> ONLINE
Forte de
Copacabana
2020

Conferência de Segurança Internacional

Novas Fronteiras e Soberania frente aos Desafios Globais

POLICY PAPERS

XVIIFORTE

International Security Conference

New Frontiers and Sovereignty in the brink of Global Challenges

POLICY PAPERS

Organisers

KONRAD ADENAUER STIFTUNG

CEBRI
BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS

Supported by

Conferência de Segurança Internacional

Novas Fronteiras e Soberania frente aos Desafios Globais

POLICY PAPERS

XVII FORTE

International Security Conference

New Frontiers and Sovereignty in the brink of Global Challenges

POLICY PAPERS

Rio de Janeiro, 2020

Editor Editor
Anja Czymmeck

Coordenação editorial Project Coordination
Aline Soares
Reinaldo Themoteo

Tradução e revisão Translation and Revision
Leslie Sasson Cohen
Linda Mandel

Projeto Gráfico Design
Daniela Knorr

Fotografias Photos
Capa Cover: Garik Barseghyan/Pixabay.com
Página Page 6: KAS-Brasil
Página Page 8: KAS-Brasil
Página Page 10: CEBRI
Página Page 12 : USA-Reisablogger/Pixabay.com

Impressão Print
Gráfica Cruzado

www.kas.de/brasil

ISSN 2176-297X

Novas Fronteiras e Soberania frente aos Desafios Globais/
New Frontiers and Sovereignty in the brink of Global Challenges (2020)

Rio de Janeiro: Konrad-Adenauer-Stiftung, 2020.

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

XVIIFORTE

INTRODUÇÃO

A Conferência de Segurança Internacional do Forte de Copacabana é o maior fórum de segurança internacional da América Latina. Desde seu início em 2003, o evento foi concebido para a promoção do diálogo entre especialistas do setor governamental, acadêmico e privado da América do Sul e da Europa. Atualmente a Conferência é realizada pela Fundação Konrad Adenauer (KAS) e pelo Centro Brasileiro de Relações Internacionais (CEBRI), com o apoio da Delegação da União Europeia no Brasil.

Realizaremos a 17ª edição da Conferência com o tema "Novas Fronteiras e Soberania frente aos desafios globais". O objetivo é apresentar assuntos no âmbito de segurança internacional que sejam de interesse comum aos dois lados do Atlântico. Neste sentido, trouxemos ao debate as constantes transformações que os conceitos de Soberania e Fronteira vêm sofrendo na ordem multilateral vigente. Primeiramente trataremos das *fronteiras tradicionais*, influenciadas pelo surgimento de novos atores políticos que têm provocado alguns conflitos em diversos lugares do mundo, desafiando os antigos paradigmas e gerando incertezas em aspectos de soberania. Outro tópico essencial será a análise das *fronteiras econômicas*, visto que o assunto da indústria de defesa tem ocupado a pauta nas grandes reuniões entre os países, e os novos acordos propostos movimentam e provocam a estrutura do sistema internacional. Por último, mas não menos importante,

INTRODUCTION

The Forte de Copacabana International Security Conference is the largest international security forum in Latin America. From its outset in 2003, the event was designed to promote dialogue between experts from the government, the academia and the private sector in South America and Europe. The Conference is currently held by the Konrad Adenauer Foundation (KAS) and the Brazilian Center for International Relations (CEBRI), with the support of the Delegation of the European Union to Brazil.

This year, we will hold the Conference's 17th edition with the theme "New Frontiers and Sovereignty in the brink of global challenges". The objective is to discuss issues in the area of international security that are of common interest to both sides of the Atlantic. In this sense, we will debate the continuous transformations of the concepts of Sovereignty and Frontiers in the current multilateral order. Firstly, we will discuss traditional borders, which are being influenced by the emergence of new political actors causing conflicts in different parts of the world, challenging the old paradigms and generating uncertainties in aspects of sovereignty. Another essential topic is the analysis of economic frontiers, since the topic of the defense industry has been on the agenda of major meetings between countries, and the new proposed agreements impact and incite the international system's structure.

XVIIFORTE

abordaremos o contexto alavancado pela pandemia, que impregnou as pautas estatais e evidenciou a necessidade dos fluxos informacionais e, por conseguinte, o aprofundamento no debate sobre os riscos de ciberataques: assunto prioritário na área de *fronteiras digitais*.

Excepcionalmente em 2020, a conferência será realizada em formato virtual, para proteger todos os envolvidos: organização, convidados e audiência. Gostaríamos de tornar este momento uma oportunidade de fazer chegar esta discussão sobre segurança internacional a inúmeras regiões do globo. Assim como a Conferência, esta coleção de Policy Papers, além de ser bilíngue, traz em reflexão seus temas centrais, como os diversos mecanismos internacionais e o papel dos vários tipos de fronteiras, e pretende identificar desafios, bem como fazer recomendações políticas para o futuro.

Esperamos que a leitura seja bastante proveitosa!

Muito obrigada!

Anja Czymmeck
Diretora da Fundação
Konrad Adenauer no Brasil

Last but not least, we will address the context leveraged by the pandemic, which permeated State agendas and highlighted the need for information flows and, therefore, the deepening of the debate on the risks of cyber attacks: a priority issue in the area of digital frontiers.

In 2020, exceptionally, the conference will be held in a virtual platform in order to protect everyone involved: organizers, guests and audience. We would like to make this an opportunity to bring this discussion about international security to many regions of the globe. Like the Conference, this collection of Policy Papers is bilingual and examines central topics such as the various international mechanisms, the different types of frontiers and their roles, and also aims to identify challenges, as well as make policy recommendations for the future.

We hope you find the content useful and enjoy reading it.

Thank you!

Anja Czymmeck
Director of the Konrad
Adenauer Foundation in Brazil

“A Democracia é mais do que uma forma de governo participativo.
É uma visão de mundo, enraizada na concepção da
dignidade, do valor e dos direitos inalienáveis da cada pessoa.”

*“Democracy is more than a form of participative government.
It is a worldview, rooted in the conception of
dignity, value and inalienable rights of each person.”*

KONRAD ADENAUER, 1965

www.kas.de/brasil KAS.Brasil KASBrasil KASBrasil

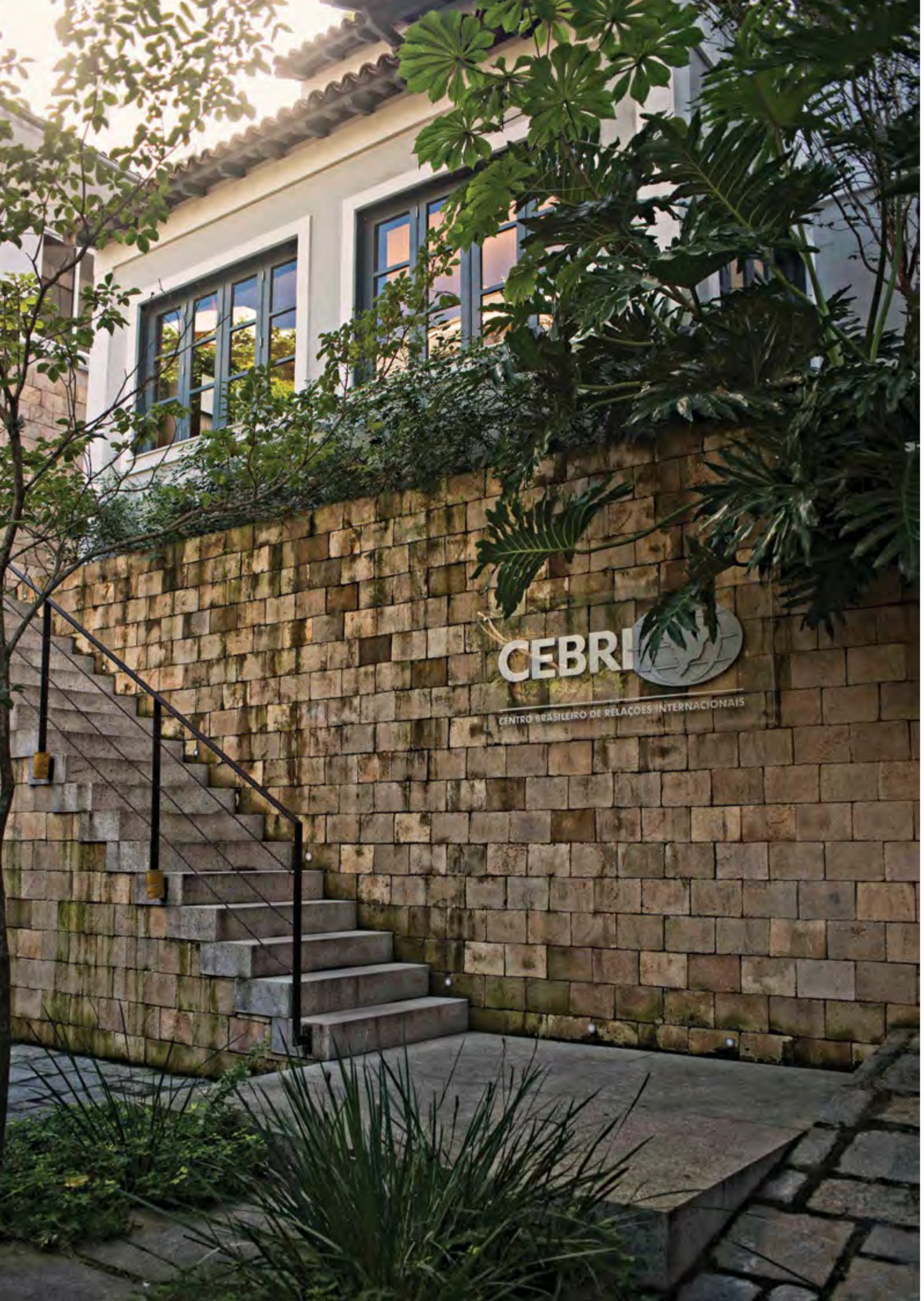
KONRAD
ADENAUER
STIFTUNG

A Fundação Konrad Adenauer (KAS) é uma fundação política alemã. Através do nosso escritório central na Alemanha e dos mais de 90 escritórios espalhados pelo mundo, gerenciamos mais de 200 projetos abrangendo mais de 120 países. Tanto na Alemanha quanto no exterior, nossos programas de educação cívica têm como objetivo promover os valores de liberdade, paz e justiça, bem como diálogo e cooperação. Como think tank e agência de consultoria, nós focamos na consolidação da democracia, na unificação da Europa, no fortalecimento das relações transatlânticas, assim como na cooperação internacional e no diálogo. Os nossos projetos, debates e análises visam o desenvolvimento de uma forte base democrática para ação política e cooperação.

No Brasil, nossas atividades concentram-se no diálogo de segurança internacional, educação política, estado de direito, funcionamento de instituições públicas e seus agentes, economia social de mercado, política ambiental e energética assim como as relações entre o Brasil, a União Europeia e a Alemanha.

The Konrad Adenauer Stiftung (KAS) is a German political foundation. From our headquarters in Germany and 90 field offices around the globe, we manage over 200 projects covering over 120 countries. At home as well as abroad, our civic education programmes aim at promoting the values of freedom and liberty, peace and justice, as well as dialogue and cooperation. As a think tank and consulting agency we focus on the consolidation of democracy, the unification of Europe, the strengthening of transatlantic relations, as well as on international cooperation and dialogue. Our projects, debates and analyses aim to develop a strong democratic base for political action and cooperation.

In Brazil our activities concentrate on international security dialogue, political education, the rule of law, the workings of public institutions and their agents, social market economy, environmental and energy policy, as well as the relations between Brazil, the European Union and Germany.



CEBRI
BRAZILIAN CENTER FOR
INTERNATIONAL RELATIONS

O Centro Brasileiro de Relações Internacionais (CEBRI) é um think tank independente, que contribui para a construção da agenda internacional do Brasil. Há mais de vinte anos, a instituição se dedica à promoção do debate plural e propositivo sobre o cenário internacional e a política externa brasileira. Em 2019 foi eleito como o segundo think tank mais relevante da América do Sul e Central pelo Global Go To Think Tank Index Report, da Universidade da Pensilvânia, além de ter figurado em posições de liderança em outras oito categorias na região.

O CEBRI prioriza em seus trabalhos temáticas de maior potencial para alavancar a inserção internacional do país à economia global, propondo soluções pragmáticas na formulação de políticas públicas.

É uma instituição sem fins lucrativos, com sede no Rio de Janeiro e reconhecida internacionalmente. Hoje, reúne cerca de 100 associados, que representam múltiplos interesses e segmentos econômicos e mobiliza uma rede de profissionais e organizações no mundo todo. Além disso, conta com um Conselho Curador atuante e formado por figuras proeminentes na sociedade brasileira.

The Brazilian Center for International Relations (CEBRI) is an independent think tank committed to contributing to the development of Brazil's international agenda. For over twenty years, the organization has been dedicated to promoting a plural and purposeful debate on the international scene and Brazilian foreign policy. In 2019 CEBRI was elected second most relevant think tank in South and Central America by the Global Go To Think Tank Index Report, compiled by the University of Pennsylvania, who also named it for top positions in other eight categories in the region.

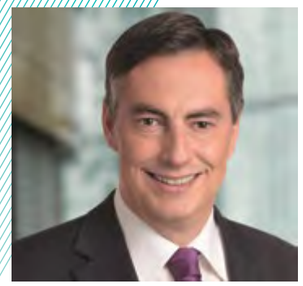
In its work, CEBRI prioritizes topics with the greatest potential to leverage the country's international insertion in the global economy, proposing pragmatic solutions for the formulation of public policies.

CEBRI is an internationally recognized non-profit organization based in Rio de Janeiro. With nearly 100 members representing multiple interests and economic segments, it engages a network of professionals and organizations worldwide. In addition, it has an active Curator Council formed by prominent figures in Brazilian society.

União Europeia

A Delegação da União Europeia (UE) no Brasil é uma das mais de 140 representações que a UE tem no mundo. Estamos focados na promoção das relações políticas, econômicas e de cooperação entre a UE e o Brasil, no âmbito da nossa Parceria Estratégica instituída em 2007. A UE e o Brasil estabeleceram relações diplomáticas em 1960, criando estreitos laços históricos, culturais, econômicos, de cooperação e políticos. Dentre os tópicos centrais dessa parceria estratégica, com mais de 30 diálogos formais e 100 projetos em curso, estão questões econômicas, a cooperação em questões-chaves de política externa e o enfrentamento conjunto de desafios globais em áreas como direitos humanos, mudanças climáticas e a luta contra a pobreza. Com a pandemia da COVID-19, estamos ainda mais empenhados a aprimorar nossa cooperação em busca de soluções que nos levem a uma reconstrução e uma recuperação ainda mais verde e mais resiliente das nossas sociedades. A União Europeia e o Brasil são parceiros comerciais importantes e os países da União Europeia recebem mais de 16% da exportação brasileira. A União Europeia também é o maior investidor estrangeiro no Brasil.

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. The EU and Brazil established diplomatic relations already 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 addressing global challenges in areas such as human rights, climate change as well as the fight against poverty. With the COVID-19 pandemic, we 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 European Union and Brazil are also important trading partners and the countries of the European Union account for over 16% of Brazil's ex¬ports. The European Union is also the largest foreign investor in Brazil.



David McAllister

David McAllister foi eleito membro do Parlamento Estadual de Niedersachsen (Baixa Saxônia) em 1998. De 2003 a 2010, ele foi Presidente do Grupo da União Democrática Cristã (CDU) e de 2010 a 2013 foi Primeiro Ministro de Niedersachsen. Desde 2014 é membro do Parlamento Europeu e Vice-Presidente do Partido Popular Europeu (PPE). Ele preside a Comissão de Assuntos Externos do Parlamento Europeu e também o Grupo de Coordenação para o Reino Unido.

David McAllister was elected as a member of the State Parliament of Niedersachsen (Lower Saxony) in 1998. From 2003 till 2010 he served as Chairman of the Christian Democratic Union (CDU) Group and from 2010 until 2013 as Prime Minister of Niedersachsen. Since 2014 he is a Member of the European Parliament and is a Vice President of the European People's Party (EPP). He chairs the Committee on Foreign Affairs in the European Parliament and also the UK Coordination Group.

O papel da UE na Ordem de Segurança Global: Qual é o papel e quais são os objetivos da UE em um Mundo de Segurança Global e Multipolar em evolução?

The Role of the EU in the Global Security Order: What are the EU's role and objectives in an evolving Global Security Order and Multipolar World?

David McAllister

Membro do Parlamento Europeu | Presidente da Comissão de Assuntos Externos do Parlamento Europeu

Member of the European Parliament | Chairman of the Committee on Foreign Affairs of the European Parliament

Introdução

A pandemia da COVID-19, tanto quanto as crises globais anteriores, como a crise financeira de 2008, são a prova de que o nível e a complexidade dos desafios globais de hoje exigem, mais do que nunca, uma abordagem concertada por parte da comunidade internacional. Isso não é apenas uma questão de escala, mas baseia-se no fato de que a maioria dos principais desafios enfrentados atualmente tanto pelos países individuais como pela comunidade internacional, têm não apenas uma dimensão transnacional, mas também transregional, com questões que muitas vezes atravessam as linhas tradicionais de política interna e externa. Além disso, deve-se observar que, já há alguns anos, estamos realizando uma transição para um sistema multipolar, onde respostas políticas eficazes só podem ser construídas sobre a base da parceria não apenas entre os atores estatais, mas também entre as regiões, e sobre um sistema de governança global

Introduction

The COVID-19 pandemic - as much as previous global crises, such as the 2008 financial crisis - are proof that the level and complexity of today's global challenges require, more than ever, a concerted approach by the international community. This is not just a matter of scale, but it is based on the fact that most of the key challenges confronting individual countries and the international community alike, nowadays, have not only a transnational, but also a trans-regional dimension, with issues often cutting across traditional internal and external policy lines. Furthermore, it should be noted that, for quite a number of years already, we have been transitioning towards a multipolar system where effective policy responses can only be built on partnership not only between state actors, but also between regions, and on an inclusive global

governance system, which can deliver on the objective of valuable and viable policy visions and the capacity to adopt fast, concerted responses.

With this in mind, this issues paper seeks to contribute to the XVII Forte de Copacabana International Security Conference with an overview of the European Union's foreign policy and security strategy in a changing multipolar world, and a discussion of avenues of further cooperation between the EU and Latin American countries both in a bilateral southern-atlanticist setting and in defence of multilateral fora and their capacity to promote consensus and policy responses amongst the international community.

A strong and coordinated EU response to current and emerging threats

The COVID-19 pandemic has shaken not only Europe, but also the entire global community to its core. This crisis is unprecedented in its scope and damages to our societies. The virus knows no borders and everyone is at risk. To mobilise resources and fight it at home is not enough. This fight requires a massive and coordinated global response to save lives, protect the health of our citizens and mitigate socio-economic consequences. The COVID-19 crisis showed us once again that we are only as strong as our ability to act in a united fashion.

The strength of the European response is in upholding our core values, founded on partnership, solidarity, rules-based multilateral solutions and coordination. Failing to defend these principles costs lives, undermines security and mutual trust and brings severe economic damages. We experienced it first hand in the EU during the initial phase of the COVID-19 outbreak. If countries start to work in discord and isolation, they will only weaken their capacity of response and become even more vulnerable. For these reasons the EU has taken a leadership role in the coordination efforts undertaken by the United Nations, the G20, the G7, the WHO and the international financial institutions.

In external policies, the EU responded to the COVID-19 crisis as 'Team Europe' drawing contributions and resources from all EU institutions, EU Member States and financial institutions, and redirecting almost EUR 36 Billion to address the consequences of COVID-19 in partner countries and regions. Furthermore, in its global reaction to COVID-19, the EU stood in the centre of the "Coronavirus Global Response Initiative". With strong support by the European Commission - under the initiative and leadership of Commission President Ursula von der Leyen and her vision for a global vaccine response - this global pledge aims to fund development of affordable vaccination, treatment and testing for COVID-19. A vaccine that would be a universal, common good. With our global partners, we secured almost EUR 10 billion (June 2020) to close the gap in funding for COVID-19 global treatment.

