilidade das telecomunicações sul-americanas

Desde a formação da Iniciativa para Integração da Infraestrutura Regional Sul-Americana (IIRSA), em 2000, as TICs são definidas como um dos objetivos estratégicos fundamentais da integração física regional, juntamente com transportes e energia (IIRSA, 2004). No entanto, o setor de telecomunicações sempre foi sub-representado nas planificações anuais. Na última carteira da IIRSA, de 2010, os projetos dessa área eram nove, correspondendo a 1,7% da carteira e 4,6% dos investimentos totais. Destes projetos, cerca de 90% correspondiam a empreendimentos de fibra óptica. Em 2011, com a nova estrutura organizacional do Conselho Sul-Americano de Infraestrutura e Planejamento (COSIPLAN), no âmbito da UNASUL, foi criado o Grupo de Trabalho de Telecomunicações. No Plano de Ação Estratégica do COSIPLAN (2012-2022), o objetivo nº 5 é "fomentar o uso intensivo de Tecnologias de Informação e Comunicação, com a finalidade de ultrapassar barreiras geográficas e operacionais na região", sendo o objetivo específico 5.3 "impulsionar projetos que promovam a integração regional sul-americana através do uso de ferramentas de TICs" (COSIPLAN, 2011, p. 10).

A América do Sul se caracteriza por amplas disparidades no acesso a tecnologias. Os países com maior número de computadores em casa, na região, são Uruguai, Argentina e Chile, com 67%, 62% e 60% dos lares, respectivamente (WEF, 2016). Países mais populosos, como o caso do Brasil, têm uma cobertura de 38%. Atualmente, há uma rede complexa de 244 cabos submarinos de fibra óptica que conectam todo o mundo. O cabo Atlantis-2 é o principal cabo entre a América do Sul e a Europa. Além destes, o Brasil está desenvolvendo outros quatro cabos, *South Atlantic Express (*SAEx), *South Atlantic Cable System* (SACS), *Camarões-Brazil Cable System* (CBCS) e EllaLink, este último com a Europa, que será apresentado adiante. O mapa abaixo mostra as sete principais redes de fibra óptica submarinas que conectam a América do Sul.

Map 1 – Submarine Fibre Optic Cables in South America

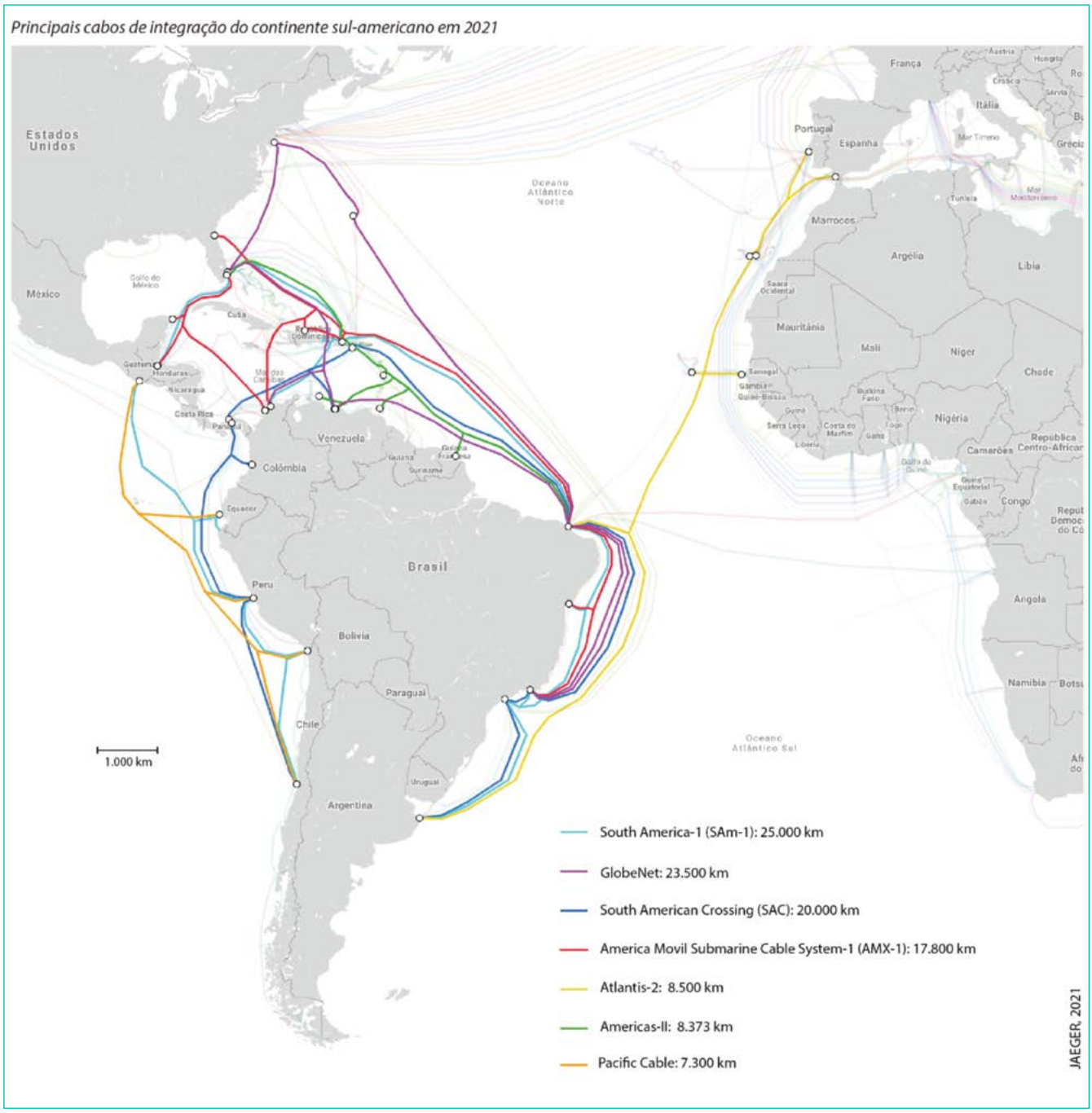
Main integration cables of the South American continent in 2021



Source: Created by the author with data from TeleGeography (2021).

The main networks seen on the map are SAm-1 and SAC because they include the largest number of South American countries. *South America-1* (in light blue) is operated by the Spanish company Telxius, which is in the process of being sold to the American company American Tower. *South American Crossing* (in dark blue) is operated by the Italian company Telecom Italia Sparkle and the American company Lumen/Century Link. The table below shows the main information on the seven chief submarine networks that interconnect the internet in the region.

Mapa 1 – Cabos submarinos de fibra óptica na América do Sul



Fonte: Elaboração própria a partir de dados do TeleGeography (2021).

Entre essas redes, as principais são a SAm-1 e a SAC, no quesito de incorporarem o maior número de países sul-americanos. A *South America-1* (em azul claro) é operada pela empresa espanhola Telxius, que se encontra em processo de venda para a empresa norte-americana American Tower. Já a *South American Crossing* (em azul escuro), por sua vez, é operada por uma empresa italiana, a Telecom Italia Sparkle, e a norte-americana Lumen/Century Link. O quadro abaixo demonstra as principais informações das sete principais redes submarinas que interconectam a internet da região.

Chart 1 – Information on the main submarine cables in the South American region

Cable	Extension	Connection Points	Providers
South America-1 (SAm-1)	25.000 km	Arica (Chile); Barranquilla (Colômbia); Boca Raton (EUA); Fortaleza (Brasil); Las Torinas (Argentina); Lurin (Peru); Mancora (Peru); Puerto Barrios (Guatemala); Puerto San Jose (Guatemala); Punta Cana (República Dominicana); Punta Camero (Equador); Rio de Janeiro (Brasil); Salvador (Bahia); San Juan (Porto Rico-EUA); Santos (Brasil) e Valparaiso (Chile).	Telxius (Espanha)
GlobeNet	23.500 km	Barranquilla (Colômbia); Boca Raton (EUA); Fortaleza (Brasil); Maiquetia (Venezuela); Rio de Janeiro (Brasil); St. David's (Bermuda); Tuckerton (EUA).	GlobeNet (Brasil)
South American Crossing (SAC)	20.000 km	Buenaventura (Colômbia); Colon (Panamá); Fort Amador (Panamá); Fortaleza (Brasil); Las Toninas (Argentina); Lurin (Peru); Puerto Viejo (Venezuela); Rio de Janeiro (Brasil); Santos (Brasil); St. Croix (EUA) e Valparaiso (Chile).	Telecom Italia Sparkle (Itália); Lumen/Century Link (EUA)
America Movil Submarine Cable System-1 (AMX-1)	17.800 km	Barranquilla (Colômbia); Cancún (México); Cartagena (Colômbia); Fortaleza (Brasil); Hollywood (EUA); Jacksonville (EUA); Puerto Barrios (Guatemala); Puerto Plata (República Dominicana); Rio de Janeiro (Brasil); Salvador (Brasil) e San Juan (Porto Rico-EUA)	América Móvil (México)
Atlantis-2	8.500 km	Carcavelos (Portugal); Conil (Espanha); Dakar (Senegal); El Médano (Ilhas Canárias-Espanha); Fortaleza (Brasil); Las Toninas (Argentina); Praia (Cabo Verde).	Embratel (Brasil); Deutsche Telekom (Alemanha); Telecom Italia Sparkle (Itália); Telecom Argentina (Argentina); Telxius (Espanha); Altice Portugal (Portugal); Orange (França); Telefónica Larga Distancia de Puerto Rico (Porto Rico-EUA); AT&T (EUA); BICS (Bahamas); KT (Coreia do Sul); Singtel (Cingapura); Tata Communications (Índia); Verizon (EUA); BT (Reino Unido); Orange Polska (Polônia).
Americas-II	8.373 km	Camuri (Venezuela); Caiena (Guiana Francesa); Fortaleza (Brasil); Hollywood (EUA); Le Lamentin (Martinica); Miramar (Porto Rico-EUA); Porto da Espanha (Trinidad e Tobago); St. Croix (EUA); Willemstad (Curaçau).	Embratel (Brasil); AT&T (EUA); Verizon (EUA); Sprint (EUA); CANTV (Venezuela); Tata Communications (Índia); CNT (Equador); Orange (França); Altice Portugal (Portugal); C&W Networks (Reino Unido); Telecom Italia Sparkle (Itália); Lumen (EUA).
Pacific Cable	7.300 km	Arica (Chile); Lurin (Peru); Puerto San Jose (Guatemala); Salinas (Equador); Valparaiso (Chile).	América Móvil (México)

Source: Created by the author with data from TeleGeography, 2021.

Quadro 1 – Informações sobre os principais cabos submarinos na região sul-americana

Cabo	Extensão	Pontos de Conexão	Empresas Operadoras
South America-1 (SAm-1)	25.000 km	Arica (Chile); Barranquilla (Colômbia); Boca Raton (EUA); Fortaleza (Brasil); Las Torinas (Argentina); Lurin (Peru); Mancora (Peru); Puerto Barrios (Guatemala); Puerto San Jose (Guatemala); Punta Cana (República Dominicana); Punta Camero (Equador); Rio de Janeiro (Brasil); Salvador (Bahia); San Juan (Porto Rico-EUA); Santos (Brasil) e Valparaiso (Chile).	Telxius (Espanha)
GlobeNet	23.500 km	Barranquilla (Colômbia); Boca Raton (EUA); Fortaleza (Brasil); Maiquetia (Venezuela); Rio de Janeiro (Brasil); St. David's (Bermuda); Tuckerton (EUA).	GlobeNet (Brasil)
South American Crossing (SAC)	20.000 km	Buenaventura (Colômbia); Colon (Panamá); Fort Amador (Panamá); Fortaleza (Brasil); Las Toninas (Argentina); Lurin (Peru); Puerto Viejo (Venezuela); Rio de Janeiro (Brasil); Santos (Brasil); St. Croix (EUA) e Valparaiso (Chile).	Telecom Italia Sparkle (Itália); Lumen/Century Link (EUA)
America Movil Submarine Cable System-1 (AMX-1)	17.800 km	Barranquilla (Colômbia); Cancún (México); Cartagena (Colômbia); Fortaleza (Brasil); Hollywood (EUA); Jacksonville (EUA); Puerto Barrios (Guatemala); Puerto Plata (República Dominicana); Rio de Janeiro (Brasil); Salvador (Brasil) e San Juan (Porto Rico-EUA)	América Móvil (México)
Atlantis-2	8.500 km	Carcavelos (Portugal); Conil (Espanha); Dakar (Senegal); El Médano (Ilhas Canárias-Espanha); Fortaleza (Brasil); Las Toninas (Argentina); Praia (Cabo Verde).	Embratel (Brasil); Deutsche Telekom (Alemanha); Telecom Italia Sparkle (Itália); Telecom Argentina (Argentina); Telxius (Espanha); Altice Portugal (Portugal); Orange (França); Telefónica Larga Distancia de Puerto Rico (Porto Rico-EUA); AT&T (EUA); BICS (Bahamas); KT (Coreia do Sul); Singtel (Cingapura); Tata Communications (Índia); Verizon (EUA); BT (Reino Unido); Orange Polska (Polônia).
Americas-II	8.373 km	Camuri (Venezuela); Caiena (Guiana Francesa); Fortaleza (Brasil); Hollywood (EUA); Le Lamentin (Martinica); Miramar (Porto Rico-EUA); Porto da Espanha (Trinidad e Tobago); St. Croix (EUA); Willemstad (Curaçau).	Embratel (Brasil); AT&T (EUA); Verizon (EUA); Sprint (EUA); CANTV (Venezuela); Tata Communications (Índia); CNT (Equador); Orange (França); Altice Portugal (Portugal); C&W Networks (Reino Unido); Telecom Italia Sparkle (Itália); Lumen (EUA).
Pacific Cable	7.300 km	Arica (Chile); Lurin (Peru); Puerto San Jose (Guatemala); Salinas (Equador); Valparaiso (Chile).	América Móvil (México)

Fonte: Elaboração própria a partir de dados de TeleGeography, 2021.

The data above confirm that the control of South American telecommunications is centred in extra-regional companies. The consequences of this cable distribution are manifold, but especially the region's dependence on connections to the USA in order to be able to connect with the rest of the world. This means that most information from South America to Europe, Asia, Africa or Oceania passes through the USA. According to data from the Regional Broadband Observatory (ORBA) of the Economic Commission for Latin America (ECLAC), "between 75% and 85% of the data circulating in South America, including local content, go through Miami, which increases the connection costs" (ECLAC, 2011, p. 8).

Brazil has four landing points for submarine cables connecting South America to the USA (Fortaleza, Salvador, Rio de Janeiro, and Santos), all operated by private companies (TELEGEOGRAPHY, 2021). With the exception of Bolivia and Paraguay, which are landlocked, all other South American countries have access to these cables. This connection via the USA represents up to 45% of the broadband cost in the region, and around 80% of international data traffic in South America passes through the USA (ZIBECHI, 2012). Shortening the path and lowering costs for this traffic should lead to an increase in internet speed. "Latin American dependence is explained in part by the logic behind infrastructure development in the region. The intention was not to connect Latin American countries to each other, but to connect them to where the content was, that is, to the United States" (ROMERO, 2019, p. 144).

Policies being adopted: creation, crisis, and collapse of the South American Optical Ring

In January 2012, the First Meeting of the COSIPLAN Working Group on Telecommunications took place in Asunción, Paraguay, with the presence of all South American countries. On the occasion, the Brazilian delegation, with a representative of the Brazilian state-owned telecommunications company TELEBRAS, presented the proposal for the South American Optical Ring as an interconnection agreement between regional telecommunication providers by building fibre optic cable networks (COSIPLAN, 2012). The strategic functions of the project presented during the meeting were to democratise internet access throughout the region, making it faster, and to ensure data and information security in South America.

In regional terms, recognizing the importance of guaranteeing the security of digital data and of democratising access accelerated efforts to form the South American Optical Ring. An understanding was reached that the development of South America's communications infrastructure was an essential requirement for less dependent and vulnerable relations with the USA. Brazil played a prominent role in the negotiations within the UNASUR due to its proportions within the region and to its national broadband access promotion agenda. At the Second Meeting of the COSIPLAN WG on Telecommunications, the Brazilian minister of communications emphasised that the South American Optical Ring project would reduce regional weaknesses in the event of a cyberattack and in terms of official and military data confidentiality. The greatest hindrance to the integration of communications in South America would be the difference in economic capacity between countries. The project, in this perspective, would only make sense if all the nations in the region adhered to it (PORTAL BRASIL, 2012).

Os dados acima evidenciam a centralidade do controle das telecomunicações sul-americanas a partir de empresas extrarregionais. As consequências dessa distribuição de cabos são múltiplas, mais especialmente a dependência da região das conexões com os EUA para poder se conectar com o resto do mundo. Isso significa que grande parte das informações da América do Sul com destino à Europa, Ásia, África ou Oceania passa pelos EUA. Segundo dados do Observatório Regional de Banda Larga (ORBA) da Comissão Econômica para a América Latina (CEPAL), "entre 75% e 85% dos dados que circulam na América do Sul, incluindo conteúdo local, passam por Miami, o que aumenta os custos de conexão" (CEPAL, 2011, p. 8).

O Brasil tem quatro saídas para cabos submarinos que conectam a América do Sul com os EUA (Fortaleza, Salvador, Rio de Janeiro e Santos), todas operadas por empresas privadas (TELEGEOGRAPHY, 2021). Com exceção de Bolívia e Paraguai, que não têm saída para o mar, todos os demais países sul-americanos também possuem acesso a esses cabos. Essa conexão com os EUA chega a representar 45% do custo de banda larga na região, e cerca de 80% do tráfego de dados internacional na América do Sul passa por território norte-americano (ZIBECHI, 2012). Reduzindo o caminho e baixando os custos para esse tráfego, a própria velocidade da internet deve aumentar. "A dependência latino-americana é explicada em parte pela lógica pela qual a infraestrutura foi desenvolvida na região. A intenção não era conectar os diversos países latino-americanos entre si, mas conectar-se ao local onde estava o conteúdo, ou seja, aos Estados Unidos" (ROMERO, 2019, p. 144).

Políticas que estão sendo adotadas: criação, crise e colapso do Anel Óptico Sul-Americano

Em janeiro de 2012 ocorreu a I Reunião do Grupo de Trabalho de Telecomunicações do COSIPLAN, em Assunção, no Paraguai, com a presença de todos os países sul-americanos. Na ocasião, a delegação brasileira, com a participação de um representante da TELEBRAS, empresa estatal brasileira de telecomunicações, apresentou a proposta de criação do Anel Óptico Sul-Americano como um acordo de interconexão entre as operadoras regionais de telecomunicação através da construção de cabos de fibra óptica (COSIPLAN, 2012). O projeto foi apresentado com as funções estratégicas de democratizar o acesso à internet por toda a região, torná-la mais rápida e, especialmente, garantir a segurança dos dados e informações na América do Sul.

Em termos regionais, o reconhecimento da importância em garantir a segurança dos dados digitais e elevar a democratização do acesso acelerou os esforços para a formação do Anel Óptico Sul-Americano. Chegou-se ao entendimento de que o desenvolvimento da infraestrutura de comunicações da América do Sul era um requisito imprescindível para relações menos dependentes e vulneráveis com os EUA. Nesse contexto, o Brasil vinha desempenhando um papel de destaque nas negociações no âmbito da UNASUL por sua dimensão na região e por sua agenda nacional de promoção do acesso à banda larga. Na II Reunião do GT de Telecomunicações do COSIPLAN, o então ministro das comunicações do Brasil destacou que o projeto do Anel Óptico Sul-Americano reduziria as fragilidades regionais em caso de ciberataque, bem como em termos de sigilo de dados oficiais e militares. A maior dificuldade para a integração das comunicações na América do Sul decorreria da diferença da capacidade econômica entre os países. O projeto, nessa perspectiva, apenas ganharia sentido com a adesão de todas as nações da região (PORTAL BRASIL, 2012).

The project was to create a network of more than 10,000 km of terrestrial fibre optic cables, which would be managed by the state-owned companies of each country. With the Optical Ring, "in Brazil, for example, price reductions for people can reach 15%, while in countries where international connectivity is more expensive, such as Bolivia, it can reach more than 50%" (ECLAC, 2011, p. 5). The proposal aimed at generating interconnections between existing infrastructure in border areas. In 2014, an agreement was signed with the Andean Development Corporation (CAF) to determine the costs of the Optical Ring (COSIPLAN, 2016a). The study concluded that building terrestrial fibre optic networks in the region would cost $100 million.

Although the project originally provided for integrated coverage in the region, in practice, only six stretches were finally consolidated into structured projects in the COSIPLAN Portfolio. In the latest version available (2017), there are six telecommunications projects, and all of them are about interconnecting fibre optic cables. The $21 million total estimated investment for these projects corresponded to about 1% of the total investment of the COSIPLAN 2017 Portfolio. Three of the six projects have been completed and three are in the profile stage. All are under government funding. Below is a map showing the location of the six regional fibre optic connection projects.

Map 2 - COSIPLAN's Optical Infrastructure (2016)

COSIPLAN's main fiber optic integration projects

Source: Created by the author with data from COSIPLAN project files (2016).

O projeto consistia na criação de uma rede de mais de 10.000 km de cabos terrestres de fibra óptica, que seria administrada pelas empresas estatais de cada país. Com o Anel Óptico "no Brasil, por exemplo, a redução das tarifas para pessoas pode chegar a 15%, enquanto em países onde a conectividade internacional é mais cara, como a Bolívia, pode chegar a mais de 50%" (CEPAL, 2011, p. 5). A proposta visava gerar interligações entre as infraestruturas existentes nas zonas de fronteira. Em 2014, foi firmado um acordo com a Coordenação Andina de Fomento (CAF) para determinar os custos do Anel Óptico (COSIPLAN, 2016a). O estudo concluiu que a construção das redes de fibras ópticas terrestres na região custaria 100 milhões de dólares.

Ainda que o projeto previsse originalmente uma cobertura integrada na região, na prática, apenas seis trechos acabaram sendo consolidados em projetos estruturados da Carteira COSIPLAN. Na versão mais recente disponível, de 2017, constam seis projetos de telecomunicações, todos de interconexão de cabos de fibra óptica. O total dos investimentos estimados desses projetos, em 21 milhões de dólares, correspondia a cerca de 1% dos investimentos totais da Carteira COSIPLAN 2017. Três deles encontram-se concluídos e três estão na etapa perfil. Todos encontram-se sob financiamento público. Abaixo, segue um mapa que ilustra a localização dos seis projetos de conexão de fibra óptica regional.

Mapa 2 – Infraestrutura óptica do COSIPLAN (2016)

Fonte: Elaboração própria, a partir de dados das fichas de projetos COSIPLAN (2016).

The prominence of projects in countries with less access to critical infrastructure in South America is noteworthy. Bolivia and Paraguay are the two countries who benefit the most from fibre optic interconnections, along with Uruguay, Venezuela and Brazil. Another relevant point is the interconnection of objectives between COSIPLAN and the South American Defence Council (CDS), also with UNASUR, by means of the South American Optical Ring. Article 5 of the founding treaty of the CDS states the objective of "promoting the exchange of information and analysis on the regional and international situation, with the purpose of identifying risk factors and threats that may affect regional and world peace" (UNASUR, 2008). Consequently, improving the use of ICT infrastructure is directly related to the advancement of the organization and cooperation among South American countries. In addition, in the COSIPLAN 2014 Work Plan, the project became part of COSIPLAN's "Network for South American Connectivity for Integration" (Red Clara), under CDS, which deals with cyber defence and fibre optic interconnection issues (COSIPLAN, 2013b). Together, CDS and COSIPLAN form the backbone of UNASUR. These are the councils that have demonstrated the most progress and institutional organization. The confluence between infrastructure and defence is critical for the success of the South American integration initiative, as the subcontinent is a strategic region, full of natural resources and with severe infrastructure bottlenecks. It is important to highlight the importance of the dual role of infrastructure — it equally serves civil and military purposes and its effects spread through all spheres of society.

Since 2013, the Optical Ring, Red Clara, and the promotion of regional integration through ICTs has appeared annually in the COSIPLAN Work Plans (Actions 5.3 and 6.2.5 of the WG on Telecommunications). The 2018 Work Plan, published in 2017, was the last one available in the institution's list of documents at the time of this research. It is noteworthy that, for the first time since 2013, these strategic actions linked to the Optical Ring have been excluded from COSIPLAN's planning. Apparently, the project lost importance and prominence in the regional integration strategy. Also, three projects in the telecommunications sector were excluded between the 2011 and 2017 portfolios. The road transport subsector, predominant in annual plans, has progressively gained more space. In the telecommunications sector, global competition has increased in the ICTs market, as can be seen in the current race for 5G technology. With the South American Optical Ring project stalled, the region and Brazil find themselves in a passive position, waiting for extra-regional broadband technologies and without regional autonomous development.

The current scenario of profound challenges makes room for new perspectives on the subject. UNASUR's and consequently COSIPLAN's ultimate crisis[1] is a direct result of the crises of the conservative regional cycle, and the Brazilian government is one of its main representatives. Since the beginning of the New Republic, it is the first time that Brazilian foreign policy has been in such profound isolation from its South American neighbours. It is possible to say that Brazil has renounced the quest for

1 The collapse of UNASUR and, consequently, of COSIPLAN, had its apex event in April 2018, when the governments of Brazil, Argentina, Chile, Colombia, Paraguay and Peru jointly decided to suspend their participation in the organization, claiming that they did so because of the prolonged institutional crisis (BRASIL, 2019).

Destaca-se a proeminência de projetos em países com menos acesso a infraestruturas fundamentais na América do Sul. Bolívia e Paraguai são os dois países mais beneficiados pelas interconexões de fibra óptica, juntamente com Uruguai, Venezuela e Brasil. Outro fator relevante de análise é a interconexão de objetivos entre COSIPLAN e Conselho de Defesa Sul-Americano (CDS), também da UNASUL, através do Anel Óptico Sul-Americano. No artigo 5º do tratado constitutivo do CDS, encontra-se o objetivo de "promover o intercâmbio de informações e análise sobre a situação regional e internacional, com o propósito de identificar os fatores de risco e ameaças que possam afetar a paz regional e mundial" (UNASUL, 2008). Nesse sentido, o aprimoramento do uso da infraestrutura de TICs está diretamente relacionado com o avanço da organização e da cooperação entre os países da América do Sul. Além disso, no Plano de Trabalho COSIPLAN 2014, o projeto passou a integrar a "Rede para a Conectividade Sul-Americana para Integração" (Red Clara) do COSIPLAN, junto ao CDS, sobre temas de defesa cibernética e interconexão de fibra óptica (COSIPLAN, 2013b). Juntos, CDS e COSIPLAN conformam a espinha dorsal da UNASUL. São os conselhos que apresentam maiores avanços e organização institucional. A confluência entre infraestrutura e defesa é fundamental para o sucesso da iniciativa de integração sul-americana, sendo o subcontinente um território estratégico, repleto de recursos naturais e com profundos gargalos infraestruturais. Ressalta-se a importância do papel dual da infraestrutura, ou seja, seus benefícios servem igualmente a propósitos civis e militares cujos efeitos se alastram por todas as esferas da sociedade.

Desde 2013, o Anel Óptico, a Red Clara e a promoção da integração regional através das TICs apareciam anualmente nos Planos de Trabalho do COSIPLAN (Ações 5.3 e 6.2.5 do GT de Telecomunicações). O Plano de Trabalho para 2018, publicado em 2017, é o último disponível nos documentos da instituição no momento desta pesquisa. Chama a atenção o fato de que, pela primeira vez desde 2013, essas ações estratégicas ligadas ao Anel Óptico foram excluídas do planejamento do COSIPLAN. Ao que tudo indica, o projeto foi perdendo importância e destaque na estratégia de integração regional. Inclusive, ressalta-se a exclusão de três projetos do setor de telecomunicações na comparação entre as carteiras de 2011 e 2017. A proeminência do subsetor rodoviário, predominante nas planificações anuais, foi ganhando progressivamente cada vez mais espaço. Além disso, no setor de telecomunicações, ressalta-se a elevação da competição global no domínio sobre as TICs, simbolizadas atualmente na disputa pela tecnologia 5G. Nesse contexto, sem avanços do projeto do Anel Óptico Sul-Americano, a região e o Brasil encontram-se em uma posição passiva de espera pela recepção de tecnologias de banda larga extrarregionais, sem um desenvolvimento autônomo regional.

A atual conjuntura de profundos desafios abre espaço para novas perspectivas acerca do tema. A crise derradeira da UNASUL[1] e, portanto, do COSIPLAN, é resultado direto das crises do ciclo regional conservador, que tem no governo brasileiro um de seus principais representantes. Na Nova República, é a primeira vez que a política externa brasileira passa por um momento de tão profundo isolamento em relação aos vizinhos sul-americanos. É possível dizer que o Brasil renunciou à busca por uma liderança

[1] O colapso da UNASUL e, consequentemente, do COSIPLAN, tem seu evento-ápice em abril de 2018, quando os governos de Brasil, Argentina, Chile, Colômbia, Paraguai e Peru decidiram de forma conjunta suspender a sua participação na organização, alegando que o fizeram devido à prolongada crise institucional (BRASIL, 2019).

regional leadership. In terms of infrastructure, the discontinuity of regional integration projects is aligned with a project to privatise large government-owned companies that subsidise control over Brazilian infrastructure. Most of the isolated infrastructure initiatives in Brazil currently follow the road transport profile and serve the interests of foreign investors. In the regional context, the period of advances in physical integration between Brazil and its neighbours is over.

As a UNASUR project, the strategic functions of the South American Optical Ring were (i) to increase security in the digital data transmission network; (ii) to reduce broadband access costs; and (iii) to integrate South American ICTs. One can thus infer that the project sought to gain security autonomy regarding digital data and to reduce external dependence, especially in the case of the submarine cables that connect the region to the USA. However, in view of the situation, the possibilities for implementing the project are limited. The promotion of cooperation with Europe is an alternative for South American countries.

The 8,500 km-long Atlantis-2 cable connects Argentina, Brazil, Cape Verde, Senegal, Portugal and Spain and was built in the year 2000. More recently, in June 2021, the 6,200 km-long EllaLink cable between Brazil, Cape Verde and Portugal was completed. The EllaLink network was specifically designed to meet the growing demand for a new low-latency route between Europe and South America. Its main objective is to create a direct data corridor between the two continents and then to Africa, the Middle East and Asia. Conceived in 2012, the cable is the first high-speed data link via submarine connection between South America and Europe. In 2018, the pan-European equity fund Marguerite II became the equity sponsor of EllaLink. The system's anchor customers are, among others, the Bella consortium, Cabo Verde Telecom and EMACOM (ELLALINK, 2021). As can be seen in map 3 below, EllaLink is connected to the European network of terrestrial fibre optic cables. This shows how important it is to promote this modality of telecommunications integration; after all, terrestrial cables promote the regional integration of contiguous territories.

In the context of the current digital dispute between the USA and

Map 3 – The EllaLink Cable Interconnections

Source: EllaLink (2021).

regional. Em termos de infraestrutura, a descontinuidade dos projetos de integração física regional encontra confluência com um projeto privatizador de grandes empresas nacionais que subsidiam o controle sobre a infraestrutura brasileira. A maioria das iniciativas isoladas referentes à infraestrutura no Brasil, atualmente, responde ao perfil rodoviarista e aos interesses dos investidores externos. No contexto regional, finda-se o período de avanços na integração física entre o Brasil e os vizinhos.

O Anel Óptico Sul-Americano, enquanto projeto da UNASUL, tinha como funções estratégicas (i) maior segurança na rede de transmissão de dados digitais; (ii) redução nos custos de acesso à banda larga; e (iii) integração das TICs sul-americanas. Nesse sentido, depreende-se a busca pelos ganhos de autonomia securitária quanto aos dados digitais e pela redução da dependência externa especialmente em relação à proeminência cabos que conectam a região aos EUA. No entanto, tendo em vista a conjuntura, as possibilidades de concretização do projeto encontram-se limitadas. Como alternativa que se abre aos países sul-americanos, destaca-se o fomento da cooperação com a Europa.