As European Parliament, we have also warned that EU institutions must step up efforts to counter the increasing malign disinformation known as "infodemic" and, in particular, must counter aggressive Russian and Chinese propaganda activities, which have

inclusivo, que possa cumprir com o objetivo de fornecer visões políticas valiosas e viáveis, assim como a capacidade de adotar respostas rápidas e concertadas.

Com isso em mente, este artigo temático tem como objetivo contribuir para a XVII Conferência Internacional de Segurança do Forte de Copacabana com uma visão geral da política externa e estratégia de segurança da União Europeia em um mundo multipolar em transformação, assim como com uma discussão sobre caminhos de maior cooperação entre a UE e os países latino-americanos, tanto em um cenário bilateral sul-atlanticista quanto em defesa dos foros multilaterais e sua capacidade de promover consenso e respostas políticas no âmbito da comunidade internacional.

Uma resposta forte e coordenada da UE às ameaças atuais e emergentes

A pandemia da COVID-19 abalou não apenas a Europa, mas também toda a comunidade global em seu âmago. Essa crise é sem precedentes em seu alcance e prejuízos a nossas sociedades. O vírus não conhece fronteiras e todos estão sob ameaça. Mobilizar recursos e combatê-lo em casa não é suficiente. Esta luta requer uma resposta global maciça e coordenada para salvar vidas, proteger a saúde de nossos cidadãos e mitigar as consequências socioeconômicas. A crise da COVID-19 nos mostrou, uma vez mais, que somos apenas tão fortes quanto a nossa capacidade de agir de forma unida.

A força da resposta europeia está na defesa de nossos valores essenciais, fundamentados em parceria, solidariedade, soluções multilaterais baseadas em regras e coordenação. Não defender esses princípios custa vidas, afeta a segurança e a confiança mútua e traz graves prejuízos econômicos. Nós vivenciamos isso em primeira mão na UE durante a fase inicial do surto da COVID-19. Se os países começarem a trabalhar em desacordo e isoladamente, eles só enfraquecerão sua capacidade de resposta e se tornarão ainda mais vulneráveis. Por essas razões, a UE assumiu um papel de liderança nos esforços de coordenação empreendidos pelas Nações Unidas, o G20, o G7, a OMS e as instituições financeiras internacionais.

No campo das políticas externas, a UE respondeu à crise da COVID-19 como "Equipe Europa", captando contribuições e recursos de todas as instituições da UE, Estados-membros da UE e instituições financeiras, e redirecionando quase 36 bilhões de euros para enfrentar as consequências da COVID-19 nos países e regiões parceiros. Além disso, em sua reação global à COVID-19, a UE esteve no centro da "Iniciativa de Resposta Global ao Coronavírus". Com forte apoio da Comissão Europeia, sob a iniciativa e liderança da Presidente da Comissão, Ursula von der Leyen, e sua visão de uma resposta global para a vacina, esse compromisso global visa a financiar o desenvolvimento de vacinação, tratamento e testes acessíveis para a COVID-19. Uma vacina que seria um bem comum e universal. Com nossos parceiros globais, conseguimos quase 10 bilhões de euros (junho de 2020) para fechar a lacuna no financiamento para o tratamento da COVID-19 em nível mundial.

Como Parlamento Europeu, também alertamos que as instituições da UE devem intensificar seus esforços para combater a crescente onda maligna de desinformação conhecida

been exploiting the COVID-19 pandemic. The updated and upgraded EU response to these threats outlined in June 2020 is indeed strong and multi-faceted and, on this, like on other issues, international cooperation is crucial.

The need for a strong and efficient EU foreign and security policy

The COVID-19 crisis has undoubtedly made clearer than ever before the need for a more assertive EU on the international stage, defending its interests in a spirit of sovereignty and promoting multilateral solutions.

Further close cooperation with NATO and the US remains of utmost importance. Yet, the EU also needs to take greater responsibility for its own security and defence, act more autonomously in this area, and work towards a genuine strategic autonomy. This is all the more crucial at a time when the US, which remains an important partner and ally for the EU and its Member States appears as increasingly sceptical about the value and strengths of the multilateral, rules-based world order and is at times withdrawing from it. In pursuing its own capacity of security and defence, the EU is also following up on its realisation of the limitations of excessive dependence on third countries in many areas.

The European Parliament is a strong promoter of a more responsive and more efficient Common Foreign and Security Policy (CFSP) and the Common Security and Defence Policy (CSDP) and has proposed several additional avenues in this respect.

First of all, these policies should be better linked to the other strands of EU external action. This was the key idea underlying the 2016 EU Global Strategy - the overarching strategy for EU action on the international scene - but many major EU-internal and international developments, including the pandemic, have happened since then. This should call for a revision of this strategy, as the European Parliament stressed in its April 2020 resolution.

Secondly, the European Union should use the full range of its assets in the foreign and security policy, and this includes a parliamentary dimension. For many decades, parliamentary diplomacy has been perceived as a secondary channel for international contacts, with a limited impact. The European Parliament, however, has emerged more and more as a decisive actor of EU foreign policy, with its own channels and strands of action, which are complementary to those of the EU's executive. Parliament's soft power, through resolutions, political dialogue, conflict prevention, mediation and democracy support actions, is helping to assert the presence and credibility of the EU on the international stage.

Thirdly, the EU must become more efficient in its decision-making and should take full advantage of the possibilities offered by the EU treaties, institutions and their procedures and be creative in establishing new formats. Moving towards a common foreign and security policy of sovereign states is an unprecedented step and therefore, unsurprisingly a rather rocky path. We have made a number of proposals in recent

como "infodemia" e, em particular, fazer face às atividades agressivas de propaganda russa e chinesa, que têm se aproveitado da pandemia da COVID-19. A resposta atualizada e aprimorada da UE a estas ameaças, definida em junho de 2020, é de fato forte e multifacetada e, em relação a isso, como em outras questões, a cooperação internacional é fundamental.

A necessidade de uma política externa e de segurança da UE forte e eficiente

A crise da COVID-19 deixou, sem dúvida, mais claro do que nunca a necessidade de uma UE mais assertiva no cenário internacional, defendendo seus interesses em um espírito de soberania e promovendo soluções multilaterais.

Dar prosseguimento à estreita cooperação com a OTAN e os EUA continua sendo da maior importância. Contudo, a UE também precisa assumir maior responsabilidade por sua própria segurança e defesa, agir de forma mais autônoma nesta área e trabalhar em prol de uma verdadeira autonomia estratégica. Isso é ainda mais crucial em uma época em que os EUA, que permanecem sendo um parceiro e aliado importante para a UE e seus Estados-Membros, mostram-se cada vez mais céticos quanto ao valor e as fortalezas da ordem mundial multilateral, que se baseia em regras, e vez por outra se retraem dela. Na busca de suas próprias capacidades de segurança e defesa, a UE está também agindo diante da percepção das limitações trazidas pela excessiva dependência de terceiros países em muitas áreas.

O Parlamento Europeu é um forte promotor de uma Política Externa e de Segurança Comum (PESC) mais ágil e mais eficiente, assim como da Política Comum de Segurança e Defesa (CSDP), tendo proposto diversos caminhos adicionais a esse respeito.

Em primeiro lugar, essas políticas deveriam estar mais bem entrosadas com as outras linhas de ação externa da UE. Essa foi a ideia-chave subjacente à Estratégia Global da UE de 2016 - a estratégia global para a ação da UE no cenário internacional - mas muitos importantes acontecimentos dentro da EU e também em nível internacional ocorreram desde então, incluindo a pandemia. Isso deverá exigir uma revisão dessa estratégia, como o Parlamento Europeu enfatizou em sua resolução de abril de 2020.

Em segundo lugar, a União Europeia deverá utilizar toda a gama de seus ativos na política externa e de segurança, e isso inclui uma dimensão parlamentar. Por muitas décadas, a diplomacia parlamentar tem sido percebida como um canal secundário para contatos internacionais, com um impacto limitado. O Parlamento Europeu, entretanto, tem surgido cada vez mais como um ator decisivo da política externa da UE, com seus próprios canais e linhas de ação, que são complementares aos das instâncias executivas da UE. O soft power do Parlamento, através de resoluções, diálogo político, prevenção de conflitos, mediação e ações de apoio à democracia, está ajudando a firmar a presença e a credibilidade da UE no cenário internacional.

Em terceiro lugar, a UE precisa tornar-se mais eficiente quanto à tomada de decisões, devendo aproveitar ao máximo as possibilidades oferecidas pelos tratados, instituições e seus procedimentos, além de ser criativa no estabelecimento de novos formatos. Avançar em direção a uma política externa e de segurança comum de Estados soberanos é um

resolutions to overcome at least some of the difficulties and have the right instruments and decision-making processes to assume a leadership role at global level.

Finally, the progress made in recent months and years towards higher autonomy and integration in the field of security and defence forms a good basis to build upon. Projects, such as the permanent structured cooperation (PESCO) and the military mobility or the European Defence Fund (EDF) all contribute to the enhancement of defence investment, capability development and operational readiness. The guideline of the President of the Commission, Ursula von der Leyen, to build, within five years, a genuine and operational European defence union, is an ambitious goal, which deserves our entire support.

Multilateralism as a predicament for the EU's foreign policy – implications for stronger ties between the EU and Latin America and closer dialogue and cooperation between the EU and Latin America in multilateral fora.

In a multipolar world, responding successfully to global crises, threats and challenges requires an efficient multilateral system founded on universal values and rules and built on a strong commitment by its members to its capacity of delivery. This is where the potential of closer cooperation between the European Union and its Member States, on the one hand, and the countries of Latin America, on the other, shows its great value.

The relationship between the EU and Latin America is often framed only in terms of closer economic links. These are obviously very important and for the benefit of both parties and we can only hope that we will continue along the path of closer trade and investment links and economic cooperation. Trade, Investment and Association Agreements have been concluded between the EU and 27 out of the 33 Latin American and Caribbean countries. We also keep strengthening our ties: this year the EU and Mexico concluded negotiations on the modernisation of the EU-Mexico Global Agreement; last year MERCOSUR and the EU reached a deal for an Association Agreement and the EU and Chile are modernizing the trade pillar of the 2003 Association Agreement. Yet, the EU and Latin American countries have so many other strategic and geopolitical interests in common. They also have an important regional neighbour, Africa, with strong ties to and tremendous potential for closer cooperation with both the EU and Latin America. The EU and Latin America can be very synergic like-minded partners in International Fora and international organisations, like the G-20 and, in particular, the UN.

If we look at our bilateral dimension, closer cooperation on security matters should be high on our common agenda. From a security and stability perspective, NATO has already expanded its capacity of security dialogue to the African continent with its Mediterranean dialogue (Morocco and Mauritania). Dialogue and cooperation on security and defence could now be expanded to Latin America, so that we can address together the increasing nexus between drug smuggling and terrorist financing, but also

passo sem precedentes e, portanto, e isso não é surpreendente, um caminho bastante cheio de obstáculos. Temos feito uma série de propostas em resoluções recentes para superar ao menos algumas das dificuldades e termos os instrumentos e processos decisórios certos para assumir um papel de liderança em nível global.

Finalmente, o progresso realizado nos últimos meses e anos em direção a uma maior autonomia e integração no campo da segurança e da defesa constitui uma boa base sobre a qual construir. Projetos como a Cooperação Estruturada Permanente (CEP) e a mobilidade militar ou o Fundo Europeu de Defesa (FED) contribuem, todos eles, para o aumento do investimento em defesa, desenvolvimento de capacidades e prontidão operacional. A diretriz da Presidente da Comissão, Ursula von der Leyen, de construir, no prazo de cinco anos, uma verdadeira união europeia de defesa em condições operacionais, é um objetivo ambicioso, que merece todo o nosso apoio.

O multilateralismo como dilema para a política externa da UE - implicações para o fortalecimento dos laços entre a UE e a América Latina e o estreitamento do diálogo e da cooperação entre a UE e a América Latina em foros multilaterais.

Em um mundo multipolar, responder com sucesso a crises, ameaças e desafios globais requer um sistema multilateral eficiente baseado em valores e regras universais e construído sobre o fundamento de um forte compromisso de seus membros com sua capacidade de cumpri-los. É aqui que o potencial de cooperação mais estreita entre a União Europeia e seus Estados-Membros, por um lado, e os países da América Latina, por outro, mostra seu grande valor.

A relação entre a UE e a América Latina é frequentemente definida apenas em termos de laços econômicos mais estreitos. Eles são obviamente muito importantes e em benefício de ambas as partes, e só podemos esperar continuar no caminho do estreitamento dos laços comerciais e de investimento, assim como da cooperação econômica. Foram concluídos acordos comerciais, de investimento e de associação entre a UE e 27 dos 33 países da América Latina e do Caribe. Continuamos, também, reforçando nossos vínculos: no corrente ano, a UE e o México concluíram as negociações para a modernização do Acordo Global UE-México; no ano passado, o MERCOSUL e a UE chegaram a um Acordo de Associação e a UE e o Chile estão modernizando o capítulo comercial do Acordo de Associação de 2003. Todavia, a UE e os países da América Latina têm tantos outros interesses estratégicos e geopolíticos em comum. Eles também têm um vizinho regional importante, a África, com fortes laços e um tremendo potencial para uma cooperação mais estreita tanto com a UE quanto com a América Latina. A UE e a América Latina podem ser parceiros muito sinérgicos e com posições comuns em Foros Internacionais e organizações internacionais, como o G-20 e, particularmente, as Nações Unidas.

Se olharmos para nossa dimensão bilateral, uma cooperação mais estreita em questões de segurança deveria ocupar um lugar de destaque na nossa agenda comum. De uma perspectiva de segurança e estabilidade, a OTAN já expandiu sua capacidade do diálogo de segurança para o continente africano através do seu Diálogo do Mediterrâneo (Marrocos

security in the Southern Atlantic, with particular regard to the Gulf of Guinea, where 82% of maritime kidnappings in the world now occur according to the International Maritime Bureau. Energy security and energy cooperation is another area where the EU, relevant Latin American countries and African countries can cooperate, thus ensuring a secure and environmentally safe common energy space. The EU and Latin America should also cooperate together with relevant African partners, including the African Union, in order to promote political and economic stability and security on the African continent. This cooperation should include continued support for peacekeeping operations, but also closer dialogue with key emerging actors on the African continent like Ethiopia, Nigeria or South Africa. In the future, a shared vision with relevant countries from the Southern Hemisphere will be essential for the environmental preservation of Antarctica. All these avenues of cooperation are about creating a common space between the EU and Latin America built on shared values, policy objectives and cooperation. They are also about pursuing a capacity of partnership together with African countries for a better future for Africa and closer political and economic links with its European and Latin American neighbours. Relevant commentators have pointed to the value of Southern Atlanticism or Wider Atlanticism and indeed this common space between the EU and Latin American countries would prove synergic with the already very strong partnership between the EU and the US and Canada, and with the longstanding relationship of many Latin American countries with both countries.

This capacity of closer dialogue and cooperation between the EU and Latin American countries is something Parliamentarians from both sides have been advocating for a long time:

Already in 2009 the Euro-Latin American Parliamentary Assembly (EuroLat) called for a Euro-Latin American Charter for Peace and Security, on the basis of the UN Charter, with joint political and security strategies to tackle the common threats. The European Parliament stressed in its 2017 resolution on EU political relations with Latin America[1] that the new geopolitical scenario reinforces the LAC region as a strategic priority and opportunity for the EU's foreign policy. The European Parliament specifically called for continued efforts to strengthen defence and security cooperation through police and military coordination, the fight against drug trafficking and organised crime and information sharing. Latin American participation in EU crisis management and peacekeeping missions, cooperation in maritime security, disarmament, non-proliferation and arms control should also be pursued. The 2019 EU-LAC strategy[2] provides an ambitious framework for a stronger partnership between the EU and Latin American countries. However, it is now time to deliver on the four priorities that have been identified in the strategy: prosperity, democracy, resilience and effective global governance.

The EU and Latin American countries can and should become synergic partners also in international fora with a view to reinforcing multilateralism as the primary avenue for

1 https://www.europarl.europa.eu/doceo/document/TA-8-2017-0345_EN.pdf

2 Joint Communication to the European Parliament and the Council European Union, Latin America and the Caribbean: joining forces for a common future

e Mauritânia). O diálogo e a cooperação em matéria de segurança e defesa podem agora ser expandidos para a América Latina, para que possamos abordar juntos a crescente ligação entre o contrabando de drogas e o financiamento do terrorismo, mas também a segurança no Atlântico Sul, com particular atenção para o Golfo da Guiné, onde ocorrem atualmente 82% dos sequestros marítimos no mundo, de acordo com o *International Maritime Bureau* (Bureau Marítimo Internacional). Segurança energética e cooperação energética é outra área onde a UE, países relevantes da América Latina e países africanos podem cooperar, assegurando assim um espaço energético comum seguro e ambientalmente sustentável. A UE e a América Latina deverão cooperar, igualmente, com parceiros africanos relevantes, incluindo a União Africana, a fim de promover a estabilidade política e econômica e a segurança no continente africano. Esta cooperação deverá incluir o apoio contínuo às operações de manutenção de paz, mas também um diálogo mais estreito com os principais atores emergentes no continente africano, como a Etiópia, Nigéria ou África do Sul. No futuro, uma visão compartilhada com países relevantes do Hemisfério Sul será essencial para a preservação ambiental da Antártida. Todos esses caminhos de cooperação estão relacionados à criação de um espaço comum entre a UE e a América Latina, construído sobre valores compartilhados, objetivos políticos e cooperação. Trata-se também de buscar evoluir na capacidade de parceria junto aos países africanos com vistas a um futuro melhor para a África e laços políticos e econômicos mais estreitos com seus vizinhos europeus e latino-americanos. Comentadores importantes têm apontado para o valor do Atlantismo Meridional ou Atlantismo Expandido e, de fato, este espaço comum entre a UE e os países latino-americanos sinérgico com a parceria já muito forte entre a UE e os EUA e Canadá, e com a relação de longa data de muitos países latino-americanos com ambos esses países.

Essa capacidade de diálogo e cooperação mais estreita entre a UE e os países da América Latina é algo que os parlamentares de ambos os lados vêm defendendo há muito tempo: Já em 2009, a Assembleia Parlamentar Euro-Latino-Americana (EuroLat) reivindicou uma Carta Euro-Latino-Americana para a Paz e Segurança, com base na Carta das Nações Unidas, com estratégias políticas e de segurança conjuntas para enfrentar as ameaças comuns. O Parlamento Europeu enfatizou em sua resolução de 2017 sobre as relações políticas da UE com a América Latina[1] que o novo cenário geopolítico reforça a região ALC como uma prioridade estratégica e uma oportunidade para a política externa da UE. O Parlamento Europeu fez um chamamento específico para esforços contínuos no sentido de fortalecer a cooperação nas áreas de defesa e segurança através da coordenação policial e militar, a luta contra o tráfico de drogas e o crime organizado, assim como o compartilhamento de informações. A participação latino-americana na gestão de crises e missões de manutenção de paz da UE, cooperação em segurança marítima, desarmamento, não-proliferação e controle de armas também devem ser objetivos a ser perseguidos. A estratégia UE-ALC de 2019[2] fornece um marco ambicioso para uma parceria mais forte entre a UE e os países da América Latina. Entretanto, é chegada a hora de dar passos concretos em relação às quatro prioridades identificadas na estratégia: prosperidade, democracia, resiliência e governança global eficaz.

1 https://www.europarl.europa.eu/doceo/document/TA-8-2017-0345_EN.pdf

2 Joint Communication to the European Parliament and the Council European Union, Latin America and the Caribbean: joining forces for a common future

consensus building in a multipolar world and encouraging other international partners to converge with their policy stances and fulfill their international commitments. The leadership of Ambassador Roberto Azevêdo as Director General of the World Trade Organization and of Dr. Michelle Bachelet as United Nations High Commissioner for Human Rights and the support by the EU for them and for the mandate of the institutions they represent attest to our shared commitment to multilateralism and to the great potential of cooperation between the EU and Latin American countries in international fora and international organisations. In particular, the EU and Latin American countries should pursue dialogue on how to support a stronger United Nations and one that can continue to promote peace and security, democracy and an inclusive system of global governance and offer global solutions to global crises. The EU and Latin American countries should support the process of reforms by the UN Secretary General and should work together and with the US on a more effective system of peacekeeping and one, which can deliver longer-term security and stability. The consensus building process on climate change mitigation measures globally is also a policy area where the EU and Latin American countries could give a very relevant contribution and promote a wider consensus across the international community. We may not always see eye to eye on how to pursue climate action, but our societies, which share so many values and so many aspirations, particularly on how to follow up on concerns for climate change, have given us a strong mandate for climate action and this is a policy area where Latin America could not only provide, in so many ways, a decisive contribution in CO_2 reduction, but could equally play a prominent role in global leadership on effective ways to manage and curb climate change.

Conclusions

The European Union was shaped by different crises and came out of them stronger and more resilient. COVID-19 has showed us that only by coordinated action in Europe and globally can we stand the chance to fight such crises and its consequences. The EU is heeding this call and internally re-enforcing its strategic objectives, fostering the European Green Deal and the Digital Agenda through its policies. At the same time, it is important to integrate the environment and climate objectives to the support provided to our external partners. Whilst the current crisis reminded us of the fragility of the global system, it also gives us all a unique opportunity to be better equipped for our future. This is a challenge we need to tackle jointly with like-minded partners and, ultimately, it is about finding common ground and agreeing on the broader notion in our contemporary world of security threats and security cooperation and how to pursue effective policy responses together. ■

Os países da UE e da América Latina podem e devem se tornar parceiros sinérgicos também em foros internacionais com vistas a reforçar o multilateralismo como principal via para a construção de consensos em um mundo multipolar, além de incentivar outros parceiros internacionais a convergir em termos de suas posições políticas e cumprir seus compromissos internacionais. A liderança do Embaixador Roberto Azevêdo como Diretor Geral da Organização Mundial do Comércio e da Dra. Michelle Bachelet como Alta Comissária das Nações Unidas para os Direitos Humanos e o apoio da UE a eles e ao mandato das instituições que representam, atestam nosso compromisso compartilhado com o multilateralismo e com o grande potencial de cooperação entre a UE e os países latino-americanos em foros internacionais e organizações internacionais. Em particular, a UE e os países da América Latina devem buscar o diálogo sobre como apoiar uma ONU mais forte e que possa continuar a promover a paz e a segurança, a democracia e um sistema inclusivo de governança global, assim como oferecer soluções globais para crises globais. A UE e os países da América Latina devem apoiar o processo de reformas do Secretário Geral da ONU e devem trabalhar juntos e com os EUA com vistas a um sistema mais efetivo de manutenção da paz, um sistema que possa proporcionar segurança e estabilidade a longo prazo. O processo de construção de consenso quanto a medidas de mitigação da mudança climática no mundo é, igualmente, uma área de política onde a UE e os países da América Latina poderiam dar uma contribuição muito relevante e promover um consenso mais amplo em toda a comunidade internacional.

Talvez nem sempre possamos ter uma visão clara sobre como buscar a ação climática, mas nossas sociedades, que compartilham tantos valores e tantas aspirações, particularmente sobre como dar seguimento às preocupações com a mudança climática, nos deram um forte mandato para a ação climática e essa é uma área de política onde a América Latina poderia, de tantas maneiras, não somente dar uma contribuição decisiva na redução de CO_2, como igualmente desempenhar um papel proeminente na liderança global sobre formas eficazes de administrar e conter a mudança climática.

Conclusões

A União Europeia foi moldada por diferentes crises e saiu delas mais forte e resiliente. A COVID-19 nos mostrou que somente através de uma ação coordenada na Europa e no mundo teremos alguma chance de combater tais crises e suas consequências. A UE está atenta a este apelo, reforçando internamente seus objetivos estratégicos e promovendo o Green Deal (Acordo Verde) europeu, assim como a Agenda Digital através de suas políticas. Ao mesmo tempo, é importante que os objetivos ambientais e climáticos sejam integrados ao apoio fornecido aos nossos parceiros externos. Embora a crise atual nos lembre a fragilidade do sistema global, ela também dá a todos nós uma oportunidade única de estarmos mais bem preparados para o nosso futuro. Esse é um desafio que precisamos enfrentar em conjunto com parceiros que compartilhem da mesma visão. Em última análise, trata-se de encontrar uma base comum e estabelecer um consenso sobre a noção mais ampla, no nosso mundo contemporâneo, das ameaças à segurança e da cooperação em matéria de segurança e como buscar respostas políticas eficazes em conjunto. ■

Ignacio Ybáñez

Ignacio Ybáñez é embaixador da União Europeia no Brasil. Diplomata espanhol, foi secretário de Estado do Ministério de Relações Exteriores e Cooperação de seu país, onde também ocupou o cargo de Diretor Geral de Política Externa e Assuntos Globais Multilaterais e Diretor Geral de África, Mediterrâneo e Oriente Médio. Além disso, ele foi embaixador espanhol na Rússia.

Ignacio Ybáñez is Ambassador of the European Union to Brazil. He is a Spanish Diplomat and was Secretary of State at the Ministry of Foreign Affairs and Cooperation of his country, where he also held the position of Director-General for Foreign Policy and Multilateral Global Affairs and Director-General of Africa, the Mediterranean and the Middle East. In addition, he was Spanish Ambassador to Russia.

A União Europeia, um ator crucial em questões de segurança e defesa global

The European Union, a crucial actor in matters of global security and defence

Ignacio Ybáñez

Embaixador, Chefe da Delegação da União Europeia no Brasil

Ambassador, Head of the Delegation of the European Union to Brazil

Nos últimos 17 anos, a Conferência do Forte de Copacabana tem oferecido de maneira continuada uma oportunidade única no Brasil para discutir questões de inquietação e interesse comuns sob o escopo do tema de Paz e Segurança. Essa oportunidade de compartilhar conhecimento e de interagir é essencial em um mundo que enfrenta vários desafios comuns e interligados e, mais ainda, desde que a pandemia da COVID-19 testou a resiliência do mundo todo.

Nosso mundo, hoje, é caracterizado por vulnerabilidades, conflitos, tensões e, acima de tudo, incerteza global, observada sobretudo ultimamente. Isso é verdade em todos os continentes, inclusive nas fronteiras da União Europeia e do Brasil. Os grandes desafios de nosso tempo exigem soluções multilaterais; em um mundo de crescente instabilidade e ameaças transfronteiriças à nossa segurança, nosso mantra continua sendo "nenhum país pode ser bem-sucedido sozinho".

Conforme ressaltado pelo Alto Representante e Vice-Presidente da Comissão Europeia Josep Borrell, "*O aumento das tensões e conflitos*

For the past 17 years, the Forte de Copacabana Conference has continued to offer a unique opportunity in Brazil to discuss issues of common concern and interest under the umbrella theme of Peace and Security. This moment of shared knowledge and interactions is essential in a world that is facing multiple intertwined common challenges, and even more so since the COVID-19 pandemics tested the resilience of the entire world.

Our world nowadays is characterized by global vulnerabilities, conflicts, tensions and, above all, uncertainty especially as seen lately. On every continent, this continues to be true, including on the borders of our European Union, as well as on those of Brazil. The great challenges of our time require multilateral solutions; in a world of increasing instability and cross-border threats to our security, our mantra remains "no country can succeed alone".

As underlined by the High Representative/ Vice-President of the European Commission Josep Borrell, "*Rising international tensions and conflicts at*

the doorstep of Europe urge us to take our collective security into our own hands". This challenging international environment calls for more European unity, solidarity and resilience, with Member States working together for a stronger European Union that promotes peace and security and protects its citizens, thereby reinforcing the European identity and its independence, in line with our Treaties. Common Security and Defence Policy/CSDP is at the very heart of the European Union's external policy. An ambitious agenda has been set out to strengthen the ability to act autonomously as a Union whenever necessary and, at the same time, to make it a better global partner and security provider.

With the Council Conclusions on Security and Defence approved on the 17th of June 2020, we can now draw lessons and recommendations from a comprehensive, 360-degrees analysis of the full range of threats and challenges, which will provide the framework for the Member States to develop a Strategic Compass document to be adopted by the Council in 2022. We need a common strategic culture: a common way of looking at the world, of defining threats and challenges as the basis for addressing them together. This Compass will enhance and guide the implementation of the Level of Ambition agreed in November 2016 in the context of the EU Global Strategy and could further contribute to developing the common European security and defence culture. It will also define policy orientations and specific goals and objectives in areas such as crisis management, resilience, capability development and partnerships.

Within the Global Strategy, on security and defence, we have shown that the European Union knows how to deliver if there is political will. We made major progress, based on the understanding that it is essential for Europe to take greater responsibility for its own security. A set of new mechanisms for coordination of planning, spending and operations were created to allow Member States and the European Union to work together in order to ensure we are fit to face the threats and challenges of tomorrow.

To deliver more capabilities through deepening European cooperation

The **Capability Development Plan (CDP)** defines the EU Capability Development Priorities jointly agreed on by Member States. We have three major instruments that are helping Member States make their defence spending more efficient, as well as develop all the military capabilities that we need – from the skies to the sea, to the cyberspace. Member States are then encouraged to take more into account the EU defence planning tools and better use them in their national defence planning processes.

A first instrument is the **Coordinated Annual Review on Defence (CARD)** created to help Member States identify opportunities for new collaborative projects. It monitors the implementation of CDP priorities by Member States.

internacionais à porta da Europa nos exorta a tomar nossa segurança coletiva em nossas próprias mãos". Este ambiente internacional desafiador exige mais unidade, solidariedade e resiliência da Europa, com os Estados-Membros trabalhando juntos por uma União Europeia mais forte que promova a paz e a segurança e proteja seus cidadãos, reforçando, assim, a identidade europeia e sua independência em consonância com nossos Tratados. A Política Comum de Segurança e Defesa/PCSD está no cerne da política externa da União Europeia. Foi estabelecida uma agenda ambiciosa para fortalecer a capacidade de agir autonomamente como União sempre que necessário e, ao mesmo tempo, se tornar um melhor parceiro global e provedor de segurança.

Com as Conclusões do Conselho sobre Segurança e Defesa aprovadas em 17 de junho de 2020, podemos, agora, extrair lições e recomendações de uma análise abrangente de toda a gama de ameaças e desafios, que fornecerá a estrutura para os Estados-Membros desenvolverem um documento da orientação estratégica a ser adotado pelo Conselho em 2022. Precisamos de uma cultura estratégica comum: uma maneira comum de entender o mundo, de definir ameaças e desafios como base para enfrenta-los juntos. Este documento melhorará e orientará a implementação do Nível de Ambição acordado em novembro de 2016 no contexto da Estratégia Global da UE e poderá contribuir ainda mais para o desenvolvimento da cultura europeia comum de segurança e defesa. Também definirá orientações políticas e metas e objetivos específicos em áreas como gestão de crises, resiliência, desenvolvimento de capacidades e parcerias.

No âmbito da Estratégia Global, sobre segurança e defesa, mostramos que a União Europeia sabe como cumprir seus compromissos quando há vontade política. Avançamos substancialmente com base no entendimento de que é essencial que a Europa assuma maior responsabilidade por sua própria segurança. Um conjunto de novos mecanismos de coordenação do planejamento, gastos e operações foi criado para permitir que os Estados-Membros e a União Europeia trabalhem juntos a fim de garantir que estejamos aptos a enfrentar as ameaças e os desafios vindouros.

Proporcionar mais capacidades através do aprofundamento da cooperação europeia

O **Plano de Desenvolvimento de Capacidades (PDC)** define as Prioridades de Desenvolvimento de Capacidades da UE acordadas em conjunto pelos Estados-Membros. Temos três instrumentos principais que estão ajudando os Estados-Membros a tornar seus gastos com defesa mais eficientes, assim como a desenvolver todas as capacidades militares de que precisamos - dos céus ao mar e ao ciberespaço. Os Estados-Membros são incentivados a ter mais em conta os instrumentos de planejamento de defesa da UE e a melhor usá-los em seus processos nacionais de planejamento de defesa.

Um primeiro instrumento é a **Análise Anual Coordenada em matéria de Defesa (AACD)**, criada para ajudar os Estados-Membros a identificar oportunidades para novos projetos colaborativos. Esse instrumento monitora a implementação das prioridades do PDC pelos Estados-Membros.

A second instrument, and perhaps the most visible one, is the **Permanent Structured Cooperation/PESCO** which gathers 25 Member States with, so far, almost 50 ongoing projects on diverse areas such as training facilities, land formation systems, maritime, air systems, cyber, joint multiple services or even space. In PESCO, we need to further implement the operational domain and the European collaborative approach (e.g. equipment procurement and defence Research & Technology). To gain more efficiency, we will soon agree on the objectives and tangible results to be achieved for the next PESCO phase (2021-2025). We are also looking forward to defining the general conditions under which third States could exceptionally be invited to participate in individual PESCO projects which would allow us to act on a larger scale if necessary.

A third and crucial instrument is the **European defence fund (EDF)** which, launched in 2017, provides a key contribution. It promotes defence cooperation among companies and between Member States to foster innovation, sustainable supply chains and develop state-of-the-art defence technology and products. This, in turn, will lead to cost-savings. The fund coordinates, supplements and amplifies national investments in defence. It could also play an important role in overcoming the consequences and effects of the ongoing economic crisis for the defence sector, including for both small and medium-sized enterprises (SMEs) and mid-caps, by fostering defence investment and cross-border cooperation. In this sense, and as part of the EDF, the European Defence Industrial Development Programme/EDIDP announced the first 19 projects selected for funding in June of 2020.

In line with the financing of the EDF, Member States also play a key role in the budgetary challenge. At a time of increased global uncertainty, they need to maintain their levels of defence spending and avoid cuts at the expense of our collective security. Above all, Member States need to spend together, through common procurement and on commonly agreed capability shortfalls. It is important to reflect our security and defence priorities in the negotiations of the next EU budget for 2021-2027: all our ambitions in the area of operations, capabilities and resilience ultimately depend on the availability of financial resources.

To strengthen our operational engagement

The EU currently conducts **17 missions and operations under the Common Security and Defence Policy (CSDP)**, 11 civilian and 6 military, deployed outside EU borders. Over 4,500 women and men are serving abroad: in Africa, the Western Balkans and Eastern Europe, the Middle East as well as at sea. Brazil is currently participating, through the Portuguese's contingency in the European Union Training Mission/EUTM in the Central African Republic.

By providing security to countries abroad, we are also contributing to security at home. As a matter of fact, conflicts and crises are a breeding ground for terrorism and organised crime, which has already had a direct impact on our security. EU missions and operations are carrying out different tasks, reflecting the situation on the ground,

Um segundo instrumento, e talvez o mais visível, é a **Cooperação Estruturada Permanente - CEP/PESCO**, que reúne 25 Estados-Membros com, até o momento, quase 50 projetos em andamento em diversas áreas, como instalações de treinamento, capacitação, sistemas terrestres, marítimos, aéreos e cibernéticos, múltiplos serviços conjuntos e até espaciais. No CEP/PESCO, precisamos avançar na implementação do domínio operacional e a abordagem colaborativa europeia (por exemplo, aquisição de equipamentos e pesquisa e tecnologia de defesa). Para obter mais eficiência, em breve chegaremos a um acordo sobre os objetivos e resultados tangíveis a serem alcançados na próxima fase do CEP/PESCO (2021-2025). Também esperamos definir as condições gerais sob as quais os países não-membros poderiam ser excepcionalmente convidados a participar de projetos CEP/PESCO específicos, o que nos permitiria agir em maior escala, se necessário.

Um terceiro e crucial instrumento é o **Fundo Europeu de Defesa (FED)**, que, lançado em 2017, oferece uma contribuição fundamental. Promove a cooperação em defesa entre empresas e entre Estados-Membros para promover a inovação, cadeias de suprimentos sustentáveis e desenvolver tecnologias de ponta e produtos para defesa. Isso, por sua vez, resultará em economia de custos. O fundo coordena, complementa e amplia os investimentos nacionais em defesa. Também poderia desempenhar um papel importante na superação das consequências e efeitos da atual crise econômica no setor de defesa, inclusive para pequenas e médias empresas (PMEs) e mid-caps (empresas de média capitalização), promovendo o investimento em defesa e a cooperação transfronteiriça. Nesse sentido, e como parte do FED, o Programa Europeu de Desenvolvimento Industrial de Defesa/PEDID anunciou os primeiros 19 projetos selecionados para receber financiamento em junho de 2020.

Em conformidade com o financiamento do FED, os Estados-Membros também desempenham um papel fundamental no desafio orçamentário. Em um momento de crescente incerteza global, eles precisam manter seus níveis de gastos com defesa e evitar cortes às custas de nossa segurança coletiva. Sobretudo, os Estados-Membros precisam gastar coletivamente, através de aquisições conjuntas e considerando déficits de capacidade coletivamente acordados. É importante refletir nossas prioridades de segurança e defesa nas negociações do próximo orçamento da UE para 2021-2027: todas as nossas ambições na área de operações, capacidades e resiliência dependem, em última análise, da disponibilidade de recursos financeiros.

Para fortalecer nosso compromisso operacional

Atualmente, a UE realiza 17 missões e operações no âmbito da **Política Comum de Segurança e Defesa (PCSD)**, sendo 11 civis e 6 militares, destacadas fora das fronteiras da UE. Mais de 4.500 mulheres e homens estão servindo no exterior: na África, nos Balcãs Ocidentais e Europa Oriental, no Oriente Médio e também no mar. O Brasil está participando atualmente, por meio da contingência de portugueses na Missão de Treinamento da União Europeia/EUTM na República Centro-Africana.

Ao fornecer segurança para países no exterior, também estamos contribuindo para a segurança em nossas fronteiras. De fato, conflitos e crises são um terreno fértil para o terrorismo e o crime organizado, que já tiveram impacto direto em nossa segurança. As

enabling the implementation of peace agreements, providing training and advice to military, police and other authorities, such as border guards, or contributing to maritime security.

Our international missions now have better command structures, and we have committed to investing more in our civilian action – which remains the pride of the European Union. The capacity of action outside Europe and the credibility of our efforts to collectively promote peace and security beyond our borders will also be enhanced by the new EUR 8 billion European Peace Facility/EPF, a fund outside of the Union's multi-annual budget. It will enable the financing of operational actions under the Common Foreign and Security Policy (CFSP) that have military or defence implications.

To deepen our partnerships and uphold multilateralism

As we strengthened ourselves, we have also strengthened our security and defence cooperation with partners all around the world. Our **global partnerships** remain a cornerstone of European security and defence. Working closely with NATO, pragmatic proposals were made to further strengthen cooperation in areas such as military mobility and exercises. By reinforcing our capabilities in security and defence, Europe is strengthening the transatlantic alliance. The European Union also intends to further develop our partnership with the United Nations not only within the ongoing CSDP missions and operations in same theatre with UN missions but also towards the UN-EU Strategic partnership in peacekeeping with actions on conflict prevention, transitions or Women, Peace and Security.

On **multilateralism**, Europe is, by definition, a cooperative and multilateral power. As underlined by the recent adoption of a new strategic agenda for 2019-2024, the European Union will remain a driving force behind multilateralism and the global rules-based international order, ensuring openness and fairness and the necessary reforms. In years when multilateralism and the UN system have undergone increasing pressure, we have invested in multilateralism like never before. We have stepped up our financial support to the United Nations and support the UN Secretary General's reform agenda and always worked to find a multilateral solution to the many difficult problems of our time.

It is then, through this work, that we have been the most successful when we have been united. A "joined-up" Union is the best way to make our action more effective. It is also in this context that our partnership with Latin America, and more precisely with South America and Brazil, is gaining new relevance and urgency. The joint communication, adopted in April 2019, called "European Union, Latin America and the Caribbean: joining forces for a common future", focuses on the four key sectors to develop our partnership: prosperity, democracy, resilience, and effective global governance, with practical steps for each of these fields. We have still work to do in all these areas.

missões e operações da UE desempenham diferentes tarefas, refletindo a situação no terreno, possibilitando a implementação de acordos de paz, fornecendo treinamento e consultoria a serviços militares, policiais e outras autoridades, como guardas de fronteira, ou contribuindo para a segurança marítima.