O cabo Atlantis-2, de 8.500 km, conecta Argentina, Brasil, Cabo Verde, Senegal, Portugal e Espanha e foi construído no ano 2000. Mais recentemente, em junho de 2021, foi concluído o cabo EllaLink, entre Brasil, Cabo Verde e Portugal, com uma extensão de 6.200 km. A rede EllaLink foi projetada especificamente para atender à crescente demanda por uma nova rota de baixa latência entre a Europa e a América do Sul. O objetivo principal é o de criar um corredor de dados direto entre os dois continentes e então para África, Oriente Médio e Ásia. Idealizado em 2012, o cabo é a primeira ligação de dados de alta velocidade via conexão submarina entre América do Sul e Europa. Em 2018, o fundo de ações pan-europeu Marguerite II tornou-se o patrocinador de ações da EllaLink. Os clientes âncora do sistema são, entre outros, o consórcio Bella, a Cabo Verde Telecom e a EMACOM (ELLALINK, 2021). Conforme pode ser visto no mapa 3 abaixo, o EllaLink se conecta à rede europeia de cabos terrestres de fibra óptica, o que evidencia a importância do fomento dessa modalidade de integração de telecomunicações para além dos cabos submarinos; afinal, são os cabos terrestres que promovem a integração regional de um território contíguo.

Mapa 3 – As interconexões do cabo EllaLink

Fonte: EllaLink (2021).

China, the cable has great strategic and economic value for both regions of the Atlantic as an autonomous position amid economic and technological warfare. In addition to fostering business opportunities, above all, it ensures greater security and stability in data connections between the two regions. The EllaLink cable is an important advance in this interconnection, and this is an important window of opportunity for the joint development of other optical fibre cables. For Europe, they represent investment advantages in a region with great potential for digital infrastructure. For South America, even though the ideal of regional integration is in a crisis, there is a chance to diversify partnerships, reduce dependence and increase security of digital data, especially if cooperation is horizontal and prioritises the autonomous interests of South American regional security.

Policy recommendations

The main policy recommendations to be implemented for security issues of common interest between Europe and South America are as follows:

(I) Promotion of South American regional integration policies and projects, as a result of a wider integration with the European territory to increase regional security and stability. Regional cooperation and cohesion arrangements are proposed based on autonomous interests in the formation of South America as an integrated space. More specifically, multilateralism in the region should be encouraged and integration projects should resume in view of the institutional dismantling of UNASUR.

(II) Due to the weaknesses found in the South American integration process, the region has been plagued by an increase in crises and vulnerabilities. Therefore, cooperation projects with extra-regional companies, mainly from the European continent, represent, in the short to medium term, a viable possibility for investment, technology exchange, and reduction of dependence on the opposite poles of the cybernetic dispute, meeting the security interests of both regions. Accordingly, the recommendation is to promote political dialogue and to expand the debate, at a strategic level, between South America and Europe with regard to ICTs, technological cooperation, and the roles they can play in a joint, integrated development. A good example is the European network of terrestrial fibre optic cables.

(III) Finally, the establishment of a technical and political forum between South America and Europe, involving governments, social organizations, universities, think tanks, and companies in order to debate and build policies for transparency and cyber security, technical-scientific cooperation, and promotion of joint investments to form a more widespread network of terrestrial and submarine cables that reduce the dependence of South American telecommunications on the USA.

No contexto de atual disputa digital entre EUA e China, o cabo apresenta grande valor estratégico e econômico para ambas as regiões do Atlântico enquanto posicionamento autônomo na conjuntura de guerra econômica e tecnológica. Além de fomentar as possibilidades de negócios, acima de tudo, garante maior segurança e estabilidade nas conexões de dados entre as duas regiões. O cabo EllaLink representa um importante avanço para essa interconexão, mas é pertinente ressaltar a janela de oportunidade para a formação conjunta de outros cabos de fibra óptica. Para a Europa, representam vantagens para investimentos em uma região com grande potencial para avanço de infraestrutura digital. Para a América do Sul, ainda que o ideal de integração regional esteja em crise, abre-se a oportunidade para diversificação de parcerias, redução de dependência e mais segurança nos dados digitais, especialmente se a cooperação for realizada de forma horizontal, priorizando os interesses autônomos da segurança regional sul-americana.

Recomendações políticas

Como recomendações de políticas a serem implementadas para as questões securitárias de interesse comum entre Europa e América do Sul, destacam-se:

(I) Fomento de políticas e projetos de integração regional sul-americana, como reflexo dos ganhos da integração no território europeu para aumento da segurança e estabilidade regional. Nesse sentido, elevam-se arranjos de cooperação e de coesão regional, a partir de interesses autônomos na formação da América do Sul enquanto espaço integrado. De forma mais específica, recomenda-se o estímulo à multilateralidade na região e a retomada de projetos de integração frente ao desmonte institucional da UNASUL.

(II) Em razão das debilidades no processo integracionista sul-americano, a região tem sido assolada por um aumento de crises e de vulnerabilidades. Dessa forma, projetos de cooperação com companhias extrarregionais, principalmente do continente europeu, representam uma possibilidade viável de curto a médio prazo para investimentos, intercâmbio tecnológico e redução da dependência em relação aos polos da disputa cibernética, atendendo aos interesses securitários de ambas as regiões. Mais especificamente, propõe-se a promoção do diálogo político e ampliação dos debates a nível estratégico entre América do Sul e Europa no que se refere às TICs, à cooperação tecnológica e às funções que apresentam ao desenvolvimento conjunto e integrado, a exemplo da rede europeia de cabos terrestres de fibra óptica.

(III) Por fim, propõe-se a construção de um fórum técnico e político entre América do Sul e Europa, envolvendo governos, organizações sociais, universidades, *think tanks* e empresas a fim de debater e construir políticas de transparência e segurança cibernética, de cooperação técnico-científica e de promoção de investimentos conjuntos para a formação de uma rede mais capilarizada de cabos terrestres e submarinos que diminuam a dependência das telecomunicações sul-americanas aos EUA.

References

BRASIL. Ministério das Relações Exteriores. **Denúncia do Tratado Constitutivo da União de Nações Sul-Americanas (UNASUL).** Nota à imprensa nº 91/2019. Published on April 15, 2019.

CEPAL. **Newsletter ELAC 2015.** No 17 Diciembre 2011. Comisión Económica para América Latina, Organización de las Naciones Unidas, 2011.

COSIPLAN (2011). **Plano de Ação Estratégico 2012-2022.** Consejo Suramericano de Infraestructura y Planeamiento, 2011.

_____(2012). **Informe Final: I Reunión del Grupo de Trabajo de Telecomunicaciones.** Consejo Suramericano de Infraestructura y Planeamiento, 2012.

_____(2013a). **Ficha del Proyeto: Líneas de fibra óptica u otra tecnología apropiada que interconecte Caracas al norte de Brasil.** Consejo Suramericano de Infraestructura y Planeamiento, 2013a.

_____(2013b). **Plan de Trabajo 2014.** Consejo Suramericano de Infraestructura y Planeamiento, 2013b.

_____ (2015). **Ficha del Proyeto: Cable Óptico entre Brasil y Uruguay.** Consejo Suramericano de Infraestructura y Planeamiento, 2015.

_____ (2016). **Cartera de Proyectos 2016.** Consejo Suramericano de Infraestructura y Planeamiento, 2016.

_____ (2017). **Plan de Trabajo 2018.** Consejo Suramericano de Infraestructura y Planeamiento, 2017.

_____ (2021). **Sistema de Información de Proyectos.** Consejo Suramericano de Infraestructura y Planeamiento.

ELLALINK. **Express optical platform between Europe and Latin America**, 2021.

IIRSA. **Cartera de Proyectos IIRSA 2004**. Planificación Territorial Indicativa. December 2004.

PORTAL BRASIL. **Comunicação apresenta proposta para construção de anel óptico na América do Sul.** 03 Feb. 2012.

ROMERO, O. J. Telecomunicaciones y dependencia en América Latina: retos para la integración autónoma. **Controversias y Concurrencias Latinoamericanas**, vol. 11, n. 19, 2019.

TELEGEOGRAPHY. **Submarine Cable Map**. Available at: https://www.submarinecablemap.com/. Acessed: 01 June 2021.

UNASUL. **Tratado Constitutivo da União de Nações Sul-Americanas.** União das Nações Sul-Americanas, Brasília, 23 May 2008.

WEF. **Global Information technology Report 2016.** The networked readiness Index. World Economic Forum, 2016.

ZIBECHI, Raúl. **Anillo óptico Sur Americano.** Programa de las Américas, 2012.

Referências

BRASIL. Ministério das Relações Exteriores. **Denúncia do Tratado Constitutivo da União de Nações Sul-Americanas (UNASUL)**. Nota à imprensa nº 91/2019. Publicado em 15 de abril de 2019.

CEPAL. **Newsletter ELAC 2015.** No 17 Diciembre 2011. Comisión Económica para América Latina, Organización de las Naciones Unidas, 2011.

COSIPLAN (2011). **Plano de Ação Estratégico 2012-2022**. Consejo Suramericano de Infraestructura y Planeamiento, 2011.

_____ (2012). **Informe Final: I Reunión del Grupo de Trabajo de Telecomunicaciones.** Consejo Suramericano de Infraestructura y Planeamiento, 2012.

_____(2013a). **Ficha del Proyeto: Líneas de fibra óptica u otra tecnología apropiada que interconecte Caracas al norte de Brasil.** Consejo Suramericano de Infraestructura y Planeamiento, 2013a.

_____(2013b). **Plan de Trabajo 2014.** Consejo Suramericano de Infraestructura y Planeamiento, 2013b.

_____ (2015). **Ficha del Proyeto: Cable Óptico entre Brasil y Uruguay.** Consejo Suramericano de Infraestructura y Planeamiento, 2015.

_____ (2016). **Cartera de Proyectos 2016.** Consejo Suramericano de Infraestructura y Planeamiento, 2016.

_____ (2017). **Plan de Trabajo 2018.** Consejo Suramericano de Infraestructura y Planeamiento, 2017.

_____ (2021). **Sistema de Información de Proyectos.** Consejo Suramericano de Infraestructura y Planeamiento.

ELLALINK. **Express optical platform between Europe and Latin America**, 2021.

IIRSA. **Cartera de Proyectos IIRSA 2004.** Planificación Territorial Indicativa. Dezembro de 2004.

PORTAL BRASIL. **Comunicação apresenta proposta para construção de anel óptico na América do Sul.** 03 fev. 2012.

ROMERO, O. J. Telecomunicaciones y dependencia en América Latina: retos para la integración autónoma. **Controversias y Concurrencias Latinoamericanas**, vol. 11, núm. 19, 2019.

TELEGEOGRAPHY. **Submarine Cable Map**. Disponível em: https://www.submarinecablemap.com/. Acesso em: 01 jun. 2021.

UNASUL. **Tratado Constitutivo da União de Nações Sul-Americanas.** União das Nações Sul-Americanas, Brasília, 23 de maio de 2008.

WEF. **Global Information technology Report 2016.** The networked readiness Index. World Economic Forum, 2016.

ZIBECHI, Raúl. **Anillo óptico Sur Americano.** Programa de las Américas, 2012.

Daniel Vidal Pérez

Daniel Vidal Pérez é pesquisador da Empresa Brasileira de Agropecuária (Embrapa) desde 1990. É docente no curso de Doutorado em Sistemas de Gestão Sustentáveis da Universidade Federal Fluminense (UFF). Desde 2019, atua como pesquisador voluntário sênior no Subgrupo Biodefesa e Segurança Alimentar no Laboratório de Simulações e Cenários da Escola de Guerra Naval (EGN).

Daniel Vidal Pérez has been a researcher at Embrapa since 1990. He is a professor in the PPSIG PhD course at UFF (Federal Fluminense University). Since 2019, he has been working as a senior volunteer researcher in the Subgroup of Biodefense and Food Security in the LSC (Simulations and Scenarios Laboratory) of the Naval War College.

Alimento: uma das principais, e menos reconhecidas, armas da paz

Food: one of the greatest and least recognized weapons of peace

Daniel Vidal Pérez

RESUMO

• Um longo e tortuoso caminho permeia diferentes níveis de conflitos e, em última instância, pode levar à guerra. A maioria dos países só começou a entender recentemente que o direito do homem a uma quantidade adequada e nutritiva de alimento é condição básica para a estabilidade e segurança de uma nação.

• Após longo período em declínio, o número de pessoas subnutridas aumentou nos últimos cinco anos, e a pandemia de COVID-19 expôs a vulnerabilidade dos sistemas globais de alimentos.

• A descontinuidade tem sido uma das principais características de políticas relacionadas à garantia de segurança alimentar na América Latina e no Caribe, especialmente no Brasil. Portanto, é apresentada uma abordagem geral para o reforço da resiliência de sistemas alimentares, levando em conta cenários possíveis e futuros de choque. Acima de tudo, todos os governos deveriam considerar a produção, a comercialização e a distribuição de alimentos como infraestrutura crítica.

EXECUTIVE SUMMARY

• There is a long and tortuous path that passes through different levels of conflict and ultimately can reach war. Only recently did most countries begin to understand that man's right to an adequate and nutritious amount of food is a basic condition for the stability and security of a nation.

• After a long period of decline, the number of undernourished people has increased over the last five years. And the COVID-19 pandemic exposed the vulnerability of global food systems.

• One of the main characteristics of policies related to ensuring food security in Latin America and the Caribbean, especially Brazil, has been discontinuity. Thus, considering future and possible shock scenarios, an overall approach to strengthening resilience in food systems have been presented. But, most of all, all governments should consider food production, marketing, and distribution as a critical infrastructure.

CONTEXT AND IMPORTANCE OF THE PROBLEM

Does No War Mean Peace? This question highlights the evident differences between a negative and a positive conceptualization of Peace. This duality was first suggested by Galtung in the editorial of the first edition of the *Journal of Peace Research* in 1964. A detailed elaboration on both concepts exceeds the scope of this article. However, some considerations must be made. First, negative peace defines war and peace as two opposite categories. However, as stated by Diehl, "how to explain that North Korea has been at peace with South Korea and the United States, since 1953, in the peace-as-not-war conception? [...] After all, no major military engagements have occurred". Furthermore, in today's environment, with disruptive technologies, the objectives of high intensity conflicts have changed from annihilation of the enemy to destruction of enemy systems, like the economy, trade, and the military, for example. Therefore, this particular definition of the nature of war based on fatalities is also undergoing a change. This is one of the reasons why a positive peace concept has emerged. It takes into account other elements that may characterize different categories of peace. Some examples of this new framework include the absence of major territorial claims; the existence of institutions for conflict management; the evaluation of non-traditional aspects of security, such as human security, the status of women, and human rights; and socioeconomic inequalities; among others. The recent decisions of the Nobel Committee in awarding the Peace Prize mostly to positive peace efforts corroborates the current inclination towards this concept.

Another approach to discuss whether no war means peace could be based on data analysis. The number of fatalities in organized violence decreased for the fifth consecutive year in 2019 according to the Uppsala Conflict Data Program (UCDP). The general decline in fatalities from organized violence does not correspond to the trend in the number of active conflicts, which remained stable but on a historically high level. However, overall global levels of peace continue to deteriorate based on the Global Peace Index of the Institute for Economics and Peace. As a matter of fact, the year of 2020 presented the ninth reduction in peacefulness in the last twelve years. It seems that, in the long term, the pattern is one of deterioration. Moreover, there is a growing global inequality in peace, with the most peaceful countries continuing to improve, while the least peaceful are plummeting into greater violence and conflict. Thus, in terms of causation, the link between war and peace does not necessarily move in opposite directions.

A third approach takes into account that, if the initial premise is true (No War Means Peace), the studies of peace and war should constitute a coherent body of research. Thus, a survey on how research papers on peace and war are distributed between its two nominal pillars was tested. For this, a linked research knowledge system was used, Dimensions (https://app.dimensions.ai/discover/publication), assigning either "peace", "war" or "peace and war" as keywords and phrase to search all publications contained within the database (just over 119,092,422 publications on May 29th 2021). The period between 1990 and 2020 was established.

CONTEXTO E IMPORTÂNCIA DO PROBLEMA

A ausência de guerras significa paz? Esta questão ressalta as evidentes diferenças entre a conceitualização negativa e a conceitualização positiva da Paz. Tal dualidade foi sugerida pela primeira vez por Galtung no editorial da primeira edição *do Journal of Peace Research* em 1964. Uma discussão detalhada dos referidos conceitos excederia o escopo deste artigo. Contudo, devem-se fazer algumas considerações. Primeiramente, paz negativa define guerra e paz como duas categorias opostas. No entanto, de acordo com Diehl, "como explicar que a Coreia do Norte está em paz com a Coreia do Sul e os Estados Unidos desde 1953 segundo o conceito de 'paz como não-guerra'? [...] Afinal, não houve nenhuma mobilização militar relevante". Ademais, no ambiente atual, com tecnologias disruptivas, o objetivo de conflitos de alta intensidade deixou de ser a aniquilação do inimigo, passando a ser destruição de seus sistemas como, por exemplo, a economia, o comércio e as forças armadas. Portanto, esta definição específica da natureza da guerra baseada em mortes também está mudando. Esta é uma das razões pelas quais surgiu o conceito de paz positiva, levando em consideração outros elementos que podem caracterizar diferentes categorias de paz. Alguns exemplos deste novo marco incluem a ausência de importantes disputas territoriais; a existência de instituições para a gestão de conflitos; a avaliação de aspectos não tradicionais de segurança, tais como segurança humana, o status das mulheres e os direitos humanos; e desigualdades socioeconômicas dentre outros. As decisões mais recentes do Comitê Nobel, de conceder o Prêmio Nobel da Paz principalmente para esforços de paz positiva, corroboram a atual preferência por tal conceito.

Outra maneira de debater se a ausência de guerras significa paz poderia se basear em análise de dados. De acordo com o Programa de Dados de Conflitos de Uppsala (UCDP), o número de mortes decorrentes de violência organizada diminuiu pelo quinto ano consecutivo. Tal diminuição geral não corresponde à tendência quanto ao número de conflitos ativos, que permaneceu estável, porém em um nível historicamente elevado. No entanto, baseado no Índice Global da Paz do Instituto para Economia e Paz, os níveis globais gerais de paz continuam a se deteriorar. Na verdade, o ano de 2020 apresentou a nona redução na pacificidade nos últimos doze anos. Aparentemente, a longo prazo, o padrão é de deterioração. Ademais, há uma crescente desigualdade global na paz, com os países mais pacíficos continuando a melhorar, ao passo que os menos pacíficos sofrem com mais violência e conflitos. Assim, em termos de causalidade, a relação entre guerra e paz não se move necessariamente em direções opostas.

Uma terceira abordagem leva em conta que, sendo verdadeira a premissa inicial (Ausência de guerras significa paz), os estudos de guerra e paz deveriam constituir um conjunto uniforme de pesquisa. Portanto, uma investigação testou a distribuição dos trabalhos científicos sobre paz e guerra em torno de seus dois pilares nominais. Para tanto, foi utilizado o Dimensions (https://app.dimensions.ai/discover/publication), um sistema de conhecimento de pesquisa vinculado, atribuindo "paz", "guerra" ou "paz e guerra" como palavras-chave e expressão para busca em todas as publicações contidas na base de dados (pouco mais de 119.092.422 publicações em 29 de maio de 2021). Estabeleceu-se o período compreendido entre 1990 e 2020.

The first finding is that studies on "war" have a dominant position over "peace". "War" was 4.4 to 2.5 times more cited in the last two decades. This is visualized in Figure 1a against Figure 1b. On average, 68% of publications dealing with "peace" also mention "war" (Figure 1b). But only 20% of publications on "war" mentioned "peace" (Figure1a). Therefore, it is evident that "peace" research is more concerned with the question of "war" than the opposite.

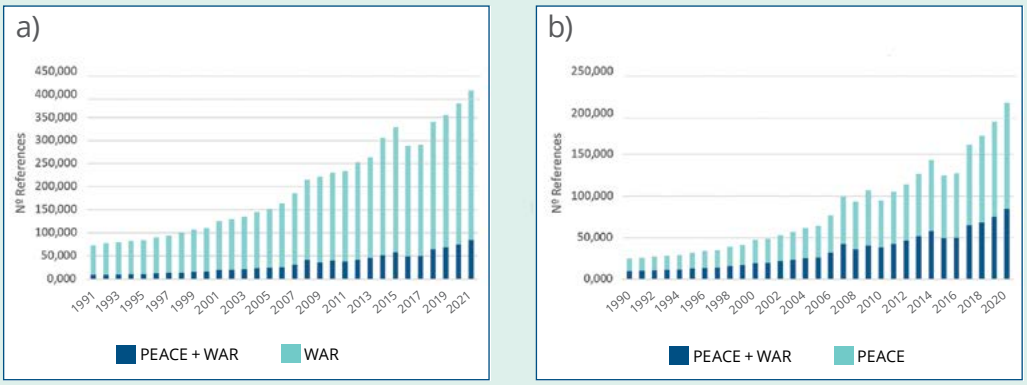


Figure 1. Results of the bibliometric study applying the program DIMENSIONS for the period of 1990 to 2020 using: a) the terms "war" and "peace and war", and b) "peace" and "peace and war".

Thus, overall, the three approaches reinforced the idea that peace and war studies seem to be a divided discipline. Or, that peace is something more than the mere absence of war.

The drivers of violence often include a wide range of factors, such as political, economic, social and environmental issues. They can include socio-economic inequalities, perceived or real injustice, a lack of jobs, conflict over natural resources and the distribution of their benefits, human rights violations, political exclusion, and grievances over corruption. In this context, food is one of the greatest and most affordable "weapons of peace" available to humanity. However, food security is one of the least recognized aspects since, in a historic perspective, it has improved dramatically worldwide. From 1991 to 2017, the number of undernourished people (i.e., those facing chronic food deprivation) declined globally. However, this number has increased over the last four years with the aggravating factor of the COVID-19 pandemic.

The definition of the term *Food Security* accepted by most authors refers mostly to Action Plan No. 1 derived from a meeting sponsored by the UN's Food and Agriculture Organization (FAO) in 1996: "Food security exists when all people, at all times, have physical and economic access to sufficient, safe and nutritious food to meet their dietary needs and food preferences for an active and healthy life." As a result, food security can be evaluated according to four categorical dimensions: availability, access and consumption/utilization, which are related to food flow, and finally, stability, which refers to the time dimension.

O primeiro achado é que estudos sobre “guerra” têm posição predominante em relação a estudos sobre “paz”. “Guerra” foi 4,4 a 2,5 vezes mais citada nas duas últimas décadas. Tal fato pode ser visualizado na Figura 1a em comparação com a Figura 1b. Na média, 68% das publicações sobre “paz” também mencionam “guerra” (Figura 1b). No entanto, apenas 20% das publicações sobre “guerra” mencionam “paz” (Figura 1a). Consequentemente, é evidente que as pesquisas sobre “paz” se preocupam mais com a questão da “guerra” do que o inverso.

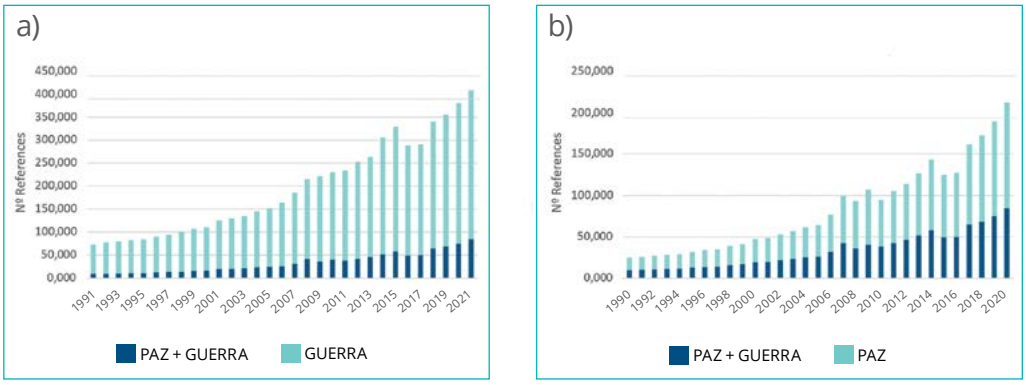


Figura 1. Resultados do estudo bibliométrico utilizando o programa DIMENSIONS para o período de 1990 a 2020 usando: a) os termos “guerra” e “paz e guerra”, e b) “paz” e “paz e guerra”.

Assim, de forma geral, as três abordagens reforçaram a ideia de que estudos de paz e guerra parecem ser uma disciplina segmentada. Ou, que paz é algo mais que a mera ausência de guerra.

Os motivos para a violência frequentemente incluem uma vasta gama de fatores, tais como questões políticas, econômicas, sociais e ambientais. Podem incluir desigualdades socioeconômicas, percepção de injustiça ou injustiça real, falta de empregos, conflitos por recursos naturais e a distribuição de seus benefícios, violações de direitos humanos, exclusão política e queixas sobre corrupção. Neste contexto, o alimento é uma das principais e mais acessíveis “armas da paz” disponíveis para a humanidade. A segurança alimentar, entretanto, é um dos aspectos menos reconhecidos pois, em perspectiva histórica, aumentou drasticamente em todo o mundo. De 1991 a 2017, o número de pessoas subnutridas (ou seja, pessoas enfrentando privação alimentar crônica) diminuiu globalmente. Contudo, este número vem aumentando ao longo dos últimos quatro anos, com o agravante da pandemia de COVID-19.

A definição do termo *Segurança Alimentar* aceita pela maioria dos autores refere-se principalmente ao Plano de Ação número 1, resultado de uma cúpula promovida pela Organização das Nações Unidas para a Alimentação e a Agricultura (FAO) em 1996: “Existe segurança alimentar quando as pessoas têm, a todo momento, acesso físico e econômico a alimentos seguros, nutritivos e suficientes para satisfazer as suas necessidades nutricionais e preferências alimentares, a fim de levarem uma vida ativa e sã.” Por conseguinte, a segurança alimentar pode ser avaliada de acordo com quatro dimensões categóricas: disponibilidade, acesso e consumo/utilização, que são relacionadas ao fluxo alimentar e, finalmente, estabilidade, que se refere à dimensão temporal.

According to FAO, Asia remains home to the greatest number of the undernourished (381 million) followed by Africa (250 million). Latin America and the Caribbean are in third position with 48 million hungry people, 7.4 percent of the entire population. An increase of 10 million compared to the 38 million people reported in 2014. Food insecurity, on the other hand, affects 187 million people in the Region. That is, 1 in 3 inhabitants of Latin American and the Caribbean countries did not have access to nutritious and sufficient food.

History tells us that lack of food — or fear of a lack of it — plays a central role in the genesis of human conflict and leads to civil unrest and, sometimes, to war. Not only is food insecurity a consequence of conflict, but it can also fuel and drive conflicts. That is to say, food insecurity is both an effect and cause of conflict.

The most obvious way a conflict leads to hunger is through the deliberate use of food as a weapon. Conflict reduces farming populations through direct attacks, terror, enslavement, forced recruitment, malnutrition, illness, and, finally, death. There are also situations of warring parties hijacking much of the food aid intended for non-combatants, using control of food to reward their supporters. Even terrorism strongly correlates with food. Not only because it undermines a country's productive capacity, but because it is frequently an important source of income or bargaining power for terrorist groups. On the other hand, extreme volatility in food prices, especially in urban areas, and acute food shortages have been found to spark unrest and trigger incidents of conflict across the world. When crops fail and prices rise, people do not have the money to purchase food, which can lead to stealing, riots, social unrest, and mass migrations. Likewise, both civil conflict and chronic food insecurity have something in common: they are generally associated with poverty and socioeconomic inequalities.

Most of the literature deals with conceptual/empirical issues in understanding the connections between food security and conflict on specific hotspots where several factors were dissected in order to determine what led to conflict. However, from an analytical point of view, it is important to consider all cases (conflict and non-conflict) in order to establish a pattern/model. Thus, we made an attempt at selecting some variables in order to represent a framework that attempts to capture the environmental, social and institutional factors that make the occurrence of conflicts and violence more likely. We used the 2018 databases of the Global Peace Index (GPI); Global Food Security Index (GFSI); Baseline Water Stress (BWS); Human Development Index (HDI); Gini Index; Gross Domestic Product (GDP); and Gross Domestic Product Per Capita (GDPPC). Considering the overlap of countries in the seven databases used, a total of 113 countries were the target of a simple correlation analyses for the present study.

De acordo com a FAO, a Ásia ainda apresenta o maior número de subnutridos (381 milhões), seguida pela África (250 milhões). A América Latina e o Caribe estão em terceiro lugar, com 48 milhões de pessoas com fome, o que corresponde a 7,4 por cento de toda sua população, com um aumento de 10 milhões em relação aos 38 milhões registrados em 2014. A insegurança alimentar, por outro lado, afeta 187 milhões de pessoas na região. Ou seja, um a cada três habitantes dos países da América Latina e do Caribe não tem acesso a alimentos nutritivos e suficientes.

A história nos mostra que a falta de alimentos — ou o medo de sua falta — tem um papel central na gênese de conflitos humanos, leva à agitação civil e, às vezes, à guerra. A insegurança alimentar não é apenas uma consequência de conflitos, podendo também inflamar e motivar conflitos. O que equivale a dizer que a insegurança alimentar é tanto efeito quanto causa de conflitos.

A maneira mais óbvia pela qual conflitos levam à fome é pelo uso intencional do alimento como arma. Conflitos reduzem populações agrícolas por meio de ataques diretos, terrorismo, escravidão, recrutamento forçado, desnutrição, doença e, finalmente, morte. Também há situações em que as partes em guerra sequestram boa parte da ajuda que chega em forma de alimentos destinados aos não-combatentes, controlando estes alimentos como forma de recompensar aqueles que lhes apoiam. Até o terrorismo tem uma forte correlação com os alimentos. Além de solapar a capacidade produtiva do país, alimentos frequentemente são uma fonte significativa de receita ou de poder de barganha para os grupos terroristas. Por outro lado, viu-se que tanto uma volatilidade extrema nos preços dos alimentos, especialmente em áreas urbanas, quanto sua pronunciada escassez podem incitar tumultos e deflagrar conflitos em diferentes partes do mundo. Quando a safra não é boa e há uma alta nos preços, a população não tem dinheiro para comprar alimentos, o que pode levar saques, tumultos, agitação social e migrações em massa. Ademais, o conflito civil e a insegurança alimentar crônica têm algo em comum: são geralmente associados à pobreza e às desigualdades socioeconômicas.

A maior parte da literatura aborda questões conceituais/empíricas no entendimento das conexões entre segurança alimentar e conflitos em localidades específicas, para as quais foram investigados vários fatores na tentativa de determinar a causa do conflito. No entanto, do ponto de vista analítico, é importante considerar todos os casos (de conflito e não-conflito) para estabelecer um padrão/modelo. Como exercício, selecionamos algumas variáveis para representar um arcabouço, na tentativa de identificar fatores ambientais, sociais e institucionais que aumentam a probabilidade da ocorrência de conflitos e violência. Utilizamos os bancos de dados de 2018 de: Índice Global da Paz (IGP); Índice Global de Segurança Alimentar (GFSI); Estresse Hídrico de Linha de Base (BWS); Índice de Desenvolvimento Humano (IDH); Índice Gini; Produto Interno Bruto (PIB); e Produto Interno Bruto per capita (PIB-pc). Levando em conta a sobreposição de países nos sete bancos de dados utilizados, 113 países, no total, foram alvo de uma análise simples de correlações para o presente estudo.

Table 1. Values of Pearson's Correlation Coefficient (r) among the seven variables.