Nossas missões internacionais agora têm melhores estruturas de comando e nos comprometemos a investir mais em nossa ação civil - que continua sendo o orgulho da União Europeia. A capacidade de ação fora da Europa e a credibilidade de nossos esforços para promover coletivamente a paz e a segurança para além de nossas fronteiras também serão aprimoradas pelo novo Fundo Europeu para a Paz. Com 8 bilhões de euros, é um fundo fora do orçamento plurianual da União e permitirá o financiamento de ações operacionais no âmbito da Política Externa e de Segurança Comum (PESC) que tenham implicações militares ou de defesa.

Para aprofundar nossas parcerias e defender o multilateralismo

À medida que nos fortalecemos, também fortalecemos nossa cooperação em segurança e defesa com parceiros em todo o mundo. Nossas parcerias globais continuam sendo a pedra angular da segurança e defesa europeias. Trabalhando em estreita colaboração com a OTAN, foram apresentadas propostas pragmáticas para fortalecer ainda mais a cooperação em áreas como mobilidade militar e exercícios militares. Ao reforçar nossas capacidades em segurança e defesa, a Europa está fortalecendo a aliança transatlântica. A União Europeia também pretende desenvolver ainda mais nossa parceria com as Nações Unidas, não apenas dentro das missões e operações da PCSD que já estão em andamento junto com as missões da ONU, mas também em direção à parceria estratégica ONU-UE em manutenção da paz, com ações relacionadas à prevenção, transições ou mulheres, Paz e segurança.

A respeito do **multilateralismo**, a Europa é, por definição, uma potência cooperativa e multilateral. Como ressaltado pela recente adoção de uma nova agenda estratégica para 2019-2024, a União Europeia continuará sendo uma força motriz por trás do multilateralismo e da ordem internacional baseada em regras globais, garantindo transparência e justiça às reformas necessárias. Nos anos em que o multilateralismo e o sistema da ONU sofreram pressões crescentes, fizemos investimentos sem precedentes no multilateralismo. Intensificamos nosso apoio financeiro às Nações Unidas e apoiamos a agenda de reformas do Secretário-Geral da ONU e sempre trabalhamos para encontrar uma solução multilateral para os muitos problemas de nosso tempo.

É, portanto, através deste trabalho que obtivemos os maiores êxitos quando unidos. Uma união forte é a melhor maneira de tornar nossa ação mais eficaz. É também nesse contexto que nossa parceria com a América Latina, e mais precisamente com a América do Sul e o Brasil, ganha nova relevância e urgência. O comunicado conjunto, adotado em abril de 2019, chamado "União Europeia, América Latina e Caribe: unindo forças para um futuro comum", concentra-se nos quatro principais setores para desenvolver nossa parceria: prosperidade, democracia, resiliência e governança global eficaz, com etapas práticas para cada uma dessas áreas, e ainda temos muito trabalho a fazer em todas elas.

The challenging international security environment and in particular the security-related consequences of the current pandemic highlight the importance of further developing the partnerships with international and core regional partner organisations, as well as with partner countries. Equally urgent is the need to strengthen our tools to counter hybrid threats, including disinformation and cyber-attacks. The outbreak of Covid-19 has been a stark reminder of how critical this subject has become in protecting our societies.

We are convinced that advancing together with countries around the world, such as Brazil and other South American partners, we can build the appropriate governance mechanisms for our challenging world. Given the nature of the dares we are facing we cannot afford going in different directions or diverging. The Forte de Copacabana Conference can help us to think together through these common challenges.

O ambiente desafiador de segurança internacional e, em particular, os efeitos da atual pandemia relacionados à segurança, ressaltam a importância de desenvolver ainda mais as parcerias com organizações parceiras regionais e internacionais, assim como com os países parceiros. Igualmente urgente é a necessidade de fortalecer nossas ferramentas para combater ameaças híbridas, incluindo a desinformação e ataques cibernéticos. O surto de Covid-19 foi um lembrete de quão crítico esse assunto se tornou na proteção de nossas sociedades.

Estamos convencidos de que, avançando unidos com países do mundo todo, como o Brasil e outros parceiros sul-americanos, podemos construir os mecanismos de governança adequados para enfrentar os desafios de nosso mundo. Dada a natureza das adversidades que estamos enfrentando, não podemos permitir avançar em direções diferentes ou divergir. A Conferência do Forte de Copacabana pode nos ajudar a pensar juntos sobre esses desafios comuns.

André Clark

André Clark é General Manager da Siemens Energy Brasil desde 1º de março de 2020, tendo sido Presidente e CEO da Siemens no Brasil e também CEO da ACCIONA para o Brasil, Bolívia, Uruguai e Paraguai. André nasceu em São Paulo e começou sua carreira no setor de Papel e Celulose em 1995. Possui 17 anos de experiência nas áreas de energia, petróleo e gás e nas áreas de indústria, logística e infraestrutura. Atua ativamente em diversas associações e entidades de classe de diversos segmentos de negócios e está presente nas mais importantes discussões sobre questões relacionadas ao Brasil. É formado em engenharia química pela Escola Politécnica da Universidade de São Paulo (USP) e possui MBA em Finanças e Gestão de Operações pela New York University Stern School of Business.

André Clark is the General Manager of Siemens Energy Brazil since March 1st, 2020, having previously been President and CEO of Siemens in Brazil and also CEO of ACCIONA for Brazil, Bolivia, Uruguay and Paraguay. André was born in São Paulo and his career began in the Pulp & Paper industry in 1995. He has 17 years of experience in Energy, Oil & Gas, Manufacturing, Logistics and Infrastructure areas. With an active role in several associations and entities from different business segments, he is present in the most important discussions about Brazil. He holds Bachelor's Degree in Chemical Engineering from Escola Politécnica of Universidade de São Paulo (USP) and MBA in Finance and Operations Management from New York University Stern School of Business.

Cibersegurança em infraestruturas críticas

Cybersecurity for critical infrastructure

André Clark

CEO da Siemens Energy no Brasil

CEO of Siemens Energy in Brazil

A infraestrutura e a defesa de um país são elementos praticamente indissociáveis. Provedores de infraestrutura (água, energia, transportes etc.), sejam eles públicos ou privados, dependem de um ambiente seguro para garantir o fornecimento desses itens à população, assegurando qualidade de vida à sociedade. À medida que a manutenção do ambiente seguro é papel das Forças Armadas e das forças de segurança, a relação entre a infraestrutura de um país e sua estrutura de defesa é direta.

Nos últimos anos, a presença da iniciativa privada na infraestrutura brasileira se intensificou, seja pelo modelo de concessões, ou mesmo por parcerias público-privadas. Ainda que o provimento da infraestrutura continue sendo papel do Estado, a viabilização de investimentos, principalmente com vistas à modernização dessas estruturas, ganhou enorme impulso com a inserção do capital privado nessa equação. Seria praticamente impossível projetar qualquer salto de crescimento econômico para o Brasil sem direcionar os grandes gargalos de infraestrutura do País e, de fato, o investimento em serviços básicos e fundamentais é a melhor poupança de uma nação que pretenda coinvestir em um determinado espaço.

A country's critical infrastructure and its defense systems are closely related. Utilities service providers (water, energy, transport, etc.), whether public or private, depend on a safe environment to guarantee the delivery of services to the population and, hence, ensure society's quality of life. As the preservation of a safe environment is the role of the Armed Forces and of the security forces, there is a direct relationship between a country's critical infrastructure and its defense structure.

In recent years, the presence of the private sector in Brazilian critical infrastructure segment has intensified, both through concessions and public-private partnerships. Although the provision of utilities remains under the responsibility of the State, the feasibility of investments, mainly to modernize these structures, has gained enormous momentum with the insertion of private capital in the equation. It would be practically impossible to project any leap in economic growth for Brazil without addressing the country's major infrastructure bottlenecks and, as a matter of fact, investing in basic and critical services is the best way to ensure resources for a nation that intends to co-invest in any given sector.

In this scenario, the relationship between infrastructure, the State and the private sector has generated countless opportunities and very important discussions. When we discuss the defense industry, the debate doesn't revolve only around weaponry, but also includes a very large amount of technology, services and products that have dual uses in the economy. Looking back, the Internet was created in a defense development environment, as well as the touch screen and many other components of daily use.

For many years Brazil gave signs of a dormant defense industry. Recently, however, this seems to be changing. Numerous initiatives have been noted, such as the revival of its naval industry, the emergence of a new way of strategic thinking for the defense industry and, in a very particular way, the creation of software involving the research and development of cybersecurity solutions. Although it is a relatively new topic in the business environment, cybersecurity has found fertile ground for development in Brazil.

This is not fortuitous. There are several everyday examples that indicate a certain pioneering spirit and undeniable maturity in the Brazilian information technology segment. For many years now, at least since 1998, Brazilians file their income tax return electronically. And for more than twenty years, account holders have also been gradually adopting the use of the Internet and applications to carry out their banking transactions. All of these activities became possible and were incorporated into daily life due to a robust computerized system created and developed in Brazil.

However, it is not because of what we have, but mainly because of what we lack, that the binomial infrastructure/information technology seems increasingly connected. Faced with numerous hindrances in its economy, Brazil seeks to develop its critical infrastructures and add productivity to them, noting this is the great frontier of economic growth for the next decade. Due to these obstacles, investing in infrastructure is possibly becoming one of the most important solutions for the country to emerge from low economic growth and boost job creation.

Therefore, these two issues - infrastructure and cybersecurity - converge since the new Infrastructure 4.0 (be it the intelligent supply of energy, water, transport or industry) has digital characteristics, bringing a high level of automation, less need for human intervention in repetitive tasks and a capacity for a more integrated vision through data, due, for example, to the concept of Internet of Things (IoT). We are moving towards the convergence of these worlds: an absolutely safe, stable and available infrastructure, and the digital environment, which changes every day, has great technological leaps, different versions and continuous changes.

This new scenario creates a very challenging interface but also one of great opportunities with great possibilities to create markets, professions, companies, jobs and businesses. Therefore, it is a strategic issue and needs to be understood as such, after all, it creates great opportunities in the Brazilian economic environment to address and build public policies for the generation of jobs, income and development, not only in the military arena, but also, in several aspects, regarding the general economic environment and other countries.

Nesse cenário, a relação entre infraestrutura, Estado e iniciativa privada tem gerado inúmeras oportunidades e discussões muito importantes. Quando falamos de indústria de defesa, o que está sendo discutido não são apenas armamentos, mas uma quantidade muito grande de tecnologia, serviços e produtos que têm utilização dual na economia. Basta lembrar que a própria internet foi criada em um ambiente de desenvolvimento de defesa, assim como a tela *touch* e muitos outros elementos.

Durante muitos anos, o Brasil deu sinais de adormecimento de sua indústria de defesa, o que parece estar sendo revertido mais recentemente. Inúmeras iniciativas têm sido registradas nos últimos tempos, como o renascimento da indústria naval, o pensamento estratégico sobre a indústria de defesa e, de maneira muito particular, a criação de *softwares* envolvendo pesquisa e desenvolvimento de soluções de cibersegurança. Embora seja um tema relativamente novo no ambiente de negócios, o tema da segurança cibernética tem encontrado terreno fértil para seu desenvolvimento no Brasil.

Isso não se dá ao acaso. Há diversos exemplos cotidianos que atestam certo pioneirismo e inegável maturidade do Brasil no segmento de tecnologia da informação. Há muitos anos, o brasileiro acostumou-se a fazer sua declaração de Imposto de Renda por via eletrônica. Pelo menos desde 1998, portanto há mais de vinte anos, os correntistas também adotaram progressivamente o uso da internet e dos aplicativos para concretizar suas transações bancárias. Todas essas atividades tornaram-se possíveis e foram incorporadas ao cotidiano por conta de um robusto sistema informatizado, criado e desenvolvido no Brasil.

Entretanto, não é apenas pelo que já temos, mas sobretudo pelo que ainda nos falta, que o binômio infraestrutura e tecnologia da informação parece cada vez mais ligado. Diante de inúmeros gargalos em sua economia, o Brasil é um país que procura desenvolver suas estruturas e agregar produtividade a elas, já que esta é a grande fronteira de crescimento econômico da próxima década. Devido a esses entraves, investir em infraestrutura está se tornando uma das grandes possíveis soluções para que o País saia de situação de baixo crescimento e impulsione a geração de emprego.

As duas questões – infraestrutura e cibersegurança –, portanto, convergem, à medida que a nova Infraestrutura 4.0 (seja o fornecimento inteligente de energia, de água, de transportes ou a indústria) tem características digitais, trazendo alto nível de automação, menor necessidade de intervenção humana em tarefas repetitivas e uma capacidade de visão integrada por meio de dados, graças, por exemplo, ao conceito de Internet das Coisas (IoT). Estamos caminhando para o encontro desses mundos: uma infraestrutura absolutamente segura, estável, disponível e o ambiente digital, que muda todos os dias, tem grandes saltos tecnológicos, versões e mudanças contínuas.

Esse novo cenário cria uma interface bastante desafiadora e também de grandes oportunidades. Existem, nesse espaço, grandes possibilidades de criar mercados, profissões, empresas, empregos e negócios. Portanto, o tema é profundamente estratégico e precisa ser encarado como tal, pois cria no espaço econômico brasileiro grandes oportunidades para endereçar e configurar a política pública para a geração de emprego, renda e desenvolvimento, não só no mundo militar, mas espalhando-se para o ambiente da economia geral em vários aspectos.

An example of one of the most interesting Brazilian public policies for the energy sector, both in the electricity and in the oil & gas segments, is the mandatory allocation, by the regulator, of a percentage of the operator´s revenues to research and development projects. In essence, this initiative can also encourage the development of cybersecurity tools and processes by using these resources to generate an impact of positive externalities even in the short term, boosting expertise in this segment and increasing the country's security spectrum.

Data protection: impact on critical infrastructure

The plan for the year 2020 was to engross discussions and strategic decision making, such as the entry into force of the General Data Protection Law (LGPD, in its Portuguese abbreviation). Although the coronavirus pandemic has postponed the implementation of some of these decisions, the issue remains one of major concern for public and private players regarding cybersecurity. The pandemic itself exposed the core of this issue, with countries monitoring the health of their citizens, in a move that often overrides individual privacy. In situations of social emergencies like the one we currently face, actions of this type are frequently used. In the national security field, which includes critical infrastructure, this also needs to be a topic addressed both by the State, especially in the figure of its defense agents, and by the private sector.

Without giving proper focus to the topic of cybersecurity associated with critical infrastructures and utilities, situations such as the interruption of water supply or electricity in a city become an increasing possibility unless measures are taken to mitigate these risks. A coordinated attack on the residential Internet infrastructure at a time of social isolation as the one imposed by the pandemic may have the potential to further paralyze a country. The infrastructure operator is, above all, a provider of utilities, being completely responsible for its consumers. In several aspects, this agent assumes risks related to State issues and, with the coronavirus pandemic, we experienced a situation in which airports and roads, many of them granted to the private sector, were practically paralyzed, causing important financial risks for operators and investors. In moments like this, these companies need to maintain the service and, at the same time, converge with the State to guarantee that the infrastructure remains active and safe, thus indicating, also in this case, the intrinsic relationship between critical infrastructures and defense.

A study by professor Tácito Augusto Silva Leite, titled "Cyber-Physical Security in Electric Companies"(https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2017/10/eBook-Seguranca-Ciberfisica-nas-Empresas-de-Energia-Tacito-Leite-2017.pdf), highlights the growing relevance of cybercrimes in the infrastructure segment. According to his study, a survey conducted by Aon, an insurance company in 2017, with two thousand respondents from 64 countries, showed that so-called cybercrimes went up from being the ninth, among the ten main risks identified by companies, to the fifth position.

However, if moments of social emergency expose a country's weaknesses, they also present opportunities for companies, entities and the government to create efficient

Um exemplo: uma das políticas públicas mais interessantes do Brasil, no setor amplo de energia, tanto elétrica quanto no setor de petróleo & gás, é a destinação obrigatória, pelo regulador, de uma porcentagem do faturamento dos operadores desses segmentos para projetos de pesquisa e desenvolvimento. Como proposta, essa iniciativa pode incentivar também o desenvolvimento de ferramentas e processos de cibersegurança, utilizando esses recursos com o objetivo de gerar um impacto de externalidades positivas até de curto prazo, impulsionando o know-how nesse segmento e aumentando o espectro de segurança do país.

Proteção de dados: impacto em infraestruturas críticas

O ano de 2020 foi planejado para absorver discussões e tomadas de decisões estratégicas, como a entrada em vigor da Lei Geral de Proteção de Dados (LGPD). Ainda que a pandemia de coronavírus tenha postergado algumas dessas decisões, o tema segue como uma das maiores preocupações dos atores públicos e privados relacionadas à cibersegurança. A própria pandemia expôs o cerne dessa questão, com países monitorando a saúde dos seus cidadãos, em um movimento que muitas vezes se sobrepõe à privacidade de cada um. Em situações de emergências sociais como esta, ações desse tipo estão sendo utilizadas e no ambiente de segurança nacional, como o das infraestruturas críticas, este também precisa ser um tema endereçado tanto pelo Estado, especialmente na figura de seus agentes de defesa, quanto pela iniciativa privada.

Sem o devido foco no tema de cibersegurança associado a infraestruturas críticas, situações como a paralização do abastecimento de água ou de energia elétrica de uma cidade passam a ser cada vez mais possíveis, se não forem adotadas medidas para mitigar esses riscos. Um ataque coordenado à infraestrutura de internet domiciliar, em um momento como o de isolamento social imposto pela pandemia, pode ter o potencial de paralisar ainda mais o País. O operador de infraestrutura é, antes de tudo, um provedor de serviços públicos, sendo completamente responsável pelos seus consumidores. Em vários aspectos, esse agente assume riscos relacionados a questões de Estado e com a pandemia do coronavírus, vivenciamos uma situação na qual aeroportos e estradas, muitos deles concedidos à iniciativa privada, ficaram praticamente paralisados, ocasionando riscos financeiros importantes para os operadores e seus investidores. É nesse momento que essas empresas precisam manter o serviço e, ao mesmo tempo, convergir com o Estado para garantir essa infraestrutura ativa e segura, evidenciando também aqui a relação intrínseca entre infraestruturas críticas e defesa.

Um estudo do professor Tácito Augusto Silva Leite, intitulado "Segurança Ciberfísica nas Empresas de Energia" (https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2017/10/eBook-Seguranca-Ciberfisica-nas-Empresas-de-Energia-Tacito-Leite-2017.pdf), evidencia a relevância crescente dos crimes cibernéticos no segmento de infraestrutura. Segundo esse estudo, uma pesquisa realizada pela seguradora Aon, em 2017, com dois mil respondentes, de 64 países, mostrou que o chamado cibercrime passou do nono lugar, entre os dez principais riscos identificados pelas companhias, para a quinta colocação.

solutions. In this respect, Brazil has stood out for its creativity in a context marked by a lack of resources. In recent years, at least eight new digital banks have been created and, in 2019, we were the world's third largest producer of unicorns (high-value start-ups), after the United States and China. We have a market economy that is democratic, open and with transparent regulatory issues in several aspects. We also have excellent IT companies in Brazil, with great success going international and this perspective is extremely favorable for the development of the cybersecurity agenda.

Recently, Brazil has seen an increase in co-creation processes between companies, customers, suppliers, startups, developers and universities. The innovation process is changing in form and scale, using, for instance, methodologies such as Agile. If in the past it took a product two, three or even four years to have an operational prototype, in the co-creation world things happen so fast that the development team in general needs to have this new prototype in much less than a month. This requires the joint effort of numerous professionals and multifunctional applications for that solution and, in this context, the critical infrastructure sector has benefited and can benefit even more from this process, including the development of cybersecurity solutions.

What we have been witnessing in this joint effort for innovation is the gathering of the network specialist with the cybersecurity specialist and with technicians from the utilities (from the electric sector, transport etc.). These are teams that need to perform with excellence and work with methodologies that accelerate processes in order to solve problems in a very dynamic and fast way. This new trend is particularly interesting in the military world, as it brings an innovative way of operating to a segment that, by nature, always needs to be very agile, creative, fast and effective in delivering solutions, which are usually related to very relevant State issues, including national security.

Incorporating such innovative methodologies is a paradigm breaker, because the skills required for the creation and development of innovative solutions are many times found in young professionals, who change the mentality of these institutions. The Armed Forces are, in their essence, strictly meritocratic institutions, but the definitions of merit in the world of cybersecurity are different and consider skills, emotional intelligence and understanding of the digital world in a very different way.

5G: special attention to infrastructure

The present moment and the coming years have the potential to transform the way in which we consume and produce energy, use the means of transportation and relate to our cities' infrastructure. But it represents more than that. An intense and profound transformation is taking place and tends to create new standards, businesses and also challenges: the advent of 5G technology. One of the main differences between 5G and previous generations of networks is its focus on machine-to-machine communication and the Internet of Things (IoT). In particular, 5G supports communications with unprecedented reliability and very low latency.

Mas, se momentos de emergência social expõem eventuais fragilidades de um país, também se mostram como oportunidades para empresas, entidades e o poder público criarem soluções eficientes. Nesse aspecto, o Brasil tem se destacado pela criatividade no contexto da falta de recursos. Nos últimos anos, o país passou a ter pelo menos oito novos bancos digitais. Em 2019, fomos o terceiro maior produtor de unicórnios (*startups* de alto valor) do mundo, atrás apenas dos Estados Unidos e da China. Temos uma economia absolutamente de mercado, democrática, aberta e com questões de regulação bastante transparentes em vários aspectos. Temos ainda excelentes empresas de TI no Brasil, com grande sucesso se internacionalizando e esse panorama é extremamente profícuo para o desenvolvimento da pauta de cibersegurança.

Recentemente, o Brasil tem visto crescer os processos de cocriação entre empresas, clientes, fornecedores, *startups*, desenvolvedores e universidades. O processo de inovação está mudando de forma e escala, utilizando metodologias como o Agile, por exemplo. Se no passado um produto demorava dois, três ou quatro anos para ter um protótipo funcional, no mundo da cocriação o processo é tão rápido que o time de desenvolvimento em geral precisa ter esse novo protótipo em muito menos de um mês. Isso exige a união de inúmeros profissionais e aplicações multifuncionais para aquela solução e, neste contexto, o setor de infraestruturas críticas tem sido e pode ser ainda mais beneficiado por esse processo, inclusive para o desenvolvimento de soluções de cibersegurança.

Nesse esforço conjunto pela inovação, o que temos assistido é o encontro do especialista em rede com o de segurança cibernética e destes com técnicos dessas infraestruturas (sejam elas do setor elétrico, de transportes etc.). Esses times precisam funcionar em alto desempenho, com metodologias que aceleram processos para resolver problemas de forma muito ágil e rápida. Esse novo movimento é particularmente interessante no mundo militar, já que traz uma forma inovadora de operar para um segmento que, por natureza, precisa ser sempre muito ágil, criativo, rápido e eficaz na entrega de soluções, que normalmente estão relacionadas a questões de Estado de alta relevância, inclusive de segurança nacional.

Incorporar tais metodologias inovadoras mostra-se até como uma quebra de paradigma, pois muitas vezes essas habilidades requeridas para a criação e o desenvolvimento de soluções inovadoras poderão estar presentes em profissionais jovens, modificando a mentalidade dessas instituições. As Forças Armadas são, em sua essência, instituições estritamente meritocráticas mas, no mundo da cibersegurança, as definições de mérito são diferentes, considerando habilidades, inteligência emocional e entendimento do mundo digital de uma forma bastante diferente.

5G: atenção especial para a infraestrutura

O momento atual e os próximos anos têm o potencial de transformar a maneira pela qual consumimos e produzimos energia, utilizamos os meios de transporte e nos relacionamos com a infraestrutura de nossas cidades, mas não só. Uma intensa e profunda transformação está acontecendo e tende a criar novos padrões, negócios e também desafios: o advento do 5G. Uma das principais diferenças entre o 5G e as gerações anteriores de

At a time when the government, technical experts and the private sector are discussing the implementation of 5G in Brazil, it is essential to observe international experiences. In Germany, for example, the topic is treated as one of the pillars for the country's competitiveness in the coming decades, as it is a technology that catalyzes the concepts of IoT, Cloud Computing, Artificial Intelligence, Big Data and others.

The concept of cloud and edge computing tends to be the method of choice for data storage and gains strength in the economy beyond its unit cost, because it allows the operator to invest in services provided in stead of investing in building its own structures. Before this technology, companies had to establish their own servers to manage their operations' data and, when they needed new applications, it was necessary to update these structures at huge costs, which included maintenance. In the cloud era, this increase in capacity is achieved with a click. Quickly, a larger storage capacity is obtained and the use of 5G tends to further enhance this model.

However, it is important to emphasize that the use of 5G networks in different sectors of the economy cannot be linked only to the telecommunications operators' public networks. The application of this technology in different segments, including the electricity and oil & gas sectors, will be fundamental, not only to optimize such critical structures and improve service to society, but also to foster the development and application of cybersecurity solutions. In addition, this new world presented by 5G has enormous potential for creating new businesses in the so-called Digital Economy, allowing data to be collected in real time for applications of Artificial Intelligence concepts, especially for the application of Machine Learning.

Technology companies, such as Siemens Energy, are expanding their portfolios to offer customers not only the equipment needed for their business but also the cybersecurity structure that guarantees their integrity. Penetration testing in compliance with the ISO 62.443 standard evaluate the IT (Information Technology) and OT (Operational Technology) infrastructures to detect possible security flaws. In addition to generating detailed reports, this type of service also suggests a list of measures to mitigate these risks. Aware of the growing demand for cybersecurity solutions, Siemens entered into a partnership with an Israeli-born startup, Claroty, providing its customers with a platform that maps and continuously detects any instability, improper behavior or threat in a critical infrastructure. The sophistication of the system is such that it enables controlling even a remote access to these networks.

In the United States, Siemens joined thirteen other participants in the Center for Threat-Informed Defense, created by the MITRE Engenuity Foundation to design and develop cybersecurity solutions capable of preventing, detecting and mitigating cyber attacks, focusing mainly on structures whose operation affects society as a whole.

Another global initiative in favor of information security is the creation of the Charter of Trust, which has the endorsement of some of the largest technology companies and advocates, through a letter of commitment, mandatory rules and standards to generate confidence in cybersecurity and to advance the digitization of companies and countries in a collaborative way.

redes está no foco dessa tecnologia na comunicação máquina-máquina e na Internet das Coisas (IoT). Em particular, o 5G suporta comunicação com confiabilidade sem precedentes e latências muito baixas.

Neste momento em que o poder público, especialistas técnicos e a iniciativa privada discutem a implementação do 5G no Brasil, é fundamental observar exemplos internacionais. Na Alemanha, por exemplo, o tema é tratado como um dos pilares para a competitividade do país nas próximas décadas, uma vez que é uma tecnologia catalisadora dos conceitos de IoT, Computação em Nuvem, Inteligência Artificial, Big Data, entre outros.

O conceito de nuvem e computação de borda, tende a ser o método de escolha para o armazenamento de dados e ganha força na economia para além de seu custo unitário, à medida que possibilita ao operador investir em serviços prestados e não mais em estruturas próprias. Antes, empresas precisavam estabelecer seus próprios servidores para a gestão dos dados de suas operações e, quando havia a necessidade de novas aplicações, era preciso atualizar essas estruturas a custos vultosos, inclusive de manutenção. Na era da nuvem, esse aumento de capacidade é obtido com um clique. Rapidamente, obtém-se uma capacidade maior de armazenamento e o uso do 5G tende a potencializar ainda mais esse modelo.

Entretanto, é importante reforçar que a utilização de redes 5G em diversos setores da economia não pode estar ligada somente às redes públicas das operadoras de telecomunicações. A aplicação desta tecnologia em segmentos diversos, inclusive no setor elétrico e de petróleo e gás será fundamental, não apenas para otimizar tais estruturas críticas e aperfeiçoar o serviço à sociedade, como também para fomentar o desenvolvimento e a aplicação de soluções de cibersegurança. Além disso, o novo mundo apresentado pelo 5G tem enorme potencial para a criação de novos negócios da chamada Economia Digital, permitindo que dados sejam coletados em tempo real para aplicações dos conceitos de Inteligência Artificial, especialmente para a aplicação do Aprendizado de Máquina (Machine Learning).

Empresas de tecnologia, como a própria Siemens Energy, estão ampliando seus portfólios para oferecer aos clientes não apenas os equipamentos necessários aos negócios como também a estrutura de cibersegurança que garanta sua integridade. Testes de intrusão, aderentes à norma ISO 62.443, avaliam as infraestruturas de IT (Information Technology) e OT (Operational Technology), para detectar eventuais falhas de segurança. Além da geração de relatórios detalhados, esse tipo de serviço também sugere um rol de medidas de mitigação para esses riscos. Atenta à demanda crescente por soluções de cibersegurança, a Siemens firmou parceria com uma *startup* de origem israelense, a Claroty, disponibilizando a seus clientes uma plataforma que mapeia e detecta, de forma contínua, qualquer instabilidade, comportamento indevido ou ameaça em uma infraestrutura crítica. A sofisticação do sistema é tanta que ele é capaz de controlar inclusive o acesso remoto a essas redes.

Nos Estados Unidos, a Siemens juntou-se a outros treze participantes no Center for Theat-Informed Defense, criado pela Fundação MITRE Engenuity para criar e desenvolver soluções de cibersegurança que sejam capazes de prevenir, detectar e mitigar ataques cibernéticos, principalmente com foco em estruturas cuja operação afete a vida da sociedade como um todo.

A strategic topic for the Brazilian power sector

The cybersecurity issue is particularly strategic for the Brazilian power sector. Brazil is one of the only countries in the world to have an integrated national grid controlled through cloud. This robust system (Energy Management Network – REGER, in its Portuguese acronym), that takes into consideration the size of Brazil, with its continental dimensions, complexities and multiple forms of generation, was entirely created and developed in the country by the Eletrobrás Electric Energy Research Center (Cepel) and by Siemens.

The Institutional Security Office (GSI) and the Ministry of Defense are already discussing the issue of security for critical infrastructures with the participation of the private sector. The creation of regulatory standards that favor cybersecurity is not only a challenge, but also a huge opportunity to build a market for products and services related to the topic in Brazil. There are, in fact, several favorable aspects aligned at this moment: the urgency of investing in infrastructure, the need for this infrastructure to be deeply efficient and intelligent and the debate on the implementation of 5G.

In this conjunction of objectives, in addition to serving the large energy generation, transmission and distribution structures, joint efforts will also impact smaller investors in these areas. The concept of renewable energies, which have a seasonality characteristic and also the fragmentation of generation sources will lead to an increasing need to use IoT to control these systems. The incorporation of digitization into the infrastructure will make distributed energy viable. It will also make feasible a greater use of renewable sources, an intelligent use of that energy in periods of competitive prices and the consolidation of the *prosumer* (economic actors that can both produce and consume energy depending on the balance between supply and demand that the market can create).

The pursuit of digitalization of infrastructures will increase and is profoundly positive for the incorporation of technologies. On the other hand, this option also means great risks for the entire system, as it creates more vulnerability. Protection of these structures is also the role of the State. It is a very interesting situation: the market will seek the high-tech scenario, the regulator will follow this movement and, with that, new cybersecurity solutions will have to emerge. This reality is emerging all over the world and, in Brazil, a country rich in varied sources of energy, this option will be practically a requirement for the proper functioning of our infrastructure. It is a circle of increased vulnerability, but it is profoundly virtuous. ■

Outra iniciativa global em prol da segurança da informação vem da criação do Charter of Trust, que conta com o endosso de algumas das maiores empresas de tecnologia e preconiza, por meio de uma carta de compromisso, regras e normas obrigatórias para gerar confiança na cibersegurança e avançar com a digitalização das empresas e países de forma colaborativa.

Tema estratégico para o setor elétrico brasileiro

O tema de cibersegurança é particularmente estratégico para o setor elétrico brasileiro. O Brasil é um dos únicos países do mundo a ter um sistema integrado nacional, todo comandando por nuvem. Esse sistema robusto (Rede de Gerenciamento de Energia – REGER), do tamanho do Brasil, com suas dimensões continentais, complexidades e múltiplas formas de geração foi todo criado e desenvolvido no país pelo Centro de Pesquisas de Energia Elétrica da Eletrobrás (Cepel) e pela Siemens.

O Gabinete de Segurança Institucional (GSI) e o Ministério da Defesa já estão discutindo o tema de segurança para infraestrutura crítica com a participação da iniciativa privada. Este não é apenas um desafio, com a criação de padrões de regulação que privilegiam a cibersegurança, mas também uma enorme oportunidade de se criar um mercado de produtos e serviços relacionados ao tema no Brasil. São, de fato, vários planetas alinhados neste momento: a urgência do investimento em infraestrutura, a necessidade de que essa infraestrutura seja profundamente eficiente e inteligente e a discussão da implementação do 5G.

Nessa conjunção de objetivos, além de atender as grandes estruturas de geração, transmissão e distribuição de energia, os esforços conjuntos irão impactar também os investidores menores dessas áreas. O conceito de energias renováveis, que têm a característica das sazonalidades, e também a pulverização de fontes geradoras levará cada vez mais à necessidade do uso de IoT para comandar esses sistemas. A própria incorporação da digitalização à infraestrutura viabilizará a energia distribuída, o maior uso de fontes renováveis, a utilização inteligente dessa energia nos períodos de preços competitivos e a consolidação da figura do *prosumer* (atores econômicos que podem tanto produzir energia quanto consumi-la, a depender do balanço entre oferta e demanda que esse mercado pode criar).

A busca pela digitalização das infraestruturas será cada vez maior, o que é profundamente positivo para a incorporação de tecnologias. Por outro lado, essa opção também significa grandes riscos para o sistema inteiro, pois gera mais vulnerabilidades. E a proteção a essas estruturas é também papel do Estado. É uma situação muito interessante: o mercado vai buscar o cenário de alta tecnologia, o regulador vai acompanhar esse movimento e, com isso, novas soluções de cibersegurança vão ter que surgir. Essa realidade está acontecendo em todo o mundo e, no Brasil, país rico em fontes variadas de energia, tal opção será praticamente um requisito para o funcionamento adequado da nossa infraestrutura. É um círculo de aumento da vulnerabilidade, mas profundamente virtuoso. ■

Henning Speck

Henning Speck é consultor de segurança nacional do Grupo Parlamentar da CDU/CSU no Bundestag alemão. Ele é diplomata de carreira do Ministério das Relações Exteriores e serviu nas embaixadas alemãs em Washington, DC e Cabul, Afeganistão, além de ter ocupado várias funções no Ministério das Relações Exteriores e na equipe de segurança nacional da Chancelaria Federal.

Henning Speck is a National Security Advisor to the CDU/CSU Parliamentary Group in the German Bundestag. He is a Diplomat from the Federal Foreign Office and served at the German Embassies in Washington, DC and Kabul, Afghanistan, as well as in various capacities in the Foreign Office and the National Security Staff of the Federal Chancellery.

Fronteiras tradicionais: questões relacionadas a Soberania e Segurança

Traditional Frontiers: issues on Sovereignty and Security

Henning Speck

Consultor de Segurança Nacional do Grupo Parlamentar da CDU/CSU no Bundestag alemão

National Security Advisor to the CDU/CSU Parliamentary Group in the German Bundestag

O ano de 2020 provavelmente será lembrado como um divisor de águas na política e na cooperação internacionais. A pandemia de COVID, bem como as diversas políticas implementadas para lidar com seus desafios, mostraram não apenas os graus de conexão e interdependência de nossas economias globais, mas também as vulnerabilidades de nosso sistema internacional. Consequentemente, teremos que repensar e redefinir cuidadosamente a política internacional e a economia global e, especialmente, a maneira como conduzimos e coordenamos políticas globais para enfrentar desafios globais.

Há um entendimento claro e permanente: ameaças globais, como uma pandemia, os crescentes desafios das mudanças climáticas, mas também ataques e sabotagem no mundo cibernético, assim como outros, não param nas fronteiras. Esses desafios afetam todos os países igualmente e exigem respostas coordenadas para que estas sejam eficientes e eficazes.

É alarmante ver o enfraquecimento sistêmico das instituições internacionais, uma crescente desconfiança em sua integridade e uma tendência a buscar soluções em nível

If we look at the year 2020, it will likely be remembered as a watershed moment for international politics and international cooperation. The COVID pandemic as well as the different policies to cope with its challenges, have not only shown the degrees of connectedness and interdependency of our global economies, but also the vulnerabilities of our international system. Thus, we will have to carefully rethink and redefine international politics and the global economy and especially the way we conduct and coordinate global policies to address global challenges.

One thing has become clear and is here to stay: global threats, such as a pandemic, the increasing challenges of climate change, but also attacks and sabotage in the cyber realm, as well as others do not stop at borders. These challenges affect all countries equally and require coordinated answers to become efficient and effective.

Alarmingly, we have seen a systemic weakening of international institutions, a growing distrust in their integrity as well as a tendency to seek solutions nationally rather than in a multilaterally coordinated

fashion. The wide-led criticism of the World Health Organization which finally resulted in the withdrawal of the U.S., potentially to be followed by a similar Brazilian move, is only the most visible example. In Europe, we self-critically had to witness that the first impetus to confront the Corona-crisis within the EU was also national, by closing borders at least for regular movement of people, separating European citizens from each other, and initiating national crisis responses.

A new, redefined concept of sovereignty in the 21st century must focus on reconciling the reflex to seek seemingly easier, national solutions that cater to the simple demand for easy, tangible answers, with the conviction that only globally coordinated answers can give sustainable solutions to global challenges. What is the role of the nation state in the 21st century multilateralism? What does this mean for national aspirations? What does this mean for international cooperation?

The core question for nation states will be, how to assure the own say within international institutions and decision-making processes and how to preserve the national or regional identity in an increasingly interconnected world.

This is where I would like to draw from the example of the European Union, far from saying that it is perfect (as the reaction to the COVID pandemic has shown). It places high value on the specific cultural, linguistic and societal identity and individuality of its member states. It protects cultural and audiovisual development, it protects denomination of origin and it gives each member state a say – according to the matter in the sense of 'one country – one vote' or in proportional terms according to population or relative economic strength.

Because every country is dependent on the system to a certain extent, it forces member states to forge a consensus on pretty much every policy item, be it finance, distribution of funds, investment in technology or key positions in foreign and security policy. What counts for the EU, also counts for international institutions as a whole: the value of compromise must be appreciated again. If only full victory counts, there will be many more losers. Such systems are dysfunctional.

The constant difficulty is that institutions have to grow with the challenges. We have seen that in full picture at the height of the European migratory crisis in 2015. External factors – such as the difficulty to protect the EU's external borders – culminated with internal factors, such as the dissent over distribution mechanisms. For any future institution it is utmost important to learn to cope with upcoming new challenges.

Taking the example of fighting climate change, the challenge for international consensus on a global scale, or for Latin American-European consensus as a first, important step, will be to reconcile not only different steps of development, but different priorities of 'protecting' vs. 'using'. To speak with a different picture, it also means reconciling 'global public goods' with 'local or national public goods'. A point in case is the Brazilian Amazon treasure. It is the right of the nation state Brazil to use its own territory and resources for the economic benefit of its population. But it also comes with the burden of carrying international responsibility to protect one of the most unique

nacional e não de maneira coordenada multilateralmente. As críticas amplamente direcionadas à Organização Mundial da Saúde, que resultaram na saída dos EUA daquela entidade e que, provavelmente será encadeada por um movimento semelhante por parte do Brasil, são apenas o exemplo mais visível. De maneira autocrítica, na Europa, testemunhamos que o primeiro ímpeto para enfrentar a crise do Corona no interior da UE também foi de caráter nacional com o fechamento das fronteiras pelo menos para a circulação regular de pessoas, separando os cidadãos europeus uns dos outros e implementando respostas nacionais à crise.