	IGP2018	*GFSI2018*	*BWS 2018*	*PIB2018*	*PIB-pc2018*	*IDH2018*	*GINI2018*
IGP2018	1						
GFSI2018	-0,565	1					
BWS 2018	0,209	0,1678	1				
PIB2018	0,011	0,2813	0,0584	1			
PIB-pc2018	-0,531	0,7645	0,0155	0,282	1		
IDH2018	-0,535	0,9187	0,1780	0,248	0,751	1	
GINI2018	0,082	0,1112	0,0100	0,137	0,142	0,142	1

Obs.: If **r** in the table is greater than 0.242 one can conclude (at the 0.01 significance level) that there is a significant linear correlation.

The Global Peace Index (GPI) correlates significantly and negatively (P<0.01) with the Global Food Security Index (GFSI), the Human Development Index (HDI), and the Gross Domestic Product per Capita (GDPPC). One must bear in mind that the smaller the GPI score, the more peaceful the country. The idea of the influence of those three variables over peace corroborates the findings of most of the literature that deals with the conceptual connections among different conflicts. However, it is noteworthy that the Global Food Security Index (GFSI) is the most impacting variable related to the Global Peace Index (GPI), not only because of the highest **r**, but because GFSI is significantly correlated with both the Gross Domestic Product per Capita (GDPPC) and the Human Development Index (HDI).

Before COVID-19 emerged, there was already a food system crisis. COVID-19 has added new and amplified pre-existing stressors and shocks across the world. The pandemic is affecting food systems directly through impacts on food supply and demand, and indirectly through a decrease in purchasing power and in the capacity to produce and distribute food, which will have a differentiated impact on and will affect the poor and vulnerable more strongly.

The joint analysis by FAO and the World Food Programme (WFP) identifies 27 countries that are on the frontline of an impending COVID-19-driven food crisis. And five are located in Latin-America and the Caribbean (Haiti, Venezuela, Guatemala, Honduras, El Salvador, Nicaragua). Additionally, 3 countries (Peru, Ecuador, Colombia) are going through a regional migrant crisis what can aggravate food insecurity.

In spite of the uncertainties posed by the pandemic, FAO's first forecasts for the 2020/21 season point to a comfortable food commodity supply and demand situation. But the FAO Food Price Index (FFPI) averaged 120.9 points in April 2021, 2.0 points (1.7 percent) higher than in March, and as much as 28.4 points (30.8 percent) above the same period last year. The increase marked the eleventh consecutive monthly rise in the value of the FFPI to its highest level since May 2014. It is possible to find an example of this in the case of Latin America and the Caribbean. This region is one of the world's leading food producers and exporters, mainly because of Brazil. The

Tabela 1. Valores para o Coeficiente de Correlação de Pearson (r) entre as sete variáveis.

	IGP2018	*GFSI2018*	*BWS 2018*	*PIB2018*	*PIB-pc2018*	*IDH2018*	*GINI2018*
IGP2018	1						
GFSI2018	-0,565	1					
BWS 2018	0,209	0,1678	1				
PIB2018	0,011	0,2813	0,0584	1			
PIB-pc2018	-0,531	0,7645	0,0155	0,282	1		
IDH2018	-0,535	0,9187	0,1780	0,248	0,751	1	
GINI2018	0,082	0,1112	0,0100	0,137	0,142	0,142	1

Obs.: Se, na tabela, **r** for maior do que 0,242, pode-se concluir (no nível de significância 0,01) que há uma correlação linear importante.

O Índice Global da Paz (IGP) se correlaciona de maneira importante e negativamente (P<0,01) com o Índice Global de Segurança Alimentar (GFSI), o Índice de Desenvolvimento Humano (IDH), e o Produto Interno Bruto per capita (PIB-pc). Deve-se ter em mente que, quanto menor for o valor do IGP, mais pacífico é o país. A ideia da influência destas três variáveis sobre a paz corrobora os achados da maior parte da literatura que lida com as conexões conceituais entre os diferentes conflitos. Contudo, vale ressaltar que o Índice Global de Segurança Alimentar (GFSI) é a variável de maior impacto relacionada ao Índice Global da Paz (IGP) não somente devido ao **r** mais elevado, mas porque o GFSI apresenta correlação importante com o Produto Interno Bruto per capita (PIB-pc) e com o Índice de Desenvolvimento Humano (IDH).

Antes do surgimento da COVID-19, já havia uma crise dos sistemas alimentares. A COVID-19 acrescentou novos fatores de estresse e choques, e intensificou os fatores preexistentes ao redor do mundo. A pandemia afeta diretamente sistemas alimentares através de impactos sobre a oferta e demanda de alimentos e, indiretamente, através da diminuição do poder aquisitivo e da capacidade de produção e distribuição de alimentos, com impactos diferenciados e que afetarão mais fortemente os pobres e vulneráveis.

A análise conjunta da FAO e do Programa Mundial de Alimentos (WFP) identifica 27 países que estão na iminência de uma crise alimentar motivada pela COVID-19. Dentre estes, cinco se localizam na região da América Latina e do Caribe (Haiti, Venezuela, Guatemala, Honduras, El Salvador e Nicarágua). Ademais, 3 países (Peru, Equador e Colômbia) passam por crises migratórias regionais que podem agravar a insegurança alimentar.

Apesar das incertezas apresentadas pela pandemia, as primeiras previsões da FAO para a safra de 2020/21 indicam uma situação confortável de oferta e demanda de commodities alimentares. No entanto, o Índice de Preços de Alimentos da Organização das Nações Unidas para Alimentação e Agricultura (FFPI) teve média de 120,9 pontos em abril de 2021, configurando uma alta de 2,0 pontos (1,7%) em relação a março, ficando 28,4 pontos (30,8%) acima dos valores para o mesmo período do ano anterior. O aumento caracterizou o décimo primeiro mês consecutivo com aumento no valor do FFPI, alcançando seu valor mais elevado desde maio de 2014. Tal paradoxo pode ser exemplificado

region produces sufficient food to meet the needs of all its inhabitants. The central problem concerning hunger in the region is not a lack of food, but rather the result of poverty and economic inequality. And, within South America, Brazil was the country that showed the greatest impact on food insecurity related to COVID-19.

Since 2004, food insecurity has been decreasing in Brazil. In 2013, it reached the lowest number of households (22.6%) as measured by the National Household Sample Survey (PNAD). But, in 2017-2018, there was a worsening as 36.7% of households (25.3 million households) were diagnosed as suffering from food insecurity with about 84.9 million people experiencing food vulnerability. From then on, the situation worsened even more intensely. From 2018 to 2020, as shown by the VigiSAN survey, hunger increased by 27.6%. That is, in just two years, the number of people in severe food insecurity jumped from 10.3 million to 19.1 million. During this period, almost 9 million Brazilians began to experience hunger in their day-to-day life. In addition, food insecurity appears unevenly among regions. The worst cases are found in the North and Northeast regions, where less than half of the households had full and regular access to food. Reductions in government farmer support programmes, such as the PAA (Food Acquisition Program), which has shrunk since 2014, are likely to increase food insecurity. The PAA alone, operated by the National Supply Company (Conab), which had already sold the food produced by 128,804 family farmers in 2012, began to market the production of only 5,855 farmers in 2019.

POLICY RECOMMENDATIONS

The pandemic has exposed weaknesses of food systems' resilience, which has impacted food security at both local and global scales. Future shocks are expected and they can come from diverse causes, for example, related to the climate crisis or a new pandemic. Also depending upon the interactions with many environmental and social systems, domino effects should be considered for risk assessment worldwide. Thus, the world must be prepared, and the lessons learned during COVID-19 should be useful in foreseeing scenarios and the challenges policymakers are likely to face in the future.

One of the main characteristics of policies related to ensuring food security in Latin America and the Caribbean, especially Brazil, has been discontinuity.

Thus, considering future and possible shock scenarios, the overall approach to strengthening resilience in food systems needs to encompass the following frameworks/strategies/principles:

Political Dimension

- Declare food production, marketing, and distribution as essential services everywhere;
- It is suggested that countries create a crisis committee to deal with the impact of disruptive shocks on food supply, involving, among others, ministries of agriculture, livestock and food supply, transport, economy, trade, and so forth;

através do caso da América Latina e do Caribe. Esta região é uma das principais produtoras e exportadoras de alimentos, principalmente por causa do Brasil, com uma produção de alimentos suficiente para atender às necessidades de todos os seus habitantes. O problema central relativo à fome na região não é a falta de alimento, mas o resultado da pobreza e desigualdades econômicas. Na América do Sul, o Brasil foi o país que apresentou o maior impacto sobre insegurança alimentar relativo à COVID-19.

A insegurança alimentar vem diminuindo no Brasil desde 2004. Em 2013, atingiu o número mais baixo de domicílios (22,6%), conforme medição da Pesquisa Nacional por Amostra de Domicílios (PNAD). Em 2017-2018, no entanto, houve uma piora, com 36,7% dos domicílios (o equivalente a 25,3milhões de domicílios) diagnosticados como sofrendo insegurança alimentar, com cerca de 84,9 milhões de pessoas vivenciando vulnerabilidade alimentar. A partir de então, houve forte aceleração na piora. De 2018 a 2020, conforme pesquisa da VigiSAN, houve um aumento de 27,6% na fome. Ou seja, em apenas dois anos, o número de pessoas em situação de insegurança alimentar severa elevou-se de 10,3 milhões para 19,1 milhões. Durante este período, quase 9 milhões de brasileiros passaram a vivenciar a fome em seu dia a dia. A insegurança alimentar apresenta-se de forma desigual entre as diferentes Regiões do país. Os piores casos encontram-se nas Regiões Norte e Nordeste, onde menos da metade dos domicílios teve acesso pleno e constante a alimentos. A redução nos programas governamentais de auxílio a agricultores familiares, tais como o PAA (Programa de Aquisição de Alimentos), em acentuado encolhimento desde 2014, pode aumentar a insegurança alimentar. Somente o PAA, operacionalizado pela Companhia Nacional de Abastecimento (Conab), que já chegou a comercializar os alimentos produzidos por 128.804 agricultores familiares em 2012, passou a comercializar a produção de apenas 5,855 agricultores familiares em 2019.

RECOMENDAÇÕES DE POLÍTICAS

A pandemia expôs fragilidades na resiliência dos sistemas alimentares, com impactos na segurança alimentar em escala local e global. Esperam-se choques futuros, que podem se originar a partir de diferentes causas relacionadas, por exemplo, à crise climática ou a uma nova pandemia. Além disso, dependendo das interações com muitos sistemas ambientais e sociais, deve-se levar em conta o efeito dominó nas avaliações de risco ao redor do mundo. Portanto, o mundo precisa estar preparado, e as lições aprendidas durante a pandemia de COVID-19 devem ser úteis na previsão de cenários e desafios que os formuladores de políticas provavelmente enfrentarão no futuro.

A descontinuidade tem sido uma das principais características de políticas relacionadas à garantia de segurança alimentar na América Latina e no Caribe, especialmente no Brasil.

Assim, considerando cenários de choque possíveis e futuros, a abordagem geral para o reforço da resiliência em sistemas alimentares deve incluir os seguintes marcos/estratégias/princípios:

Dimensão Política

- Declarar a produção, a comercialização e a distribuição de alimentos como serviços essenciais em todos os lugares;

- Preserve critical humanitarian food, livelihood and nutrition assistance;
- Promote coordinated action between governments and other public and private actors to monitor food security indicators on time;
- Simplify administrative procedures to encourage retailers and businesses to donate food;
- Strengthen public and private donation campaigns to food banks, which are preparing for an increased demand;
- Inform and promote the reduction of food waste in urban areas;
- Inform about methods to reduce waste generation, recycle, reuse, or compost in rural areas;

Economical/Logistic Dimension

- Allow movement of seasonal workers and transport operators (e.g., truck drivers) across domestic and international borders;
- Adopt measures like "green corridors" for critical agricultural products and production materials such as fruits and vegetables to minimize hurdles in transport;
- In the absence of demand from the closing down of food services and restaurants, leverage the power of public procurement on essential agricultural supplies and ensure that market channels and logistics are still available to farmers;
- If possible, allow local markets to remain open, or, if feasible, relocate markets to larger spaces;
- Coordinate governments with NGOs, food banks, civil society and the private sector, to strengthen logistic mechanisms and enable food from social protection or school programmes to be distributed to those who need it most, contributing to the development of resilience in communities in need;
- Improve internet connectivity in rural areas, since e-commerce has become a resourceful tool to help farmers, consumers and logistics companies to better coordinate actions to increase the market mechanisms of supply and demand;
- Promote IT applications and social media as innovative ways to coordinate supplies of fresh produce from farm to consumers;
- Strengthen home delivery to ensure consumers' access to fresh and local products;

- Sugere-se que os países criem um comitê de crise para lidar com o impacto de choques que causem rupturas no fornecimento de alimentos, com o envolvimento, dentre outros, de ministros da agricultura, pecuária e abastecimento, dos transportes, da economia e do comércio;

- Preservar a assistência humanitária essencial alimentar, de renda e nutricional;

- Promover ações coordenadas entre governos e outros atores públicos e privados para o monitoramento oportuno de indicadores de segurança alimentar;

- Simplificar procedimentos administrativos para incentivar varejistas e empresas a doarem alimentos;

- Reforçar campanhas públicas e privadas de doações a bancos de alimentos, que estão se preparando para um aumento na demanda;

- Informar e promover a redução do desperdício alimentar em áreas urbanas;

- Informar sobre métodos para a redução na geração de resíduos, a reciclagem, o reuso, ou a compostagem em áreas rurais;

Dimensão Econômica/Logística

- Permitir a movimentação de trabalhadores sazonais e operadores de transportes (p. ex.: motoristas de caminhão) pelas divisas estaduais e fronteiras internacionais;

- Adotar medidas como "corredores verdes" para produtos agrícolas e materiais de produção críticos, como frutas e verduras, para minimizar os obstáculos no transporte;

- Na ausência de demanda devido ao fechamento de serviços alimentares e restaurantes, alavancar o poder de compras públicas de produtos agrícolas essenciais e garantir que canais de mercado e logística ainda estejam disponíveis para agricultores;

- Se possível, permitir que mercados locais permaneçam abertos, ou, se possível, realocar mercados para espaços maiores;

- Promover a coordenação de governos com ONGs, bancos de alimentos, a sociedade civil e o setor privado para fortalecer mecanismos de logística e permitir que alimentos de programas de proteção social ou programas escolares sejam distribuídos para aqueles em maior necessidade, contribuindo para o desenvolvimento da resiliência em comunidades carentes;

- Melhorar a conexão à internet em áreas rurais, pois o e-commerce (comércio eletrônico) tornou-se uma ferramenta flexível para auxiliar agricultores, consumidores e empresas de logística para melhor coordenarem ações que aumentem os mecanismos mercadológicos de oferta e demanda;

- Promover aplicações de TI e mídia social como formas inovadoras de coordenação da oferta de produtos frescos das fazendas para os consumidores;

Social Dimension

Gather essential information of needs specific to rural populations;

- Social protection systems need to be expanded to ensure ongoing access to food, and to ensure the resilience of food systems. They also need to be adapted to ensure that no disruptions occur in locations of possible future shock scenarios;
- Provide adequate social protection support to family farmers and those involved along food chains;
- Social protection interventions to protect income and support production throughout theagri-food system (e.g., distribution of seeds, market access, public purchases from familyproducers);
- Social assistance: non-contributory transfer programmes targeted to family farmers. Forinstance: social cash transfers, school feeding, food distribution, fee waivers, etc.;
- Food and nutrition assistance needs to be at the heart of social protection programmes to protect food access for the most vulnerable;

It should be reinforced that in the event of a health crisis linked to a new pandemic, the adequate health screening, testing, and safety protection measures should be guaranteed to all under any circumstances.

In conclusion, all governments should consider food production, marketing, and distribution as a critical infrastructure.

SOURCES CONSULTED OR RECOMMENDED

BELLINGER, N.; KATTELMAN, K.T. Domestic terrorism in the developing world: role of food security. **Journal of International Relations and Development**, v. 24, p. 306-332, 2021.

BREISINGER, C. et al. **How to Build Resilience to Conflict**: The Role of Food Security. Washington, DC: International Food Policy Research Institute, 2014. 38 p.

BRIGHT, J.; GLEDHILL, J. A divided discipline? Mapping peace and conflict studies. **International Studies Perspectives**, v. 19, p. 128–147, 2018.

BRÜCK, T.; d'ERRICO, M. Reprint of: Food security and violent conflict: Introduction to the special issue. **World Development**, v. 119, p. 145–149, 2019.

DIEHL, P.F. Exploring Peace: Looking Beyond War and Negative Peace. **International Studies Quarterly**, v. 60, p. 1–10, 2016.

FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS. **Social protection and COVID-19 response in rural areas**. Rome: FAO, 2020. 10 p. Available at: <https://doi.org/10.4060/ca8561en>. Accessed on: 25 May 2021.

- Fortalecer entregas domiciliares para garantir o acesso dos consumidores a produtos frescos e locais;

Dimensão Social

- Coleta de informações essenciais quanto às necessidades específicas de populações rurais;
- Sistemas de proteção social precisam ser expandidos para garantir acesso continuado a alimentos e garantir a resiliência de sistemas alimentares. Também precisam ser adaptados para garantir que não haja interrupções no caso de possíveis cenários futuros de choques;
- Fornecer o apoio de proteção social adequada para agricultores familiares e os envolvidos nas cadeias alimentares;
- Intervenções de proteção social para proteger a renda e apoiar a produção por todo o sistema agroalimentar (por exemplo, distribuição de sementes, acesso aos mercados, compras públicas de produtores familiares);
- Assistência social: programas de transferência não-contributivos tendo como alvo a agricultura familiar. Por exemplo: transferências sociais de dinheiro, alimentação escolar, distribuição alimentar, isenção de tarifas etc.;
- A assistência alimentar e nutricional deve compor o cerne de programas de proteção social para proteger o acesso a alimentos para os mais vulneráveis;

Deve-se ressaltar que, no caso de uma crise de saúde relacionada à nova pandemia, a triagem, os exames e as medidas de proteção devem ser garantidos a todos em qualquer circunstância.

Concluindo, todos os governos deveriam considerar a produção, a comercialização e a distribuição de alimentos como infraestrutura crítica.

FONTES CONSULTADAS OU RECOMENDADAS

BELLINGER, N.; KATTELMAN, K.T. Domestic terrorism in the developing world: role of food security. **Journal of International Relations and Development**, v. 24, p. 306-332, 2021.

BREISINGER, C. et al. **How to Build Resilience to Conflict:** The Role of Food Security. Washington, DC: International Food Policy Research Institute, 2014. 38 p.

BRIGHT, J.; GLEDHILL, J. A divided discipline? Mapping peace and conflict studies. **International Studies Perspectives**, v. 19, p. 128–147, 2018.

BRÜCK, T.; d'ERRICO, M. Reprint of: Food security and violent conflict: Introduction to the special issue. **World Development**, v. 119, p. 145–149, 2019.

_____. **Responding to the impact of the COVID-19 outbreak on food value chains through efficient logistics**. Rome: FAO, 2020. 4 p. Available at: <https://doi.org/10.4060/ca8466en>. Accessed on: 25 May 2021.

_____. WORLD FOOD PROGRAMME. **FAO-WFP early warning analysis of acute food insecurity hotspots.** FAO: Rome, 2020. 24 p. Available at: <http://www.fao.org/3/cb0258en/CB0258EN.pdf>. Accessed on: 25 May 2021.

_____ et al. **The State of Food Security and Nutrition in the World 2020**: Transforming food systems for affordable healthy diets. Rome: FAO, 2020. 320 p. Available at: <https://doi.org/10.4060/ca9692en>. Accessed on: 16 Nov. 2020.

_____ et al. **Panorama de la seguridad alimentaria y nutrición en América Latina y el Caribe 2020**. Santiago de Chile: FAO, OPS, WFP and UNICEF, 2020. 132 p. Available at: <https://doi.org/10.4060/cb2242es>. Accessed on: 24 May 2021.

HENDRIX, C.; BRINKMAN, H. Food Insecurity and Conflict Dynamics: Causal Linkages and Complex Feedbacks. **Stability**: International Journal of Security & Development, v. 2, n. 2, art. 26, 2013.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. 10,3 milhões de pessoas moram em domicílios com insegurança alimentar grave. **Agência de Notícias IBGE**, Rio de Janeiro, 17 set. 2020. Available at: <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de noticias/noticias/28903-10-3-milhoes-de-pessoas-moram-em-domicilios-com- inseguranca-alimentar-grave>. Accessed on: 24 May 2021.

INSTITUTE FOR ECONOMICS & PEACE. **Global Peace Index 2016**. Sydney: IEP, 2016. Available from: <https://www.economicsandpeace.org/wp- content/uploads/2016/06/GPI-2016-Report_2.pdf>. Accessed on: 26 May 2021.

KUSCH-BRANDT, S. Towards More Sustainable Food Systems—14 Lessons Learned. **Int. J. Environ. Res. Public Health**, v. 17, art. 4005, 2020. doi:10.3390/ijerph17114005.

PENSSAN. **VIGISAN**: Inquérito Nacional sobre Insegurança Alimentar no Contexto da Pandemia da Covid-19 no Brasil. S.l.: Rede Penssan, 2021. Available at: <http://olheparaafome.com.br/VIGISAN_Inseguranca_alimentar.pdf>. Accessed on: 23 May 2021.

PETTERSSON, T.; ÖBERG, M. Organized violence, 1989-2019. **Journal of Peace Research**, v. 57, n. 4, p. 597–613, 2020.

SALAZAR, L. et al. **Una mirada regional a la seguridad alimentaria en América Latina y el Caribe durante el primer año de COVID-19**. Washington, D.C.: Inter-American Development Bank, 2021. Available at: <https://publications.iadb.org/publications/spanish/document/Una-mirada- regional-a-la-seguridad-alimentaria-en-America-Latina-y-el-Caribe-durante-el- primer-ano-de-COVID-19.pdf>. Accessed on: 25 May 2021.

SEDIK, T. S.; XU, R. A **Vicious Cycle**: How Pandemics Lead to Economic Despair and Social Unrest. Washington, D.C.: International Monetary Fund, 2020. 22p. (Working Paper No. 2020/216). Available at: <https://www.imf.org/media/Files/Publications/WP/2020/English/wpiea2020216-print-pdf.ashx>. Accessed on: 25 May 2021.

DIEHL, P.F. Exploring Peace: Looking Beyond War and Negative Peace. **International Studies Quarterly**, v. 60, p. 1–10, 2016.

FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS. **Social protection and COVID-19 response in rural areas.** Roma: FAO, 2020. 10 p. Disponível em: <https://doi.org/10.4060/ca8561en>. Acessado em: 25 maio 2021.

_____. **Responding to the impact of the COVID-19 outbreak on food value chains through efficient logistics.** Roma: FAO, 2020. 4 p. Disponível em: <https://doi.org/10.4060/ca8466en>. Acessado em: 25 maio 2021.

_____. WORLD FOOD PROGRAMME. **FAO-WFP early warning analysis of acute food insecurity hotspots.** FAO: Roma, 2020. 24 p. Disponível em: <http://www.fao.org/3/cb0258en/CB0258EN.pdf>. Acessado em: 25 maio 2021.

_____ et al. **The State of Food Security and Nutrition in the World 2020**: Transforming food systems for affordable healthy diets. Roma: FAO, 2020. 320 p. Disponível em: <https://doi.org/10.4060/ca9692en>. Acessado em: 16 nov. 2020.

_____ et al. **Panorama de la seguridad alimentaria y nutrición en América Latina y el Caribe 2020**. Santiago de Chile: FAO, OPS, WFP e UNICEF, 2020. 132 p. Disponível em: <https://doi.org/10.4060/cb2242es>. Acessado em: 24 maio 2021.

HENDRIX, C.; BRINKMAN, H. Food Insecurity and Conflict Dynamics: Causal Linkages and Complex Feedbacks. **Stability**: International Journal of Security & Development, v. 2, n. 2, art. 26, 2013.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. 10,3 milhões de pessoas moram em domicílios com insegurança alimentar grave. **Agência de notícias BGE**, Rio de Janeiro, 17 set. 2020. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/28903-10-3-milhoes-de-pessoas-moram-em-domicilios-com-inseguranca-alimentar-grave>. Acessado em: 24 maio 2021.

INSTITUTE FOR ECONOMICS & PEACE. **Global Peace Index 2016**. Sydney: IEP, 2016. Disponível em: <https://www.economicsandpeace.org/wp- content/uploads/2016/06/GPI-2016-Report_2.pdf>. Acessado em: 26 maio 2021.

KUSCH-BRANDT, S. Towards More Sustainable Food Systems—14 Lessons Learned. **Int. J. Environ. Res. Public Health**, v. 17, art. 4005, 2020. doi:10.3390/ijerph17114005.

PENSSAN. **VIGISAN**: Inquérito Nacional sobre Insegurança Alimentar no Contexto da Pandemia da Covid-19 no Brasil. S.l.: Rede Penssan, 2021. Disponível em: <http://olheparaafome.com.br/VIGISAN_Inseguranca_alimentar.pdf>. Acessado em: 23 maio 2021.

PETTERSSON, T.; ÖBERG, M. Organized violence, 1989-2019. **Journal of Peace Research**, v. 57, n. 4, p. 597–613, 2020.

SALAZAR, L. et al. **Una mirada regional a la seguridad alimentaria en América Latina y el Caribe durante el primer año de COVID-19**. Washington, D.C.: Inter-American Development Bank, 2021. Disponível em: <https://publications.iadb.org/publications/spanish/document/Una-mirada-regional-a-la-seguridad-alimentaria-en-America-Latina-y-el-Caribe-durante-el-primer-ano-de-COVID-19.pdf>. Acessado em: 25 maio 2021.

SENRA, R. **Como o mesmo Brasil que alimenta 1 bilhão ultrapassou 10 milhões de famintos 'dentro de casa'**? BBC, 2020. Available at: <https://www.bbc.com/portuguese/brasil-54288952>. Accessed on: 23 May 2021.

WEBB, P.; FLYNN, D.J.; KELLY, N.M.; THOMAS, S.M.; BENTON, T.G. COVID-19 and Food Systems: Rebuilding for Resilience. New York: United Nations, 2021. (United Nations Food Systems Summit 2021). Available at: <https://sc- fss2021.org/wp-content/uploads/2021/05/FSS_Brief_COVID- 19_and_food_systems.pdf>. Accessed on: 25 May 2021.

WORLD FOOD PROGRAM USA. **Winning the Peace**: Hunger and Instability. Washington, D.C.: World Food Program USA, 2017. 103 p. Available at: <https://www.wfpusa.org/wp-content/uploads/2019/03/wfp_food_security_final- web-1.pdf>. Accessed 26 Oct. 2020.

SEDIK, T. S.; XU, R. A **Vicious Cycle**: How Pandemics Lead to Economic Despair and Social Unrest. Washington, D.C.: International Monetary Fund, 2020. 22p. (Working Paper No. 2020/216). Disponível em: <https://www.imf.org/- /media/Files/Publications/WP/2020/English/wpiea2020216-print-pdf.ashx>. Acessado em: 25 maio 2021.

SENRA, R. **Como o mesmo Brasil que alimenta 1 bilhão ultrapassou 10 milhões de famintos 'dentro de casa'?** BBC, 2020. Disponível em: <https://www.bbc.com/portuguese/brasil-54288952>. Acessado em: 23 maio 2021.

WEBB, P.; FLYNN, D.J.; KELLY, N.M.; THOMAS, S.M.; BENTON, T.G. COVID-19 and Food Systems: Rebuilding for Resilience. New York: United Nations, 2021. (United Nations Food Systems Summit 2021). Disponível em: <https://sc-fss2021.org/wp-content/uploads/2021/05/FSS_Brief_COVID- 19_and_food_systems.pdf>. Acessado em: 25 maio 2021.

WORLD FOOD PROGRAM USA. **Winning the Peace**: Hunger and Instability. Washington, D.C.: World Food Program USA, 2017. 103 p. Disponível em: <https://www.wfpusa.org/wp-content/uploads/2019/03/wfp_food_security_final-web-1.pdf>. Acessado em: 26 out. 2020.

Irene Giner-Reichl

A Dra. Irene Giner-Reichl, diplomata aposentada, trabalhou extensamente com questões globais e desenvolvimento sustentável. Serviu como Representante Permanente da Áustria nas Nações Unidas, foi Diretora Geral de Desenvolvimento e Embaixadora na China e no Brasil.

Dr. Irene Giner-Reichl, former diplomat, has worked extensively on global issues and sustainable development. She served as Austria's Permanent Representative to the UN in Vienna, Director General for Development, and Ambassador to the PR of China and Brazil.

Garantir a segurança energética através de uma Transição Inclusiva, uma dimensão crucial em qualquer Estratégia de Segurança Internacional

Ensuring Energy Security through Inclusive Energy Transitions, a Crucial Dimension of any International Security Strategy

Irene Giner-Reichl

Resumo executivo

Garantir o acesso confiável ao fornecimento necessário de energia tem sido, desde sempre, uma dimensão de estratégias de segurança em qualquer nível. Os atuais sistemas de energia não conseguem oferecer segurança energética, nem agora nem no futuro. As mudanças climáticas são uma ameaça real à subsistência de milhões de pessoas, aos assentamentos (incluindo grandes cidades) em áreas costeiras, e à estabilidade e ao bem-estar global. Os compromissos globais para proteger o sistema climático precisam de uma drástica reorientação dos sistemas de energia em direção a sistemas de baixo ou zero carbono nos próximos vinte anos.

A necessária transição energética deve acontecer tendo como pano de fundo a importante mudança no centro de gravidade mundial do ocidente para o oriente. A atual rivalidade bipolar entre as superpotências Estados Unidos-China é alimentada pela competição tecnológica. Os Estados Unidos e a América Latina precisam estabelecer uma cooperação tecnológica para proteger seus interesses. A segurança energética é um pré-requisito fundamental para os avanços tecnológicos.

Executive Summary

Ensuring reliable access to needed energy supplies has long been a dimension of security strategies at any level. Current energy systems cannot deliver energy security, neither now nor in the future. Climate change is a real threat to the livelihood of millions of people, to settlements (including major cities) in low coastal areas, and to global stability and well-being. Global commitments to protect the climate system necessitate a drastic reorientation of energy systems towards low/zero-carbon systems in the next twenty years.

The necessary energy transitions must occur against the backdrop of major shifts of the world's centres of gravity from the West to the East. The current bipolar US-China super-power rivalry is fuelled by technological competition. The EU and Latin America need to engage in technological cooperation to safeguard their interests. Energy security is a key pre-requisite for technological advances.

Orderly, well-planned, inclusive and participatory energy transitions are key for ensuring energy security in the future. They constitute an important pillar of any serious international security strategy in the new global order.

Part I. Setting the Stage: the Current International Context

For some time now, the epicentres of power – economically, demographically and politically – have been moving from the Western to the Eastern hemisphere. The West can no longer take for granted support for its values and principles. The rules-based international order to which the EU and Latin America attach importance is under increasing pressure from various directions.

The emerging international architecture is clearly bipolar, defined by the relationship between the "old" super-power USA and the emerging super-power China. According to Yan Xuetong, professor at Beijing's renowned Tsinghua University and policy advisor to his government, this bipolarity exhibits characteristics that are different from the cold war bipolarity. During the cold war superpower rivalry was expressed through the arms race; mutually exclusive zones of interest and influence were established. Today's superpower struggle occurs in the context of globalisation's multiple entanglements; it is waged mainly in the field of technology (especially digitalisation, 5G and artificial intelligence).

Technological superiority can neither be maintained nor achieved without vast, diverse and international cooperative networks. The future, therefore, Yan Xuetong concludes, most likely will not lead to major interstate war. But there will be behaviours and situations which will impact negatively on security, on state security and even more on human security: double dealing, treaty infringements, cyberattacks, technological decoupling etc.