Um conceito novo e redefinido de soberania no século XXI deve se concentrar na reconciliação do ímpeto de buscar soluções nacionais aparentemente mais fáceis, que atendem à simples demanda por respostas fáceis e tangíveis, com a convicção de que apenas respostas coordenadas globalmente podem fornecer soluções sustentáveis para os desafios globais. Qual é o papel do Estado-nação no multilateralismo do século XXI? O que isso representa para as aspirações nacionais? O que isso significa para a cooperação internacional?

A questão central para os Estados-nação será: como garantir o próprio ponto de vista dentro das instituições internacionais e nos processos de tomada de decisão e como preservar a identidade nacional ou regional em um mundo cada vez mais interconectado.

É aqui que gostaria de extrair o exemplo da União Europeia, embora esteja longe de ser perfeito (como a reação à pandemia da COVID demonstrou). A UE valoriza a identidade e individualidade cultural, linguística e social específica de seus Estados membros. Ela protege o desenvolvimento cultural e audiovisual, protege a denominação de origem e dá voz a cada Estado membro de acordo com o assunto no sentido de 'um país, um voto' ou em termos proporcionais de acordo com a população ou força econômica relativa.

Como todo país depende, em certa medida, do sistema, os Estados membros se veem obrigados a estabelecer um consenso em praticamente todos os itens de política, estejam relacionados a finanças, distribuição de fundos, investimento em tecnologia ou posições-chave em política externa e de segurança. O que vale para a UE também vale, de modo geral, para as instituições internacionais: o valor do compromisso deve ser apreciado novamente. Se apenas a vitória completa contar, haverá muito mais perdedores. Tais sistemas são disfuncionais.

A dificuldade constante é que as instituições precisam crescer com os desafios. Vimos isso de maneira integral no auge da crise migratória europeia em 2015. Fatores externos - como a dificuldade de proteger as fronteiras externas da UE - culminaram em fatores internos, como a divergência sobre os mecanismos de distribuição. Para qualquer instituição futura, é extremamente importante aprender a lidar com os novos desafios vindouros.

Tomando o exemplo do combate às mudanças climáticas, o desafio do consenso internacional em escala global ou o consenso latino-americano-europeu como primeiro e importante passo será conciliar não apenas diferentes etapas do desenvolvimento, mas diferentes prioridades de 'proteção' vs. 'uso'. Explicando de outro modo, também significa conciliar 'bens públicos globais' com 'bens públicos locais ou nacionais'. Um exemplo é o

and important ecological treasures of the world that provides core public goods for the world: clean air, biodiversity and water resources.

So, what do we conclude from all this?

It is high time to reconsider and reassess the value of international cooperation and of international institutions. Even though some populists seek the future in a more nationalist and deglobalized outlook, reality shows that this will not be possible. Global phenomena, processes, events and trends will not stop at borders. This time has passed. Our welfare, our eagerness to participate in state-of-the-art technology, our news cycle is already too dependent on the connected global village and its value chains. The core task of our decade is to create a "New Deal for International Institutions" and redefine newly and widely accepted rules of the game.

The challenge of this "New Deal for International Institutions" is at least four-fold:

1. The system must newly accommodate great powers or rising powers so that they have an incentive to adhere to the system and contribute to supporting it. This requires prudent steps on our behalf. Because this new multilateralism of the 21st century cannot and must not be arbitrary in its foundation. It must be deeply rooted in the values we share and that make the foundation of the Western value system in its broader, not geographic sense: the respect for the dignity of each individual, the respect for human rights, freedom, equality, democracy and the rule of law. All these values bring the Americas, Europe and key nations of Asia and Africa together: A significant mass of countries that could and would subscribe to a New Deal for International Institutions. On the other hand, it must accommodate the different powers to have a universal reach. Hence, it requires principles-led pragmatism.

2. The system must open a new and convincing cost-benefit-analysis for the powers to make the case that supporting the system and its institutions is in the very own national interest; and that the answers and solutions it provides can be done better in a coordinated, multilateral fashion. This is undoubtedly the case when fighting climate change. But it is also the case when fighting global diseases. It should and will hopefully be the case, distributing global public goods as well as scarce resources according to a fixed and fair set of rules.

3. The "New Deal for International Institutions" should incentivize great powers again to provide global public goods in the national and in the international interest, such as a framework for stability or a capable system of non-violent crisis resolution. It should also provide the backbone for an ambitious and fair global trading scheme.

4. Last but not least – and this is an issue specifically countries from Latin America and Europe will look at -, a new system must include a more timely and adequate measure of representation. The decision-making processes of the Post World War II-Institutions are outdated and need an upgrade – also to prevent the creation of more, at the same time lesser legitimate 'coalitions of the willing' such as the G7, G20 or G77.

tesouro da Amazônia brasileira. É direito do Estado-nação Brasil usar seu próprio território e recursos para o benefício econômico de sua população. Mas há também o ônus de assumir a responsabilidade internacional de proteger um dos tesouros ecológicos mais exclusivos e importantes do mundo e que fornece bens públicos essenciais para todo o planeta: ar puro, biodiversidade e recursos hídricos.

Então, o que podemos concluir de tudo isso?

É chegada a hora de reconsiderar e reavaliar o valor da cooperação internacional e das instituições internacionais. Embora alguns populistas busquem o futuro por uma perspectiva mais nacionalista e desglobalizada, a realidade mostra que isso não será possível. Fenômenos, processos, eventos e tendências globais não se detêm nas fronteiras. Esse tempo já passou. Nosso bem-estar, nosso desejo de desfrutar de tecnologia de ponta, nosso ciclo de notícias já depende muito da aldeia global conectada e de suas cadeias de valor. A principal tarefa da nossa década é criar um "Novo Acordo para Instituições Internacionais" e redefinir novas regras do jogo amplamente aceitas.

O desafio deste "Novo Acordo para Instituições Internacionais" tem quatro pilares:

1. O sistema deve reacomodar grandes potências ou potências emergentes, para incentivá-las a aderir ao sistema e contribuir para apoiá-lo. Isso requer etapas prudentes porque esse novo multilateralismo do século XXI não pode e não deve ser arbitrário em sua fundação. Ele deve estar profundamente enraizado nos valores que compartilhamos e que firmam a base do sistema de valores ocidental em seu sentido mais amplo, e não geográfico: o respeito à dignidade de cada indivíduo, o respeito aos direitos humanos, liberdade, igualdade, democracia e o Estado de Direito. Todos esses valores aproximam as Américas, a Europa e os principais países da Ásia e África: Um conjunto significativo de países que poderiam e iriam assinar um Novo Acordo para Instituições Internacionais. Por outro lado, deve acomodar as diversas potências para ter um alcance universal. Por isso, requer pragmatismo guiado por princípios.

2. Uma análise do custo-benefício deve ser estabelecida de maneira convincente para que as potências defendam que apoiar o sistema e suas instituições é do próprio interesse nacional e que as respostas e soluções que fornece podem ser melhor realizadas de maneira coordenada e multilateral. Este é sem dúvida o caso no combate às mudanças climáticas, mas também no caso do combate a doenças globais. Deveria ser e será o caso na distribuição de bens públicos globais e de recursos escassos, de acordo com um conjunto de regras estabelecido e justo.

3. O "Novo Acordo para Instituições Internacionais" deve, mais uma vez, incentivar as grandes potências a fornecer bens públicos globais no interesse nacional e internacional, como uma estrutura de estabilidade ou um sistema capaz de implementar a resolução não violenta de crises. Deve também fornecer a base para um esquema de comércio global ambicioso e justo.

4. Por último, mas não menos importante - e esta é uma questão que deve ser especificamente abordada pelos países da América Latina e da Europa -, um novo sistema

Such a “New Deal for International Institutions” can only be achieved through international negotiation and cooperation. We need to recalibrate multilateralism in the 21st century. By default – and especially due to power shifts in the past 70 years as well as technological progress – this multilateralism must and will look different to the one of the mid-20th century. But we must make the effort to find this newly negotiated common ground. Otherwise we will run into the danger of a great power competition that is likely to produce many victims among the middle and small powers.

This points directly to the need of an enhanced cooperation between Latin America and Europe (and some countries in Asia, for that matter). Especially Latin America – or more widely, the Americas – and Europe are predetermined to strengthen cooperative international institutions. With the Organization of American States, the Americas look back at a history with the oldest still existing regional institution. Since its inception, the OAS has been promoting and protecting core elements of our societal as well as value system such as democracy, the rule of law and the protection of human rights. Despite differences in the relative size and power of individual nations, such as Brazil or Mexico, the systems have forced nations to work together and find a common consensus.

This also applies to Europe. The European Union has not only been a pivotal provider of peace and stability, but also an unmatched catalyst for economic and social cohesion in a formerly heterogeneous region. And this process has led to an unparalleled system of political consultation and decision making between states. Europe is also constantly calibrating the balance between integration versus institutionalization. This will be another challenge for new institutions to come. The EU has already become a key actor in the world in terms of economic cooperation or the fight against climate change, but it must take an even sounder and more robust role on the global stage in other areas too. This requires even more cohesion and determination.

Bringing these two similar, yet different perspectives and experiences together, can help us find the best blueprint for a multilateralism of the 21st century.

The challenges that await us are already becoming visible: The longer-term results of the pandemic will become even clearer in the next months and years when the full repercussions on weak health systems in developing countries but also the whole economic consequences fully kick in.

In addition, and currently under the threshold of international attention, already existing crises and threats have gained new intensity. A new regional expansion and reordering of IS in parts of the Middle East and North Africa is under way and threatening the bordering countries immediately, as well as adjacent Europe. Equally, terrorist organizations have gained strength across the countries of the Sahel further deteriorating the humanitarian situation.

An outbreak of other diseases, such as Ebola in parts of Africa is putting additional pressure on the health systems and governance structures of already weak states. Let alone the mid- to long-term effect of so many missed vaccinations during the crisis.

deve incluir uma medida de representação mais tempestiva e adequada. Os processos de tomada de decisão das instituições do pós-Segunda Guerra Mundial estão desatualizados e precisam de aprimoramentos - também para impedir a criação de novas ‘coalizões dos dispostos’ menos legítimas, como o G7, G20 ou G77.

Esse “Novo Acordo para Instituições Internacionais” só pode ser alcançado por meio de negociação e cooperação internacionais. Precisamos reajustar o multilateralismo no século XXI. Por princípio - e especialmente devido às mudanças de poder nos últimos 70 anos, bem como ao progresso tecnológico - esse multilateralismo deve ser e será diferente daquele observado em meados do século XX. Mas devemos fazer o esforço para encontrar esses pontos em comum recentemente negociados. Caso contrário, correremos o risco de uma grande competição por poder que provavelmente produzirá muitas vítimas entre as médias e pequenas potências.

Isso aponta diretamente para a necessidade de uma cooperação aprimorada entre a América Latina e a Europa (e alguns países da Ásia). Especialmente a América Latina - ou mais amplamente, as Américas - e a Europa estão predeterminadas a fortalecer instituições internacionais de cooperação. Com a Organização dos Estados Americanos, as Américas evocam uma história com a mais antiga instituição regional ainda existente. Desde a sua criação, a OEA vem promovendo e protegendo elementos essenciais de nosso sistema social e de valores, como a democracia, o Estado de direito e a proteção dos direitos humanos. Apesar das diferenças no tamanho e poder relativo de nações individuais, como Brasil ou México, os sistemas obrigaram as nações a trabalharem juntas e chegarem a um consenso.

Isto também se aplica à Europa. A União Europeia não só tem sido um promotor essencial de paz e estabilidade, mas também um catalisador incomparável para a coesão econômica e social em uma região anteriormente heterogênea. E esse processo levou a um sistema incomparável de consulta política e tomada de decisão entre os Estados. A Europa também está constantemente ajustando o equilíbrio entre integração e institucionalização. Este será outro desafio para as novas instituições que surgirem. A UE já se tornou um ator-chave no mundo em termos de cooperação econômica e de combate às mudanças climáticas, mas deve assumir um papel ainda mais sólido e robusto no cenário global em outras áreas também e isso requer ainda mais coesão e determinação.

Reunir essas duas perspectivas e experiências semelhantes, porém diferentes, pode ajudar-nos a encontrar o melhor plano para um multilateralismo do século XXI.

Os desafios que nos aguardam já estão se tornando visíveis: os resultados da pandemia a longo prazo se tornarão ainda mais claros nos próximos meses e anos quando as repercussões nos fracos sistemas de saúde dos países em desenvolvimento e todas as consequências econômicas ficarem patentes.

Além disso, e atualmente sob a luz da atenção internacional, crises e ameaças já existentes ganharam nova intensidade. Uma nova expansão regional e reordenação do Estado Islâmico (EI) em partes do Oriente Médio e Norte da África está em andamento e representa uma ameaça imediata aos países da região, assim como à Europa adjacente. Igualmente,

In Latin America, the repercussions of the COVID pandemic on health systems, economies, etc. are specifically striking, also because the continent is much more integrated into the global economy than parts of Africa. Venezuela – the weakest of all countries due to the power usurpation of the leading regime and deliberate bleeding of the economy – is yet to confront the whole consequences without a functioning health system. To the detriment of its people, neighboring countries and the rest of the world, the Maduro regime has used the crisis to further tighten its repressive grip on the system.

As a consequence of these various developments, we will likely be seeing new migration flows in different parts of the world, either fleeing from the lack of economic and social prospects in their countries of origin or fleeing from raising instability and suppression. The consequences of migratory flows have already determined the international debate some three, four and five years ago. Countries such as Colombia, Ecuador and Brazil are already carrying heavy burdens. So are Germany and other countries in Europe. We might be confronted with a similar debate, although one might hope, that an international response comes in a more coordinated fashion the next time. The Global Compact for Safe, Orderly and Regular Migration as well as the Global Compact on Refugees have helped to build an international consensus on this very delicate issue and given nation states the tool to address these challenges cooperatively.

These are foreseeable trends and developments. Many more are to be expected or can be predicted. We are witnessing a daily increase in cyberattacks targeting the backbone of essential services in our countries, but increasingly also democratic institutions. This does not only have an impact on the immediate results of elections, but on the legitimacy of democratic institutions in the longer term. New weapon systems are circumventing existing arms control regimes, potentially leading into dangerous new cycles of arms races. And engaging in hybrid warfare by making use of semi-autonomous non-state actors has become a distressing trend not only challenging systems of collective defense, but also the international law of armed conflicts.

One would think that given these myriad challenges, the countries of the world would come closer together and strengthen those institutions that are uniquely legitimate to confront these challenges in a coordinated way, first and foremost the United Nations and its sub-organizations. But the exact opposite is the case. Due to vested own strategic interests, growing antagonism between the most powerful members of the UN Security Council and a general distrust in the institutions, which is also reflected by a decreasing willingness to invest in the UN system by some key actors, the United Nations were forced to keep an unsatisfying role solving such detrimental crises as in Syria, Libya, Yemen, North Korea or Venezuela. They become less able to conduct their very core mission as enshrined in Article 1 of the UN Charter: “to maintain international peace and security”.

Even when nation states agreed to a pretended consensus in the UN Security Council in recent times and subscribed to UNSC resolutions, international actors became much less ashamed to openly breach international law in the perceived certainty, that they will not be sanctioned. This was the case with the efforts to stop fueling the humanitarian crisis in Libya by executing the existing arms embargo, or by enforcing the

as organizações terroristas ganharam força nos países do Sahel, deteriorando ainda mais a situação humanitária.

Surtos de outras doenças, como o Ebola, em partes da África, está pressionando mais os sistemas de saúde e as estruturas de governança dos Estados já fracos. Sem falar no efeito a médio e longo prazo de tantas vacinas não administradas durante a crise.

Na América Latina, os efeitos da pandemia de COVID nos sistemas de saúde, na economia etc. são particularmente impressionantes porque o continente está muito mais integrado à economia global do que partes da África. A Venezuela - o mais fraco de todos os países devido à usurpação de poder pelo regime e ao sangramento deliberado da economia - ainda enfrenta todas as consequências sem um sistema de saúde que funcione. Em detrimento de seu povo, dos países vizinhos e do resto do mundo, o regime de Maduro usou a crise para reforçar ainda mais seu domínio repressivo no sistema.

Como consequência desses vários acontecimentos, provavelmente veremos novos fluxos migratórios em diferentes partes do mundo, seja de pessoas fugindo da falta de perspectivas econômicas e sociais em seus países de origem ou fugindo do aumento da instabilidade e da opressão. As consequências dos fluxos migratórios já determinaram o debate internacional há três, quatro e cinco anos atrás. Países como Colômbia, Equador e Brasil já carregam cargas pesadas. O mesmo acontece com a Alemanha e outros países da Europa. Podemos ser confrontados com um debate semelhante, embora esperemos, que uma resposta internacional venha de maneira mais coordenada da próxima vez. O Pacto Global para Migração Segura, Ordenada e Regular, bem como o Pacto Global sobre Refugiados, ajudaram a construir um consenso internacional sobre esse assunto tão delicado, e deram aos Estados-nação a ferramenta para enfrentar esses desafios de forma cooperativa.

Estas são tendências e acontecimentos previsíveis. Muitos mais são esperados ou podem ser previstos. Estamos testemunhando um aumento diário de ataques cibernéticos que visam os pilares de serviços essenciais em nossos países, mas também, cada vez mais, instituições democráticas. Isso não apenas afeta os resultados imediatos das eleições, mas também a legitimidade das instituições democráticas no longo prazo. Novos sistemas de armamentos estão evitando os regimes de controle de armas existentes, levando, potencialmente, a novos e perigosos ciclos de corridas armamentistas. E envolver-se em guerra híbrida utilizando atores não estatais semiautônomos tornou-se uma tendência assustadora, não apenas por desafiar os sistemas de defesa coletiva, mas também o direito internacional sobre conflitos armados.

Poderíamos pensar que, diante desses inúmeros desafios, os países do mundo se aproximariam e fortaleceriam as instituições que são exclusivamente legitimadas para enfrentar esses desafios de maneira coordenada, principalmente as Nações Unidas e suas sub-organizações. Mas exatamente o oposto é o que ocorre. Devido a interesses estratégicos próprios, crescente antagonismo entre os membros mais poderosos do Conselho de Segurança da ONU e uma desconfiança geral nas instituições, o que também é refletido pela menor disposição de investir no sistema da ONU por alguns atores-chave, as Nações Unidas foram forçadas a manter um papel insatisfatório na solução de crises adversas como na Síria, Líbia, Iêmen, Coréia do Norte ou Venezuela. Tornam-se

prohibition of the use of chemical weapons in the Syrian war. This further erodes trust in the system and gives new ammunition to critical voices.

I use this example very much on purpose because international law used to be a "traditional frontier" for decades. But we are witnessing that this globally accepted frontier becomes less and less relevant. This, too, should distress us because this will in the end affect all of us, especially those "middle powers" that are so predominant both in Latin America and in Europe.

Departing from the zones of war and conflict, there is also an utmost need to restructure international trade. We are all supportive of bilateral and bi-regional agreements that enhance trade and elevate social as well as environmental standards. The EU-Mercosur trade agreement should be ratified the soonest possible, because it would bring a necessary and long-term economic stimulus to recession-prone economies. But the aim must be higher: We should work together to reform the World Trade Organization and enhance rules-based international trade under its umbrella. Together, as Latin American and European countries, we must push those actors who are blocking reform, dodging existing rules or preventing the institution from carrying out its due tasks.

Access to Artificial Intelligence and new types of data management must not become a privilege for the people in some, more affluent countries. And the regulation cannot be done by only some, more affluent countries. When it comes to core technologies and hence core global common goods of the future, everyone should be allowed to have access and have a say when it comes to standards and regulations. We should therefore come together – preferably under the umbrella of the United Nations – to design the new rules of the game.

All these examples lead to the conclusion that multilateralism of the 21st century must be redefined and must find ways to reconcile national as well as global aspirations. This is not an easy task. But it is worth working on it. The past has shown that severe global crises have often led to a push for more integration and more cooperation. That was the case with the UN and the Bretton Woods system post World War II, and it was the case with European integration after the Cold War. We might use the current health crisis and the resulting economic crisis to redefine our global multilateralism and its institutions. The world can become stronger. And it can move closer together again. This will be a generational task. Hence, it can also be a bridge to include the younger generation who will bear the consequences of what we will be designing today. One way or the other. ■

menos capazes de conduzir sua missão central, consagrada no artigo 1o da Carta da ONU: "manter a paz e a segurança internacionais".

Mesmo quando os Estados-nação concordaram com um pretenso consenso no Conselho de Segurança da ONU recentemente e subscreveram as resoluções desse mesmo Conselho, os atores internacionais não se sentiram constrangidos em violar abertamente o direito internacional na certeza percebida de que não seriam punidos. Esse foi o caso dos esforços para parar de alimentar a crise humanitária na Líbia executando o embargo de armas existente ou para impor a proibição do uso de armas químicas na guerra síria. Casos assim diminuem ainda mais a confiança no sistema e dão nova munição a vozes críticas.

Eu uso muito esse exemplo muito porque, por décadas, o direito internacional foi uma "fronteira tradicional". Porém estamos testemunhando que essa fronteira globalmente aceita torna-se cada vez menos relevante. Isso também deveria nos perturbar, pois afetará todos nós, especialmente as "potências médias" que são tão predominantes na América Latina e na Europa.

Deixando de lado um pouco as zonas de guerra e conflito, há também uma necessidade extrema de reestruturar o comércio internacional. Todos apoiamos acordos bilaterais e bi-regionais que melhoram o comércio e elevam os padrões sociais e ambientais. O acordo comercial Mercosul-UE deve ser ratificado o mais rápido possível, pois traria um estímulo econômico necessário e de longo prazo às economias propensas à recessão. O objetivo, no entanto, deve ser maior: devemos trabalhar juntos para reformar a Organização Mundial do Comércio e aprimorar o comércio internacional baseado em regras sob seu escopo. Juntos, como países da América Latina e da Europa, devemos pressionar os atores que estão bloqueando as reformas, esquivando-se das regras existentes ou impedindo a instituição de realizar suas tarefas.

O acesso à inteligência artificial e novos tipos de gerenciamento de dados não devem se tornar um privilégio para as populações de alguns países mais ricos. E a regulamentação não pode ser elaborada apenas por alguns países mais ricos. Quando se trata de tecnologias essenciais e, portanto, bens comuns globais do futuro, todos devem ter acesso e voz com relação às normas e regulamentos. Portanto, devemos nos unir - de preferência sob a égide das Nações Unidas - para elaborar as novas regras do jogo.

Todos esses exemplos nos levam à conclusão de que o multilateralismo do século XXI deve ser redefinido e deve encontrar maneiras de conciliar aspirações nacionais e globais. Não é uma tarefa fácil, mas é uma na qual vale a pena trabalhar. O passado mostrou que graves crises globais muitas vezes resultaram em pressão por mais integração e mais cooperação. Esse foi o caso do sistema das Nações Unidas e de Bretton Woods após a Segunda Guerra Mundial, e foi o caso também da integração europeia após a Guerra Fria. Podemos usar a atual crise da saúde e a resultante crise econômica para redefinir nosso multilateralismo global e suas instituições. O mundo pode se tornar mais forte. E pode se aproximar novamente. Esta será uma tarefa para gerações. Portanto, também pode ser uma ponte para incluir a geração mais jovem que arcará com as consequências do que projetarmos hoje. De um jeito ou de outro. ■

Jackson Schneider

Jackson Schneider é o Presidente da Embraer Defesa & Segurança desde 2014. Ele é formado em Direito pela Universidade de Brasília (UNB) e possui MBA pela Business School São Paulo (BSP). Ele também é membro ativo de diversas organizações sem fins lucrativos, como a Fundação Bienal de São Paulo, a AACD (Associação de Assistência à Criança Deficiente), é membro da Diretoria Executiva do MASP - Museu de Arte de São Paulo Assis Chateaubriand e do Conselho Consultivo do Instituto Serzedello Corrêa do TCU (Tribunal de Contas da União), além de Presidente da Seção Brasileira do Conselho Empresarial do BRICS (CEBRICS).

Jackson Schneider is President of Embraer Defense & Security, as of 2014. He has a law degree from the University of Brasilia (UNB) and MBA from B.S of SP. He is currently Member of Estácio Participações S.A Board of Directors. He is also an active member of various non-profit organizations such as the Biennial Foundation of SP, the AACD (Association to Support Disabled Children), MASP "Art Museum" Executive Board, Advisory Council of Instituto Serzedello Corrêa from TCU (Brazil´s General Accounting Office) and Chair of the Brazilian Chapter of BRICS Business Council (CEBRICS).

Novo mundo, novos desafios, nova indústria!

New World, new challenges, new industry!

Jackson Schneider

Presidente e CEO, Embraer Defesa & Segurança

President and CEO, Embraer Defense & Security

Antes de qualquer reflexão sobre os pontos propostos pela Fundação Konrad Adenauer e o CEBRI, Centro Brasileiro de Relações Internacionais, para a XVII Conferência de Segurança Internacional do Forte de Copacabana, no âmbito do Seminário Novas Fronteiras e Soberania Frente aos Desafios Globais, para o painel Fronteiras Econômicas: a Indústria de Defesa no Mundo Globalizado – pontos estes pensados antes da maior crise mundial de nossa geração – vale perguntar o que significa, ou significará, em perspectiva, um mundo globalizado após a pandemia do Covid-19. E principalmente no contexto da indústria de defesa.

Ele se reapresentará como até há pouco o víamos, com fluxos comerciais e financeiros dinâmicos e internacionais, cadeias de produção globalmente integradas e um trânsito de pessoas e mercadorias sem igual? Ou, como muitos têm especulado, será mais protecionista, com os países resguardando seus mercados e seus empregos, mais ensimesmados, menos integrados? E como se desdobrarão os ainda não totalmente conhecidos efeitos de tendências geopolíticas, aceleradas pela atual crise, nas tomadas de decisão do segmento militar numa revisita dos planejamentos estratégicos?

Before pondering on the items proposed by the Konrad Adenauer Foundation and CEBRI, the Brazilian Center for International Relations, for the XVII Forte de Copacabana International Security Conference, within the scope of the Seminar on New Frontiers and Sovereignty Facing Global Challenges, for the panel Economic Frontiers: The Defense Industry in a Globalized World, - which were considered before the greatest global crisis of our generation - it is worth asking what, in perspective, a globalized world after the Covid-19 pandemic means; And mainly in the context of the defense industry.

Will it be as it was until recently, with dynamic international trade and financial flows, globally integrated production chains and an unprecedented flow of people and goods? Or, as many have speculated, will we see more protectionism, with countries protecting their markets and jobs, being more self-absorbed and less integrated? And how will the effects of geopolitical trends, accelerated by the current crisis, unfold in the decision making of the military segment in a review of strategic plans?

The consolidation and spread of Chinese and American “decoupling”, which today goes well beyond the decision about the new global digital technological platform, may, for example, have important consequences for everything and everyone, both economically and ideologically. Some analysts foresee a new Cold War ahead, disguising the hegemonic dispute between the world’s two main economies.

The phenomenon of Non-States, unconventional wars and insurgent movements, terrorism, nationalism, the connection of organized crime with paramilitary movements, some with political representation, religious radicalism, territorial conflicts, the “Rogue States ” and regional leadership disputes are some of the many sensitive issues that will unfortunately continue present in our daily lives. Perhaps these themes will present themselves with a different dynamic. One that is more socially sensitive, less predictable and with the capacity to cause more damage and more pain, either due to the influence of this new Cold War, or to the new space and cyber weapons.

The effective defense capacity, supported by effective products and solutions, will be the backdrop or spearhead for these challenges of power projection, protection of interests, protection of life and property. No country is master of its destiny or truly sovereign, without the possibility of defending its convictions, its territory and its population. Even if only as an alert when necessary, even if to form more elevated multilateral defense alliances, even if to negotiate in better conditions. And, in order to answer the questions posed by the coordinators of our panel, we must take this into account. Perhaps we will shift from a model that is more open to partnerships, complementing defense solutions and industrial integration, to a more suspicious environment, where countries with the capacity to develop their solutions and defense responses will do so with partnerships that supplement their own ability.

Bearing this in mind, and considering our reality, with which we must effectively be concerned, it seems to me that the suggested topics guide this reflection very well:
a) Is the partnership between the defense industries of Latin America and Europe possible?
b) What is the potential for technology transfer between the private and defense sectors?
c) How to improve the protection of strategic and sensitive data and critical infrastructure such as energy, water and the financial sector?
d) How do countries allocate their resources to the defense industry and multilateral partners?

As the above topics intertwine and influence each other, I will try to discuss their main characteristics, their potentials and their challenges jointly. A myriad of new technologies, new behaviors, new forms of communication, relationships, economic flows and geopolitical positions will have significant effects in various fields of our lives with repercussions not yet fully deciphered. However, their contours have left the speculation sphere and are consolidated as fact. This future will not necessarily be bleak, nor will it be heavenly. It will depend on the decisions made and how much influence we can exert.

This is the context in which we will live in the world, in Latin America and in Brazil. The defense industry, of course, will not be immune to this. In some aspects it may mean

A consolidação e espraiamento do “decoupling” chinês e americano, hoje bem além da decisão da nova plataforma tecnológica digital mundial, por exemplo, poderá ter consequências importantes para tudo e todos, econômica ou ideologicamente. Alguns analistas falam até de uma nova Guerra Fria que se avizinha, disfarce da disputa hegemônica entre as duas principais economias do mundo.

O fenômeno dos Não-Estados , as guerras não convencionais e os movimentos insurgentes, o terrorismo, o nacionalismo, a conexão do crime organizado com movimentos paramilitares, alguns até mesmo com representação política, o radicalismo religioso, os conflitos territoriais, os “Rogue States”, as disputas de liderança regional são alguns dos muitos temas sensíveis que continuarão, infelizmente, presentes no nosso cotidiano. Talvez estes temas se apresentem com outra dinâmica, mais sensível socialmente, menos previsível e com capacidade de causar mais danos, de provocar mais dor, seja pela influência desta nova Guerra Fria, seja pelas novas armas do espaço e cibernéticas. A capacidade efetiva de defesa, amparada em produtos e solução eficazes será o pano de fundo ou a ponta de lança para estes desafios de projeção de poder, de resguardo de interesses, de proteção de vida e propriedades. Nenhum país é senhor de seu destino, verdadeiramente soberano, sem a possibilidade de defender suas convicções, seu território e sua população. Mesmo que apenas como alerta quando necessário, mesmo que para compor de forma mais altiva alianças multilaterais de defesa, mesmo que para negociar em melhores condições. E para responder as indagações apresentadas pelos coordenadores do nosso painel devemos ter isto em conta. Talvez saiamos de um modelo mais aberto a parcerias, complementação de soluções de defesa e integração industrial, para um ambiente mais desconfiado, onde os países que puderem, desenvolverão suas soluções, suas respostas de defesa com parcerias suplementares às suas capacidades de fazer.

Tendo isso em mente, e considerando nossa realidade, com a qual devemos nos preocupar efetivamente, parece-me que os tópicos sugeridos norteiam muito bem esta reflexão:
a) É possível a parceria entre as indústrias de defesa da América Latina e da Europa?
b) Qual o potencial de transferência de tecnologia entre os setores privados e de defesa?
c) Como aprimorar a proteção de dados estratégicos e sensíveis e de infraestruturas críticas como energia, água e setor financeiro?
d) Como os países alocam seus recursos na indústria de defesa e em seus parceiros multilaterais?

Como os tópicos acima se entrelaçam e têm influência entre si, tentarei discorrer conjuntamente sobre suas principais características, seus potenciais e seus desafios. Uma miríade de novas tecnologias, novos comportamentos, novas formas de comunicação, relacionamentos, fluxos econômicos e posicionamentos geopolíticos terá consequências significativas em vários campos de nossas vidas com repercussões ainda não totalmente decifradas, mas cujos contornos já saem da esfera da especulação e se consolidam como fato. Este futuro não será necessariamente sombrio, nem nirvânico. Dependerá das decisões a serem tomadas e de como poderemos influenciá-lo.

E é neste quadro que viveremos no mundo, na América Latina e no Brasil. A indústria de defesa, por óbvio, não estará imune a isto. Em alguns aspectos pode significar alteração no paradigma de colaboração e parcerias estratégicas, como tem ocorrido entre

a change in the paradigm of collaboration and strategic partnerships, as has been the case among countries and industries with common interests in technological development, for example. We can migrate to a new kind of cooperation, with the development of specific responses to local threats, which are more independent and effective.

With few exceptions, Embraer may be the most relevant example. Latin America has been characterized as a region that buys ready-made solutions, some very distant from the reality of local use and others exotic even. Many, after being acquired, quickly become inoperative despite consuming important resources from the region's budgets, whether due to inadequate maintenance, usage capacity that is not consistent with the local reality, poor training or other reasons.

However, I am not going to discuss the reasons for misuse. There are several. Some are clear and others are not. This could and should be different, as countries have similar challenges, characteristics and needs. Synergy in the design, acquisition, maintenance, production and consumption of defense products would be beneficial not only for a country individually, but for the region as a whole. Joint development projects that are already born considering these market's circumstances and taking into account the acquisition price, operating environment, maintenance costs and installed capacity may even, to some extent, promote a "detente" for chauvinistic passions that find it difficult to think and understand the world in the 21st century. I am not talking about a plan as broad as the European claim or promise to build a single Industrial Defense Base, integrating national solutions and aiming to mitigate deficiencies in strategic sectors that still depend on foreign technology and supplies from outside the Community.

But I do think that Latin America has enough critical mass to take steps towards the elaboration of its own military and defense doctrine in a collaborative and integrative manner, using the technological and industrial capacity of key companies in the region to dominate cycles, with local design and manpower, without unbalanced unilateral strategic alignments, whose final consequences are always the well-known refrain "your market for my product"! Partnerships with other countries or regions, including Europe, can and should exist, but they should be complementary, positive and not use institutional weaknesses or personal greed to impose unnecessary and costly solutions. These partnerships, if designed to support the region's progress, will have effects beyond the defense industry's realm. They will be able to promote research and innovation in other areas of knowledge, in other industries, with effective collaboration between the military and the private sectors. This dual effect, which is mature in developed countries, uses the defense industry as the vanguard of cutting-edge research in innovation and science, often with direct procurement of pure technology, even before the final product that will use it has been defined; it is a "commission of technology". Once the solution is mastered, it can also be used in private sector products with the payment of royalties.

These investments in defense innovation have been extremely fruitful in generating benefits for the private sector in several countries, with visible and tangible effects. This can be seen in the training of highly qualified labor originating from military academies or research institutes that work on cutting-edge projects in private companies.

países e indústrias com interesses comuns no desenvolvimento tecnológico por exemplo. Podemos migrar para uma nova espécie de cooperação, com elaboração de respostas próprias para ameaças locais, mais independentes e efetivas.

Salvo poucas exceções, e a Embraer talvez seja o exemplo mais relevante, a América Latina tem se caracterizado como uma região compradora de soluções prontas, algumas muito distantes da realidade de emprego local, outras exóticas até. Muitas, após serem adquiridas, em pouco tempo se tornam inoperantes apesar de consumirem recursos importantes dos orçamentos da região, seja por manutenção inadequada, capacidade de emprego não condizente com a realidade local, treinamento deficiente ou outras razões.

Não vou discorrer, contudo, sobre as motivações dos desperdícios. São várias. Algumas visíveis, outras não. Isto poderia, e deveria, ser diferente, pois os países têm desafios, características e necessidades semelhantes. Sinergia na concepção, aquisição, manutenção, produção e consumo de produtos de defesa, seria benéfico não apenas para um país independentemente, mas para a região como um todo. Projetos conjuntos de desenvolvimento que já nasçam pensando nas circunstâncias desses mercados levando em conta o preço de aquisição, ambiente de operação, custos de manutenção e capacidade instalada podem inclusive, em certa medida, estimular uma "detente" para paixões chauvinistas com dificuldade de pensar e compreender o mundo do século XXI. Não falo de plano tão amplo como a pretensão ou promessa europeia de confecção de Base Industrial de Defesa única, integradora das soluções nacionais e com objetivo de mitigar deficiências em setores estratégicos ainda dependente de tecnologia e suprimentos de fora da Comunidade.

Mas penso, sim, que a América Latina tem massa crítica para dar passos visando a elaboração de doutrina militar própria, de defesa, colaborativa, integradora e que possa, utilizando-se da capacidade tecnológica e industrial de empresas chaves da região, dominar ciclos, com o pensar e o fazer locais, sem alinhamentos estratégicos unilaterais desbalanceados, cujas consequências finais são sempre o conhecido refrão do "teu mercado para o meu produto"! As parcerias com outros países ou regiões, Europa inclusive, podem e devem existir, mas complementares, positivas e não utilizadoras de fraquezas institucionais ou cupidez pessoal para impor soluções não necessárias e custosas. E estas parcerias, se desenhadas para apoiar o progresso da região, terão efeitos além do horizonte da indústria de defesa. Elas poderão estimular pesquisa e inovação em outras áreas de conhecimento, em outras indústrias, com colaboração efetiva entre os setores militares e a iniciativa privada. Este efeito dual, maduro em países desenvolvidos, utiliza a indústria de defesa como vanguarda da pesquisa de ponta em inovação e ciência, muitas vezes com contratação direta de tecnologia pura, mesmo sem ainda se ter a definição do produto final que a utilizará, a "encomenda tecnológica". Uma vez dominada a solução, ela pode também ser usada em produtos do setor privado com o pagamento de "royalties".

Estes investimentos em inovação de defesa têm se mostrado extremamente profícuos na geração de benefícios para o setor privado de vários países, com efeitos visíveis e tangíveis. Isto pode ser presenciado na formação de mão de obra altamente qualificada advinda de institutos de ensino ou de pesquisa militares que atuam em projetos de ponta em empresas privadas. Institutos como ITA e IME, no Brasil são exemplos de

Institutions like ITA (Brazilian Aeronautics Institute of Technology) and IME (Brazilian Military Engineering Institute) in Brazil are examples of successful experiences supporting science and technology. The concept of "Defense House" encouraging national suppliers, also provides local supply chains, multipliers of positive economic effect in the generation of income, jobs, taxes and technology. Added to this is the frequent spin over of knowledge and research in the defense industry as an important source of expertise for the high-tech civil sector with electro-optical applications for inspection services or imaging for diagnostic health as examples.

However, this environment of development, production and conception of new defense technologies is where the sector faces new threats that, until very recently were only seen in science fiction books and the minds of creative film directors. Today, this fiction is reality with the increased use of cyber and space technologies, autonomous applications and artificial intelligence, among others, to attack, threaten, influence, access information from countries, companies and people. What started as a juvenile diatribe decades ago has evolved into private crimes, not all of which are yet typified, and hence to nationwide initiatives. The preparedness of countries, with strengths and efforts for cyber conflicts, is exciting and revolutionary. Hardware is giving way to Software, and the product will, at most, be a platform for solutions without there being perception of its use. And, it is in this "new world", I don't know if brave and admirable or not, that the defense industry must learn, understand and operate. These are new solutions, far beyond the conventional, the traditional ones and, sometimes, distant from the comfort zone of decision makers, whether due to doctrinal training or generational conflict. This challenge can be understood as an opportunity, a "leap frog", as it allows countries, by encouraging their own solutions with complementary and controlled partnerships where necessary, to format their programs for the protection of their critical infrastructures and sensitive data. In addition, it has the potential dual effect of fostering the private environment of the digital economy, of the technology of the future.

However, in order for this to happen, there must be a change in the semantic understanding of what defense means. As long as we continue to understand defense as something related only to the military world, it will not be possible to justify this epistemic step that I explained. It is clear that the military sector is the greatest expression of the national defense environment, but the reality of the world in 2020 and especially of this new reality that awaits us after the pandemic, makes it clear that other sectors are relevant to national defense. This broad understanding of defense makes it possible to perceive that the defense industry is not simply a military industry.

This coordination between public and private sectors, with the definition of integrating companies capable of supporting the State in the implementation of a cyber protection program, should also involve the local Universities and Research Centers, fostering science and encouraging critical thinking for the benefit of the country. In this sense, the correct allocation of government resources is crucial!