The Covid-19 pandemic has reinforced the power shifts from the West to the East. China emerges as the only major economy with absolute growth in 2021 vis-a-vis 2019 while many other countries – especially middle-income countries – see years of social progress wiped out. Reactions to the pandemic have strengthened the agency of governments to the point of reinforcing totalitarian tendencies, as governments chose national responses over multilateral approaches. This weakened international solidarity further.

The pandemic has also accelerated digitalisation. The existing digital divide has disadvantaged underserved communities even more acutely.

Part II. The Problem: Energy Insecurity

Energy poverty is a source of acute insecurity for individuals, communities and indeed nations. Unsustainable energy systems are also a major source of greenhouse gas emissions, and thus are directly linked to global warming. Global warming is arguably the greatest threat to security: to international security, because of its

As transições energéticas organizadas, bem planejadas, inclusivas e participativas são fundamentais para garantir a segurança energética no futuro. Elas constituem um pilar importante de toda estratégia de segurança internacional séria na nova ordem mundial.

Parte I. Preparando o cenário: o atual contexto internacional

Já há algum tempo, os epicentros do poder econômico, demográfico e político estão se deslocando do hemisfério ocidental para o hemisfério oriental. O ocidente não pode mais pressupor o apoio a seus valores e princípios. A ordem internacional baseada em regras às quais a União Europeia e a América Latina atribuem importância está sob crescente pressão oriunda de diversos lugares.

A arquitetura internacional emergente é claramente bipolar, definida pela relação entre a "antiga" superpotência, os Estados Unidos, e a superpotência emergente, a China. De acordo com Yan Xuetong, professor da famosa Universidade Tsinghua de Beijing e assessor político do governo, esta bipolaridade tem características diferentes da bipolaridade da guerra fria. Durante a guerra fria, a rivalidade das superpotências se expressava através de uma corrida armamentista; áreas de interesse e de influência mutuamente exclusivas eram estabelecidas. Hoje, a disputa das superpotências se dá em um contexto de globalização com múltiplas ramificações; e se trava, principalmente, na área da tecnologia (especialmente digitalização, 5G e inteligência artificial).

A superioridade tecnológica não pode ser alcançada e nem mantida sem uma ampla e variada rede de cooperação internacional. O futuro, portanto, conclui Yan Xuetong, muito provavelmente não nos levará a uma grande guerra entre estados. Mas haverá comportamentos e situações que terão um impacto negativo na segurança, na segurança do estado e ainda mais na segurança humana: jogo duplo, violações aos tratados, ataques cibernéticos, distanciamento tecnológico etc.

A pandemia da Covid-19 reforçou o deslocamento do poder do ocidente para o oriente. A China emerge como a única grande economia com crescimento absoluto em 2021 em relação a 2019, enquanto muitos outros países, especialmente países em desenvolvimento, vêm anos de avanços sociais serem destruídos. As reações à pandemia fortaleceram os órgãos governamentais a ponto de reforçar tendências totalitárias, na medida em que, como governos, priorizam respostas nacionais em relação a visões multilaterais. Isso enfraquece ainda mais a solidariedade internacional.

A pandemia também acelerou a digitalização. O abismo digital existente deixou em desvantagem ainda maior às comunidades vulneráveis.

Parte II. O Problema: Insegurança energética

A escassez energética é uma fonte de grande insegurança para os indivíduos, as comunidades e até mesmo as nações. Sistemas de energia insustentável também são uma fonte importante de emissão de gases de efeito estufa e, por isso, estão diretamente relacionados ao aquecimento global. O aquecimento global é, sem dúvida, a maior ameaça à

potential to uproot populations and cause large migratory movements, and to security of communities and individuals, because of the cascading negative effects once ecosystems reach tipping points.

Just energy transitions are the antidote to the insecurities of energy poverty and of climate change. Energy transition strategies need to be part and parcel of any serious security strategy.

Current energy systems do not ensure energy security

The global current energy situation is unsustainable:

- Because it withholds access to modern energy services to more than a third of the world's population: 840 million people are currently without access to electricity; close to three billion people without access to clean cooking solutions;
- Because it continues to rely heavily on fossil fuels[1] which is incompatible with stabilizing the global climate as per the Paris Climate Agreement;
- Because it continues to fan inter- and intra-state tensions and conflicts.

The international community had included "sustainable energy for all" as one of the SDGs in the Agenda 2030, adopted in 2015 by consensus in the UN General Assembly, as the blueprint for future worldwide development. SDG 7 on "sustainable energy for all", however, is currently not on track for complete and timely implementation. And even if it were fully implemented, it would not ensure global energy security. **The continuation of current trends would actually undermine global safety and prosperity** in general by further intensifying global warming beyond the 1.5 degrees Celsius established as a goal at the Paris Climate Conference. It would furthermore continue to place a significant portion of the world population into severe energy poverty characterised by lack of access to electricity (estimated 620 million in 2030) and/or lack of access to clean cooking (estimated 2.3 billion in 2030). Because of insufficient progress on energy efficiency, valuable resources would continue to be wasted and development opportunities missed.

This is the **bad news**.

In order to stabilise the global climate as agreed in Paris, the world must stop emitting greenhouse gases by 2050 and move towards negative emissions beyond that date. The **good news** is that renewables have become cost-effective for electricity generation in practically all regions of the world. Safe ways of integrating high amounts of intermittent renewable energy sources are practiced by grids around the world[2].

---

[1] In 2018, the global final energy consumption was about 378 Exajoules. According to REN21 Global Status Report 2020, p. 32 (www.ren21.net)79,9 % of it are met by fossil fuels; 11,0 % are met by modern renewables; 2,2 % by nuclear energy and 6,9 % by traditional biomass.

[2] https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2015/IRENA-ETSAP_Tech_Brief_Power_Grid_Integration_2015.pdf, page 22

segurança: à segurança internacional, devido ao seu potencial de deslocar populações e causar grandes movimentos migratórios, e à segurança de comunidades e indivíduos, devido aos efeitos negativos em cascata uma vez que os ecossistemas cheguem ao ponto de não retorno.

A transição energética justa é o antídoto para as inseguranças da escassez energética e das mudanças climáticas. As estratégias de transição energética precisam ser parte integrante de qualquer estratégia séria de segurança.

Os sistemas atuais de energia não garantem segurança energética

A atual situação energética global é insustentável:

- Porque impede o acesso a serviços de energia modernos a mais de um terço da população mundial: 840 milhões de pessoas atualmente não têm acesso à eletricidade; quase 3 bilhões de pessoas sem acesso a soluções para cozinhar de forma limpa;
- Porque continua dependendo fortemente de combustíveis fósseis,[1] o que é incompatível com a estabilização do clima global tal como consta do Acordo de Paris sobre o clima;
- Porque continua a incentivar tensões e conflitos inter- e intraestados.

A comunidade internacional incluiu "energia sustentável para todos" como um dos objetivos da Agenda 2030 para o Desenvolvimento Sustentável da, adotada por consenso em 2015 na Assembleia Geral das Nações Unidas, como um modelo para o desenvolvimento futuro do mundo todo. O ODS 7 sobre "energia sustentável para todos", no entanto, não está no caminho correto para sua completa e oportuna implementação. E, ainda que fosse plenamente implementado, não garantiria a segurança energética global. **A continuidade das tendências globais irá, na verdade, prejudicar a prosperidade e a segurança globais** em geral ao aumentar ainda mais o aquecimento global além do 1,5 grau Celsius estabelecido como objetivo na Conferência de Paris sobre o Clima. Além do mais, irá manter uma parte significativa da população mundial sob uma escassez energética extrema caracterizada pela falta de acesso à eletricidade (estimada em 620 milhões de pessoas em 2030) e/ou à falta de acesso a formas limpas para cozinhar (estimada em 2.3 bilhões de pessoas em 2030). Devido ao avanço insuficiente na eficiência energética, recursos valiosos continuarão sendo desperdiçados e oportunidades de desenvolvimento perdidas.

Essas são as **más notícias**.

Para conseguir estabilizar o clima global como acordado em Paris, o mundo precisa parar de emitir gases de efeito estufa em 2050 e avançar rumo a emissões negativas após essa data. A **boa notícia** é que as energias renováveis se tornaram custo-efetivas para a geração de eletricidade em praticamente todas as regiões do mundo. Formas

[1] Em 2018, o consumo de energia total global foi de aproximadamente 378 Exajoules. De acordo com o Relatório da Situação Global REN21 2020, p. 32 (www.ren21.net) 79,9% correspondem a combustíveis fósseis; 11,0% a renováveis modernos; 2,2% à energia nuclear e 6,9%àa biomassa tradicional.

Technologies are ripe and analysis is abundant. To decarbonise the energy sector, interventions from companies and citizens are needed; the finance sector needs to align to this goal as well. Government policies are essential to steer decisions in the right direction.

Part III: The Solution: Just Transitions to Low/Zero Carbon Energy Systems

Decarbonisation Is a Must and Is Possible

Currently, roughly 80 % of the global final energy consumption is made up by fossil fuels; the energy system is responsible for about two thirds of global greenhouse gas emissions and for an estimated 4 million premature deaths as a result of air pollution, especially in developing countries' mega-cities.

Clearly, the **global energy system must be decarbonised in order to be future-ready**. The task at hand is Herculean and the time to do it is very limited. There is a silver lining: renewable-based technologies – at least for the electricity sector – are mature and price-competitive in practically all regions of the world. Financing is shifting away from fossils to renewables and renewables' stocks are rising[3]. Consumer awareness is growing. Small – but growing - numbers of people attempt to consciously adopt low-carbon lifestyles and cultivate behaviours such as buying locally, recycling and re-using, sharing (instead of owning), un-cluttering and decelerating (slowing down). Digitalisation and smart grids will hasten the electrification of overall energy use, making it also more efficient, and blur the lines between producers and consumers, thereby creating new democratic and participatory decision-making processes.

The major challenges ahead are in the area of **clean cooking, transport and thermal applications** (heating and cooling). These challenges can be solved by appropriate policies and adequate regulation – in particular, putting a price on carbon - that stimulates market-based solutions which have driven the energy transition to a large degree until now.

Energy Transitions need to be Inclusive and Favour Diversity

Currently the energy sector shows a sharp under-representation of women and a general lack of diversity at all levels. According to IRENA, women represent at best 33 % of the workforce in renewables. When it comes to STEM jobs and to leadership positions in corporations, women's representation is still lower. The persistence of gender stereotypes and unconscious bias make it hard for women to enter the sector at all, or – if they have entered – to advance on a par with their male colleagues. While this situation is unacceptable on human rights grounds, it is also undesirable from an economic and developmental standpoint. Analysis from actors as diverse as the World

[3] https://about.bnef.com/clean-energy-investment/

seguras de integrar grandes quantidades de energias renováveis intermitentes são utilizadas em muitas redes no mundo[2].

As tecnologias estão maduras e há análises em abundância. Para descarbonizar o setor energético, são necessárias intervenções das empresas e dos cidadãos; o setor financeiro também precisa se alinhar a este objetivo. As políticas governamentais são essenciais para orientar as decisões na direção correta.

Parte III. A solução: Transição justa a sistemas de energia de zero ou baixo carbono

A descarbonização é uma necessidade e é possível

Atualmente, aproximadamente 80% do consumo de energia final global é composto por combustíveis fósseis; o sistema de energia é responsável por quase 2/3 das emissões de gases de efeito estufa e por uma estimativa de 4 milhões de mortes prematuras causadas pela poluição do ar, principalmente nas megacidades dos "países em desenvolvimento".

Claramente, o **sistema energético global precisa ser descarbonizado para estar preparado para o futuro.** A tarefa em questão é hercúlea e o prazo para realizá-la é muito limitado. O aspecto positivo é que as tecnologias renováveis, pelo menos para o setor elétrico, estão maduras e são competitivas em termos de preço em quase todas as regiões do mundo. O financiamento está se deslocando de fósseis para renováveis e as ações das renováveis estão subindo[3]. O consumidor está mais consciente. Um número pequeno, porém crescente, de pessoas, tem tentado adotar conscientemente um estilo de vida de baixo carbono e cultivar comportamentos como comprar localmente, reciclar, reutilizar, compartilhar (ao invés de possuir), desapegar e desacelerar (ir mais devagar). A digitalização e as redes inteligentes irão incrementar a eletrificação do uso geral de energia, tornando-o mais eficiente, e eliminando a separação entre produtores e consumidores, criando, portanto, novos processos de tomada de decisões mais democráticos e participativos.

Os principais desafios que temos pela frente são **cozinhar de forma limpa, o transporte e os usos térmicos** (calefação e refrigeração). Estes desafios podem ser resolvidos com políticas adequadas e regulamentação apropriada — em particular colocando um preço no carbono — que estimule soluções baseadas no mercado que elevem a transição energética ao seu mais alto nível até hoje.

A transição energética precisa ser inclusiva e favorecer a diversidade

Atualmente, o setor energético mostra uma acentuada sub representação das mulheres e uma falta de diversidade generalizada em todos os níveis. De acordo com IRENA, as mulheres representam no máximo somente 33% da força de trabalho das renováveis.

[2] https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2015/IRENA-ETSAP_Tech_Brief_Power_Grid_Integration_2015.pdf, pág. 22.

[3] https://about.bnef.com/clean-energy-investment/

Bank, McKinsey and the World Economic Forum show clearly that diversity is good for the bottom line of companies and for the development of national economies and societies. The renewables sector is projected to grow from providing employment to roughly 11 million people worldwide today to 42 million in 2050; women need to be able to participate in and contribute to the growth of the sector. Leaders in the field already implement a wide variety of approaches to help level the playing field for women in sustainable energy.[4]

Energy transitions entail much more than shifting from a fossil fuel to a renewable one; they are deep societal transformations and will present many challenges. Therefore, it is imperative that they are able to draw on all available expertise, life experience and talent.

Multilateral processes need to be optimised

The absence of good multilateral processes to help in the transformation adds to the challenge. Where can the necessary deals be made which compensate for losses and promote social and technological innovation and demand-side management? While SDG 7 is part of the consensually agreed Agenda 2030, there are no multilateral fora in which to debate, let alone to address the multifaceted challenges of the global energy transition in an integrated fashion. UNFCCC has been bogged down in intense battles over preserving short term vested interests of certain groupings at the expense of sustainability. There are many technical organisations which are doing valuable work, IOs like IRENA and UNIDO; policy-networks like REN21; international NGOs like SEforALL (Sustainable Energy for All) or GWNET (Global Women´s Network for the Energy Transition); they attempt to build consensus on the aspects of energy transitions that pertain to their specialised mandates. But there is no place yet to come together and work out compensatory schemes or look at issues holistically.

Wealth Displacement Needs to be Addressed Pro-Actively at All Levels of Governance

The needed new policies to usher in low- or zero-carbon energy systems will by necessity displace wealth generation – e.g., away from coal mines, SUV manufacturers and oil companies – with potentially severe impacts on prevailing employment and income situations. At the **national level**, governments will need to find ways to **buffer this wealth generation displacement through appropriate measures,** such as re-training of the labour force, fostering of new economic opportunities, and, where needed, social transfer schemes.

[4] Many examples are given in the study commissioned by the Global Women's Network for the Energy Transition (GWNET), entitled „Women for Sustainable Energy. Fostering Women's Talent for Transformational Change. Austria, 2019."

No que diz respeito às carreiras de ciências, tecnologia, engenharia e matemática e aos cargos de liderança nas empresas, a representatividade das mulheres é ainda menor. A persistência de estereótipos de gênero e o viés inconsciente torna ainda mais difícil a entrada das mulheres neste setor ou se entram nele, não conseguem alcançar o mesmo nível de seus colegas homens. Esta é uma situação inaceitável na perspectiva dos direitos humanos, e é indesejável do ponto de vista econômico e do desenvolvimento. Análises de entidades tão diferentes quanto o Banco Mundial, McKinsey e o Fórum Econômico Mundial mostram claramente que a diversidade é boa para os resultados das empresas e para o desenvolvimento das sociedades e das economias nacionais. Projeta-se um crescimento do setor de renováveis no número de empregos dos atuais 11 milhões aproximadamente para 42 milhões em 2050. As mulheres precisam poder participar e contribuir para o crescimento do setor. Líderes na área já implementam uma série de estratégias para ajudar a oferecer condições equitativas para as mulheres na energia sustentável[4].

A transição energética acarreta muito mais do que uma mudança do combustível fóssil para um renovável, é uma transformação profunda na sociedade e vai apresentar muitos desafios. Por isso, é imperativo que possa aproveitar todo o talento, experiência de vida e conhecimento disponível.

Os processos multilaterais precisam ser otimizados

A ausência de bons processos multilaterais para ajudar na transformação aumenta o desafio. Onde se darão as necessárias negociações para compensar as perdas e promover a inovação social e tecnológica e a gestão do lado da demanda? Enquanto o OSD 7 faz parte da Agenda 2030 acordada por consenso, não existe um fórum multilateral no qual se possa debater, sem falar em lidar com os desafios multifacetados da transição energética global de forma integrada. A CQNUMC se viu atolada em intensas batalhas de interesses próprios de curto prazo de determinados grupos a expensas da sustentabilidade. Existem muitas organizações técnicas que estão fazendo um trabalho valioso, organizações internacionais como IRENA e UNIDO; redes de políticas como a REN21; ONGs internacionais como a SEforALL (Energia Sustentável para Todos) ou a GWNET (Rede Global de Mulheres pela Transição Energética); elas tentam criar consensos nos aspectos da transição energética que diz respeito aos seus mandatos especializados. Mas ainda falta um lugar onde se possam reunir e encontrar esquemas compensatórios ou pensar as questões de forma holística.

O deslocamento da riqueza precisa ser abordado de forma pró ativa em todos os níveis de governança

As novas políticas essenciais para levar adiante os sistemas de energia de zero ou baixo carbono serão um deslocamento necessário de geração de riqueza, por exemplo, para longe das minas de carvão, produtores de SUV e empresas de petróleo; com potenciais

[4] Muitos exemplos são dados no estudo encomendado pela Rede Global de Mulheres pela Transição Energética (Global Women's Network for the Energy Transition, GWNET), intitulado "Mulheres a favor da Energia Sustentável. Incentivando o Talento das Mulheres para uma Mudança Transformadora. Áustria, 2019".

At the **international level**, it will take **a re-ordering of the geopolitical network of** (power and economic) **relations** of momentous magnitude[5]. The energy system of the 20th century was fuelled by oil and gas. It gave exceptional clout **to oil-producing countries** and created dependencies that dwarf ideological alliances.

In recent decades, because of technological advances in prospecting for and development of fossil fuel deposits – including off-shore and in remote areas, such as the Arctic – the number of countries which aspire to draw wealth from their fossil fuel endowments have significantly increased; many of these countries are located in the so-called "**Global South**".

China has also risen as a major player in energy trade and cooperation. China has led the pack in terms of additions to installed capacity fuelled by renewables over the last several years. It has re-committed (most recently, through the speech of Xi Jinping before the UN General Assembly in September 2020[6]) to an ambitious national climate policy which will also help it address air pollution, a major domestic challenge[7]. China dominates the manufacture of most renewables' equipment. Its powerful State Grid Corp of China is a major investor in the energy sector in all continents, especially in Africa. Virtually all of the world's electric busses operate in China[8].

China will continue on this path of decarbonisation[9], high-tech production and digitalisation, mainly to satisfy its own middle class which insistently demands clean air and a healthy environment. By the same token, it will increase its productivity and competitiveness. Through the Belt and Road Initiative[10] which by now reaches two thirds of the world's population, China can be expected to export its approach to its partner countries as well.

The Covid-19 pandemic reduced the demand for oil by a fifth[11] [12] and the oil price collapsed. This foreshadows in a certain way what needs to come in terms of decarbonizing the global energy system. For a good part of 2020 the oil price was at around 40.00 USD a barrel; it has climbed again to about 70.00 USD a barrel. Oil States such as Saudi Arabia need the price to be about 70-80 USD to balance their budgets. Roughly 900 million people live in "petrostates". If the energy transition accelerates – as

---

5 https://www.irena.org/publications/2019/Jan/A-New-World-The-Geopolitics-of-the-Energy-Transformation#:~:text=Chaired%20by%20former%20President%20%C3%93lafur,%2C%20trade%2C%20environment%20and%20development

6 https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1817098.shtml

7 Irene Giner-Reichl, Domestic and International Strategies of the PR of China: Chances for Climate Neutral Development. In Gerd Kaminski (Ed.), Chinese Strategies in Politics, Foreign Policy, Security Policy, Economy and Law. Vienna 2019

8 REN21, Global Status Report 2020, p. 181

9 In September 2020 China announced to become carbon-neutral by 2060 https://news.un.org/en/story/2020/09/1073052

10 Irene Giner-Reichl, One Belt One Road – Chinas Seidenstraßen-Initiative. In Bayer/Giner-Reichl (Ed.) Entwicklungspolitik 2030 – Auf dem Weg zur Nachhaltigkeit. Mainz 2017.

11 The Economist, p. 13, Sept. 19, 2020

12 https://www.iea.org/news/world-energy-outlook-2020-shows-how-the-response-to-the-covid-crisis-can-reshape-the-future-of-energy

impactos graves na situação vigente de emprego e de renda. Em **nível nacional**, os governos precisarão encontrar formas de **diminuir o impacto do deslocamento de geração de riqueza através de medidas adequadas,** como a recapacitação da força de trabalho, a criação de novas oportunidades econômicas e, quando necessário, esquemas de transferência social.

No **nível internacional,** será preciso uma **reorganização das redes de relações geopolíticas** (poder e economia) à altura da grandeza do momento[5]. O sistema energético do século XX foi movido a petróleo e gás. Deu um poder enorme aos países produtores de petróleo e criou dependências que diminuíram alianças ideológicas.

Nas últimas décadas, devido aos avanços tecnológicos em prospecção e ao desenvolvimento de depósitos de combustíveis fósseis, incluindo offshore e áreas remotas como o Ártico, o número de países que desejam obter riquezas de seus recursos de combustíveis fósseis aumentou significativamente; e muitos desses países estão localizados no chamado **"Sul Global".**

A **China** também despontou como um ator importante no comércio e cooperação energética. A China tomou a dianteira em termos do aumento da capacidade instalada baseada em energias renováveis nos últimos anos. E se comprometeu novamente, (mais recentemente no discurso de Xi Jinping diante na Assembleia Geral das Nações Unidas em setembro de 2020[6]) com uma política climática nacional ambiciosa que ajudará a lidar com a poluição do ar, um imenso desafio nacional[7]. A China domina a produção da maioria dos equipamentos de energias renováveis. Sua poderosa Companhia Nacional da Rede Elétrica da China é uma grande investidora no setor energético em todos os continentes, especialmente na África. Praticamente todos os ônibus elétricos do mundo funcionam na China[8].

A China continuará no caminho da descarbonização[9], produção de alta tecnologia e digitalização, principalmente para satisfazer a sua própria classe média que, de forma insistente, exige ar puro e um ambiente saudável. Da mesma maneira, aumentará sua produtividade e competitividade. Através da Iniciativa Cinturão e Rota[10] que atualmente atinge dois terços da população mundial, pode se esperar que a China exporte também sua visão aos seus países parceiros.

---

5 https://www.irena.org/publications/2019/Jan/A-New-World-The-Geopolitics-of-the-Energy-Transformation#:~:text=Chaired%20by%20former%20President%20%C3%93lafur,%2C%20trade%2C%20environment%20and%20development

6 https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1817098.shtml

7 Irene Giner-Reichl, Estratégias Nacionais e Internacionais da RP da China: Oportunidades para o Desenvolvimento Neutro Climático. Em Gerd Kaminski (Ed.), Estratégias chinesas na Política, Política Externa, Política de Segurança, Economia e Legislação. Viena 2019.

8 REN21, Relatório da Situação Global 2020, p. 181.

9 Em setembro de 2020 a China anunciou será neutra em carbono em 2060 https://news.un.org/en/story/2020/09/1073052.

10 Irene Giner-Reichl, One Belt One Road –– Chinas Seidenstraßen-Initiative. Em Bayer/Giner-Reichl (Ed.) Entwicklungspolitik 2030 – Auf dem Weg zur Nachhaltigkeit. Mainz 2017.

it must in order to achieve climate stabilisation – competition among the oil-producing countries will become fiercer, with potentially huge impacts on peace and stability in key regions of the world.

Covid-19 diverted the attention of policymakers away from climate change and its negative impacts. It is to be feared that public resources to help overcome energy poverty in the poorest countries (where reliance on market mechanisms alone is not possible) will also dry up.

Part IV: Conclusions and Recommendations

There will be a strong temptation to slow down the energy transition to accommodate those with vested interests in the current system. Rather than slowing down decarbonisation, governments everywhere need to adopt an **integrated policy approach** to address the multi-dimensional challenges of the energy transition comprehensively, with **social justice** as a key priority.

At the **international level,** through existing and new mechanisms, nations need to work together to **develop new collaborative approaches,** taking into account the new geopolitical realities, to **cushion against harsh side effects of the energy transition** that could result in armed strife, social unrest, and unmanaged migration. This could be summarised by the call for a **New Energy Diplomacy in the 21st Century, as part of comprehensive international security strategies in at least six areas:**

- There is a need for pathways and international cooperation to support petro- and coal states in managing their "carbon withdrawal" discomfort and as they develop more diversified national economies.

- There is a need to assist so-called developing countries to avoid the Global North's mistakes of the past; instead of replicating 20th century's patterns of development, they can and should be assisted to leapfrog to energy systems of the future. This seems all the more important as megacities spring up and grow fast in many developing countries; to avoid that undesirable infrastructure is locked in for decades to come, better alternatives need to be opened up to them now.

- New infrastructure needs to be carbon-neutral; existing infrastructure needs to be retrofitted as much as possible. Most of the infrastructure can be expected to cross national borders [13] which raises many issues, from legal liabilities to protection of the investment to labour rights issues and strategic (in)dependence. Standards and

[13] State Grid Corp of China, China's huge state grid makes major strives to create an integrated grid infrastructure n the context of the Chinese government's Belt and Road initiative; cf. e.g. https://www.beltandroad.news/2020/10/10/state-grid-of-china-to-further-step-up-innovation/; „China already has a number of power lines connected to other countries, including Myanmar, Laos and Vietnam, while lines into Thailand, Pakistan and Bangladesh are under consideration. For emerging economies hampered by chronic electricity shortages, such investments may be a blessing", https://asia.nikkei.com/Spotlight/Asia-Insight/China-s-Belt-and-Road-power-grids-keep-security-critics-awake.

A pandemia da Covid-19 reduziu a demanda de petróleo a um quinto [11] [12] e o preço do petróleo despencou. Isso prenuncia, de certo modo, o que está em jogo em termos de descarbonização do sistema energético global. Durante boa parte de 2020, o preço do petróleo esteve em torno de US$ 40,00 o barril e voltou a subir a US$70,00 o barril. Países produtores de petróleo, como a Arábia Saudita, precisam que o preço esteja entre 70,00 e 80,00 dólares para equilibrar seu orçamento. Aproximadamente 900 milhões de pessoas vivem em "petroestados". Se a transição energética for acelerada, o que deve acontecer para se alcançar a estabilização do clima, a concorrência entre os países produtores será mais feroz, com um imenso potencial de impacto na paz e na estabilidade de importantes regiões do mundo.

A Covid-19 desviou a atenção dos dirigentes das mudanças climáticas e seus impactos negativos. Há temor de que os recursos públicos para ajudar a superar a escassez energética nos países mais pobres (nos quais confiar nos mecanismos d mercado apenas não é possível) também desapareçam.

Parte IV. Conclusões e Recomendações

Haverá uma grande tentação para diminuir o ritmo da transição energética para acomodar os interesses particulares no atual sistema. Em vez de desacelerar a descarbonização, os governos precisam adotar uma **estratégia de política integradas** para lidar com os desafios multidimensionais da transição energética de forma ampla, com **justiça social** como prioridade fundamental.

No **cenário internacional,** os países precisam trabalhar juntos, com novos mecanismos e com os já existentes, para **desenvolver novos métodos de colaboração,** levando em conta as novas realidades geopolíticas, para **atenuar os graves efeitos adversos da transição energética** que poderia resultar em conflito armado, agitação social e migração desordenada. Isto poderia ser resumido com um apelo a uma **Nova Diplomacia Energética no século XXI, como parte de uma ampla estratégia de segurança internacional em pelo menos seis áreas:**

- Há uma necessidade de caminhos e de cooperação internacional para ajudar estados com economias baseadas no petróleo e no carvão para lidar com a dificuldade da "retirada do carbono" enquanto desenvolvem economias nacionais mais diversificadas.

- Há uma necessidade de ajudar os chamados países em desenvolvimento para evitar os erros do passado por parte do "Norte Global"; ao invés de reproduzir os padrões de desenvolvimento do século XX, eles podem e devem ser ajudados a dar o salto para sistemas energéticos do futuro. Tudo isso é ainda mais importante na medida em que megacidades surgem e crescem rapidamente em muitos países em desenvolvimento; para evitar que infraestruturas indesejadas permaneçam por décadas futuras alternativas melhores devem ser oferecidas a eles agora.

[11] The Economist, p. 13, Set. 19, 2020.

[12] https://www.iea.org/news/world-energy-outlook-2020-shows-how-the-response-to-the-covid-crisis-can-reshape-the-future-of-energy

good practices should be developed and implemented. Modalities for multilateral cooperation around infrastructure issues need to be improved or grown from scratch.

- The EU and Latin America should intensify their exchange of experience with regard to sustainable, inclusive and just energy transitions.

- The EU and Latin America should pro-actively engage with China over the issue of energy transitions. China's strong role in sustainable energy is a compelling reason to place energy and climate change diplomacy at the forefront of dealings with China. Brazil's longstanding partnership with China should be leveraged in this respect as well.

- There is a need to conceptualise – in an inclusive and participatory process – the international architecture and tools needed to address the multifaceted dimensions of energy transitions peacefully, cooperatively and effectively.

- A nova infraestrutura precisa ser neutra em carbono; a infraestrutura existente precisa ser readaptada o máximo possível. Pode-se esperar que a maior parte das infraestruturas atravessem fronteiras[13] o que levanta muitas questões, desde responsabilidades legais e proteção do investimento a questões trabalhistas e (in)dependência estratégica. Padrões e boas práticas devem ser desenvolvidos e implementados. Formas de cooperação multilateral relacionadas à infraestrutura devem ser aperfeiçoadas ou criadas.

- A União Europeia e a América Latina devem intensificar o intercâmbio de experiências em relação à transição energética justa, inclusiva e sustentável.

- A União Europeia e a América Latina devem se envolver proativamente com a China acerca das questões da transição energética. O importante papel desempenhado pela China em energia sustentável é uma razão contundente para colocar a diplomacia das mudanças climáticas e da energia no primeiro plano das negociações com a China. A parceria de longa data do Brasil com a China também deve ser impulsionada neste sentido.

- É necessário conceitualizar, em um processo inclusivo e participativo, a arquitetura internacional e os instrumentos necessários para lidar com as dimensões multifacetadas da transição energética de forma pacífica, cooperativa e efetiva.

[13] A Companhia Nacional da Rede Elétrica da China, a imensa rede elétrica da China faz grandes esforços para criar uma infraestrutura de rede integrada no contexto da Iniciativa Cinturão e Rota do governo chinês; cf. e.g. https://www.beltandroad.news/2020/10/10/state-grid-of-china-to-further-step-up-innovation/; "A China já tem uma série de linhas de transmissão de energia conectadas a outros países, incluindo Myanmar, Laos e Vietnã, enquanto linhas de transmissão na Tailândia, Paquistão e Bangladesh estão em análise. Para economias emergentes prejudicadas pela falta crônica de eletricidade, esses investimentos podem ser uma bênção", https://asia.nikkei.com/Spotlight/Asia-Insight/China-s-Belt-and-Road-power-grids-keep-security-critics-awake.

XVIIIFORTE

Conferência de Segurança Internacional
Forte de Copacabana 2021
International Security Conference

ISSN 2176-297X