Nations define their investment priorities in the defense industries based on their military doctrines and geopolitical strategies based on possible threats or assumptions that are addressed through the Armed Forces and are capable of projecting deterrent

experiências bem-sucedidas de apoio à ciência e à tecnologia. Também o conceito de "Casa de Defesa", com o estímulo a fornecedores nacionais, propicia cadeias de suprimentos locais, multiplicadoras de efeito econômico positivo na geração de renda, empregos, tributos e tecnologia. E acrescente-se a tudo isto o frequente "spin over" de conhecimento e pesquisa da indústria de defesa como importante fonte de "Know How" de conhecimento para o setor civil de alta tecnologia com as aplicações eletro-ópticas para serviços de inspeção ou o imageamento para a saúde diagnóstica como exemplos.

E é neste ambiente de desenvolvimento, produção e concepção de novas tecnologias de defesa que o setor se depara com ameaças novas, até pouco tempo presentes apenas nos livros de ficção científica e na imaginação de criativos diretores de cinema. Esta ficção hoje foi superada pela realidade com uso crescente de tecnologia cibernética e do espaço, aplicação autônoma e inteligência artificial, entre outros, para atacar, ameaçar, influir, acessar informações de países, empresas e pessoas. O que começou como diatribe juvenil, há décadas, evoluiu para crimes privados, nem todos ainda tipificados, e daí para iniciativas de nações. A preparação de países, com forças e esforços para conflitos cibernéticos é instigante e revolucionária. O hardware cedendo espaço para o software, onde o produto será apenas, quando muito, plataforma de soluções sem que tenhamos, muitas vezes, a percepção de seu emprego. E é neste "novo mundo", não sei se admirável, que a indústria de defesa deve compreender e atuar. São novas soluções além, muito além, do convencional, do tradicional, por vezes distantes da zona de conforto dos tomadores de decisão, seja por formação doutrinária, seja por conflito geracional. Este desafio pode ser compreendido como uma oportunidade, um "leap frog", pois propicia que países, através do incentivo a soluções próprias, com parcerias complementares e controladas onde se fizer necessário, possam formatar seus programas de proteção de suas infraestruturas críticas e dados sensíveis. E com o efeito dual potencial de fomentar o ambiente privado de economia digital, de tecnologia do futuro.

Para que isso aconteça, contudo, se faz necessária uma mudança também de compreensão semântica do que significa defesa. Enquanto seguirmos entendendo defesa como algo relativo ao mundo militar somente, não será possível justificar esse passo epistêmico que explicitei. O Ambiente de defesa nacional obviamente tem no setor militar seu vetor de maior expressão, mas a realidade do mundo em 2020 e principalmente deste mundo que nos espera após a pandemia, deixa claro que outros setores são relevantes para defesa nacional. Este entendimento amplo de defesa é que permite compreender que a indústria de defesa não é simplesmente uma indústria militar.

Esta coordenação entre setores públicos e privados, com definição de empresas integradoras capazes de apoiar o Estado na implantação de programa de proteção cibernética deve também ter o envolvimento das Universidades e Centros de Pesquisa locais, fomentando ciência, incentivando massa crítica pensante para benefício do país. Para isso a correta alocação dos recursos do governo é crucial!

As nações definem suas prioridades de investimentos nas indústrias de defesa com base nas suas doutrinas militares e estratégias geopolíticas com eventuais ameaças ou pretensões sendo endereçadas através de Forças Armadas capazes de projetar poder dissuasório ou intimidatório, amparadas em capacidade de emprego pertinente e efetivo. Uma

or intimidating power, supported by pertinent and effective deployment capacity. A local, national defense industry that is strong and has the capacity for cutting-edge technological development represents, in itself, an important and concrete deterrent. As observed, there are several aspects in the doctrine that can be relevant to guide the decision of countries regarding defense investments, from issues related to their economic development to strategic alliances with other nations, search for power projection regionally or globally, external and internal threats including territorial disputes and even guarantee of peace. Responses to the employment of military doctrine are defined based on these factors through national training or importation of means. The threats and challenges that manifest themselves today, however, are not those classically qualified as military, therefore, the understanding of what a defense industry should be must also be broadened.

Many are the advantages of a local industry, not only as a deterrent or cost reduction factor, but also as a stimulator of other economic sectors. And I am not referring to an industry that does not interact with the world in general, either regionally or globally. Although there is a tendency to imagine a less globalized world after the pandemic, it is important that we keep in mind that a nationally isolated industry is not sustainable, mainly because challenges in the defense field are increasingly global and it is no longer possible to develop solutions exclusively on the national level. Leading the development of a defense industry with an international impact, however, is another aspect in which Brazil and the region can and are able to advance, taking into account what has already been built. Developing the capacity to outline regional defense visions and coordinate scientific and technological efforts that lead to the strengthening of the platform of a local defense industry will guarantee its sustainability and international penetration. ■

indústria de defesa local, nacional, forte e com capacidade de desenvolvimento tecnológico de ponta, representa, por si só, um elemento de dissuasão importante e concreto. Como vemos, há vários aspectos na doutrina que podem ser relevantes para direcionar a decisão de países relativamente aos investimentos de defesa, desde relacionados a seu desenvolvimento econômico até alianças estratégicas com outras nações, busca de projeção do poder, regional ou global, ameaças, internas inclusive, disputas territoriais e, até mesmo, garantia da paz. Com base nestes fatores são definidas as respostas de emprego da doutrina militar via capacitação nacional ou importação de meios. As ameaças e desafios que se manifestam hoje, contudo, não são aquelas tipificadas classicamente como militares, portanto, o entendimento do que deve ser uma indústria de defesa deve também ampliar seu horizonte.

E são muitas as vantagens de uma indústria local, não apenas como fator dissuasório ou de redução de custos, mas como estimuladora de outros setores econômicos. E não falo de uma indústria sem interação com o mundo em geral, seja regionalmente, seja globalmente. Ainda que haja uma tendência de se imaginar um mundo menos globalizado após a pandemia, é importante que não esqueçamos que não é sustentável uma indústria nacionalmente isolada. Isso porque os desafios de defesa são cada vez mais globais e não é mais possível o desenvolvimento de soluções com exclusividade nacional. Capitanear o desenvolvimento de uma indústria de defesa com impacto internacional, contudo, é outro aspecto. E nesse ponto o Brasil e a região podem avançar e têm condições de fazê-lo, levando em conta o que já se foi capaz de construir até hoje. Desenvolver capacidade de delinear visões regionais de defesa e coordenar esforços científicos e tecnológicos que conduzam ao fortalecimento de plataforma de uma indústria de defesa local garantirão sua sustentabilidade e penetração internacional. ■

Elena Lazarou

A Dra. Elena Lazarou é analista sênior de política no Serviço de Estudos do Parlamento Europeu (EPRS), onde foca sua pesquisa nos temas de segurança e defesa, governança global, relações transatlânticas e política externa da UE. Antes de ingressar na EPRS, foi professora assistente e chefe do Centro de Relações Internacionais da Fundação Getúlio Vargas (FGV), no Brasil. Em 2008, ela recebeu o título de Ph.D. em Relações Internacionais pela Universidade de Cambridge. Ela foi pesquisadora nas Universidades de Cambridge e de Sheffield e na London School of Economics (LSE). Ela também é membro associado do programa "Os EUA e as Américas" na Chatham House.

Dr. Elena Lazarou is a Senior Policy Analyst in the European Parliamentary Research Service (EPRS), where her research focuses on security and defence, global governance, transatlantic relations and EU foreign policy. Prior to joining EPRS, she was assistant professor and Head of the Center for International Relations of the Getulio Vargas Foundation (FGV), Brazil. She received a Ph.D. in International Relations from the University of Cambridge in 2008. She has held research positions at the University of Cambridge, the University of Sheffield and the London School of Economics (LSE). She is also an Associate Fellow on the "US and Americas" programme at Chatham House.

Segurança, soberania e cooperação internacional em tempos de ameaças transfronteiriças

Security, sovereignty and international cooperation in a time of transborder threats

Elena Lazarou

Membro do Serviço de Estudos do Parlamento Europeu, Bélgica

Member of the European Parliamentary Research Service, Belgium

Durante a última década, se não por mais tempo, especialistas e formuladores de políticas observaram e reconheceram mudanças profundas no ambiente geopolítico. O desenvolvimento da capacidade de previsão, big data e IA forneceu evidências que apontam para novas tendências significativas em economia, tecnologia e em nosso ambiente natural, que estão continuamente redefinindo a forma das relações internacionais, a identidade dos atores internacionais - governamentais e não governamentais -, bem como noções-chave como segurança, cooperação e soberania. Em 2020, a pandemia de Covid-19 serviu, até agora, como o maior exemplo de como as observações e hipóteses sobre um novo ambiente internacional são muito reais e têm forte impacto sobre como o mundo pode lidar com uma crise de segurança (sanitária) global. Também demonstrou, mais uma vez, que, embora no século XXI o Estado-nação continue sendo o principal ator na segurança internacional, algumas das principais ameaças de nosso tempo transcendem as fronteiras tradicionais e só podem ser enfrentadas por meio de cooperação multilateral. Mudanças climáticas,

For the past decade, if not longer, experts and policy makers have been observing and acknowledging profound shifts in the geopolitical environment. The development of foresight capacity, big data and AI have provided evidence which points to significant new trends in economics, technology and in our natural environment which are continuously redefining the shape of international relations, the identity of international – governmental and non-governmental – actors, as well as key notions such as security, cooperation and sovereignty. In 2020, the Covid-19 pandemic has so far served as perhaps the greatest example of how observations and hypotheses regarding a new international environment are very real and have a tremendous impact on how the world can deal with a global (health) security crisis. It has also illustrated, once again, that while in the 21st century the nation state continues to be the principle actor in international security, some of the major threats of our time transcend traditional borders and can only be addressed through

multilateral cooperation. Climate change, cybersecurity and pandemics are some of those global threats that evidence the limitations of fragmented national responses, highlight the relevance of effective multinational organizations as well as the short-sightedness of nationalist exceptionalism when dealing with these issues.

As argued by some of the major foreign policy analysts of our times, while the current perception is that the global pandemic has fundamentally altered the course of the global order, it is more likely that it has merely exacerbated pre-existing trends[1]. Some of the major trends that foresight reports and expert analysis had been pointing to, even ahead of the global pandemic, were the following:

1. New security threats of a transborder nature, notably climate change and cyber warfare, were growing significantly.
2. Multilateral cooperation was weakening, as great power rivalry – notably between China and the US – was reemerging.
3. Multilateral structures had not adequately adapted to address the new transborder threats of our times.
4. The perceived insufficient provision of public goods, such as security and welfare, by the establishment was gradually linking to popular discontent that fed resurgent nationalism and boosted populist movements.
5. The growth of connectivity and technology in all its forms meant that transactions, relationships and cross border flows of various nature were defining the global order increasingly more than institutions and rules.
6. Technological progress could also be used as a weapon in various types of modern warfare be it through the recruitment of terrorists, lethal operations, or operations to destabilise democracy and its structures via disinformation, mass surveillance and election meddling.
7. Trade and material/resource dependencies could also potentially be weaponised in the context of emerging power competition and the resurgence of realist international politics.
8. In the context of globalization and interconnectivity, local governance actors were increasingly assuming a great role in areas such as climate policy, digital policy and even security.
9. The causes and consequences of traditional threats such as interstate wars, violent conflict, state fragility and economic crises were being fundamentally altered by all of the above requiring rethinking and adaptation of established approaches and solutions[2].

1 Haass, R. (2020) The Pandemic Will Accelerate History Rather Than Reshape It. Not Every Crisis Is a Turning Point, Foreign Affairs, April 7, 2020.

2 ESPAS (2019), Global Trends to 2030: Challenges and choices for Europe; Lazarou, E., The ESPAS analysis so far, unpublished note, EPRS, December 2019.

cibersegurança e pandemias são algumas das ameaças globais que evidenciam as limitações de respostas nacionais fragmentadas, destacam a relevância de organizações multinacionais eficazes, bem como a falta de visão do excepcionalismo nacionalista ao lidar com essas questões.

Alguns dos principais analistas de política externa contemporâneos têm afirmado que, embora a percepção atual seja de que a pandemia global alterou fundamentalmente o curso da ordem global, é mais provável que tenha apenas exacerbado tendências pré-existentes[1]. Algumas das principais tendências apontadas pelos relatórios prospectivos e pelas análises de especialistas, mesmo antes da pandemia global, são as seguintes:

1. Novas ameaças à segurança de natureza transfronteiriça, notadamente as mudanças climáticas e a guerra cibernética, estavam crescendo significativamente.
2. A cooperação multilateral estava enfraquecendo à medida em que a grande rivalidade entre potências - principalmente entre a China e os EUA - estava ressurgindo.
3. As estruturas multilaterais não estavam adequadamente adaptadas para enfrentar as novas ameaças transfronteiriças de nossos tempos.
4. O fornecimento insuficiente de bens públicos, como segurança e bem-estar, pelos poderes estabelecidos foi gradualmente vinculado ao descontentamento popular que alimentou o ressurgimento do nacionalismo e impulsionou os movimentos populistas.
5. O crescimento da conectividade e da tecnologia em todas as suas formas mostrou que transações, relacionamentos e fluxos transfronteiriços de várias naturezas estavam, cada vez mais, definindo a ordem global em detrimento de instituições e normas.
6. O progresso tecnológico também pode ser usado como arma em vários tipos de guerra moderna, seja através do recrutamento de terroristas, operações letais ou operações para desestabilizar a democracia e suas estruturas através da desinformação, vigilância em massa e interferência em eleições.
7. As dependências comerciais e de materiais/recursos também poderiam potencialmente ser usadas como armas no contexto da emergente competição entre as potências e do ressurgimento da política internacional realista.
8. No contexto da globalização e interconectividade, os atores da governança local estavam assumindo cada vez mais um papel fundamental em áreas como política climática, política digital e até segurança.
9. As causas e consequências de ameaças tradicionais, como guerras entre Estados, conflitos violentos, fragilidade do Estado e crises econômicas, foram fundamentalmente alteradas por todas as tendências anteriores, exigindo repensar e adaptar as abordagens e soluções estabelecidas[2].

1 Haass, R. (2020) The Pandemic Will Accelerate History Rather Than Reshape It. Not Every Crisis Is a Turning Point, Foreign Affairs, April 7, 2020.

2 ESPAS (2019), Global Trends to 2030: Challenges and choices for Europe; Lazarou, E., The ESPAS analysis so far, unpublished note, EPRS, December 2019.

These trends, compounded by the COVID 19 crisis, clearly indicate a new security environment, more "global" in its challenges than ever before. At the same time, political and social trends have brought to power governments which base their rhetoric on a "nation state first" approach and "othering" the international society, hampering support and trust in solutions and policies with a globally encompassing reach. In this context the challenge for policy makers resembles an extremely complex riddle: it involves simultaneously creating a renewed push for effective multilateralism, while ensuring that strategic elements of sovereignty remain in place to minimize dependency risks as well as public skepticism towards cosmopolitanism.

Climate change and geopolitics: the undisputed evidence of the need for global cooperation

Climate change serves as the most striking example of how challenges that transcend national borders are fundamentally altering geopolitics. In 2018 the United Nations Intergovernmental Panel on Climate Change (IPCC), alarmingly reported the detrimental impacts of global warming of 1.5 °C. The related risk would, for example, include a significant increase of poverty in Africa and Asia, and consequently global inequality. Global warming will likely bring risks to energy, food and water security and generate extreme weather events and natural hazards that will affect large numbers of people and entire populations. Coastal areas and desert areas will suffer enormous consequences for their socioeconomic activities. In turn, this may - and will by many accounts – translate into an increased likelihood of conflict in fragile regions, significant population movements with internal and international migration (and climate refugees). According to the Internal Displacement Monitoring Center (IDMC), since 2008, events referred to as natural hazards – many of them linked to climate change - have forcibly displaced approximately 265 million people, amounting to more than three times as many forced movements as those caused by conflict and violence. The security risks related to climate and the deterioration of quality of life could, in a vicious cycle, also be used to the benefit of authoritarian and ultra-nationalist propaganda at the detriment of democracy, as fear further guides affected populations to extreme political beliefs, in search for answers[3].

Much like climate change, many of the transborder/global risks identified in today's environment act as risk multipliers, as they not only pose a threat in themselves, but also aggravate additional threats – be they economic, geopolitical or sociopolitical. Much like climate change, the coronavirus pandemic has not only threatened public health worldwide, but also created further disruption through its negative impact on economies (including rising unemployment), the disruption of global trade, its impact on access to essential goods (including food and water in some places). These global threats, when combined with the widespread use of disinformation and propaganda, are often weaponized in ways that compromise democracy and privacy.

3 Lazarou, Elena (2020), EU Peace and Security Outlook 2020, European Parliamentary Research Service.

Essas tendências, agravadas pela crise da COVID 19, indicam claramente um novo ambiente de segurança, mais "global" do que nunca em seus desafios. Ao mesmo tempo, tendências políticas e sociais trouxeram ao poder governos que baseiam sua retórica em uma abordagem de "Estado-nação em primeiro lugar" e "marginalizando" a sociedade internacional, dificultando o apoio e a confiança em soluções e políticas com alcance global. Nesse contexto, o desafio para os formuladores de políticas se assemelha a um enigma extremamente complexo: envolve simultaneamente a criação de um impulso renovado pelo multilateralismo eficaz, garantindo ao mesmo tempo a manutenção de elementos estratégicos de soberania para minimizar os riscos de dependência e o ceticismo público em relação ao cosmopolitismo.

Mudança climática e geopolítica: a evidente e indiscutível necessidade de cooperação global

A mudança climática serve como o exemplo mais impressionante de como os desafios que transcendem as fronteiras nacionais estão alterando fundamentalmente a geopolítica. Em 2018, o Painel Intergovernamental sobre Mudanças Climáticas das Nações Unidas (IPCC) relatou sobre os alarmantes impactos negativos do aquecimento global de 1,5°C. O risco incluiria, por exemplo, um aumento significativo da pobreza na África e na Ásia e, consequentemente, aumento da desigualdade global. O aquecimento global provavelmente trará riscos à segurança energética, alimentar e hídrica e gerará eventos climáticos extremos e riscos naturais que afetarão um grande número de pessoas e populações inteiras. As áreas costeiras e desérticas sofrerão enormes efeitos em suas atividades socioeconômicas. Por sua vez, isso pode - e de acordo com muitos relatos irá - se tradir em uma maior probabilidade de conflito em regiões frágeis, movimentos populacionais significativos com migração interna e internacional (e refugiados climáticos). De acordo com o Centro de Monitoramento de Deslocamento Interno (IDMC), desde 2008, eventos chamados de riscos naturais - muitos deles relacionados à mudança climática - deslocaram à força aproximadamente 265 milhões de pessoas, perfazendo mais de três vezes o número de movimentos forçados causados por conflito e violência. Os riscos de segurança relacionados ao clima e a deterioração da qualidade de vida podem, em um ciclo vicioso, também ser usados em benefício da propaganda autoritária e ultranacionalista em detrimento da democracia, pois o medo guiaria as populações afetadas em direção a crenças políticas extremas em busca de respostas[3].

Assim como as mudanças climáticas, muitos dos riscos transfronteiriços/globais identificados no ambiente atual atuam como multiplicadores de riscos, pois não apenas representam uma ameaça em si, mas também agravam ameaças adicionais - sejam econômicas, geopolíticas ou sociopolíticas. Assim como a mudança climática, a pandemia do novo coronavírus não apenas ameaça a saúde pública em todo o mundo, mas também criou novas perturbações devido ao seu impacto negativo nas economias (incluindo o aumento do desemprego), a interrupção do comércio global, o impacto no acesso a bens essenciais (incluindo comida e água em alguns lugares). Essas ameaças globais, quando combinadas com o amplo uso de desinformação e propaganda, são geralmente usadas como armas de maneira que comprometem a democracia e a privacidade.

3 Lazarou, Elena (2020), EU Peace and Security Outlook 2020, European Parliamentary Research Service.

Looking ahead: multilateralism, strategic sovereignty and new partnerships?

Undoubtedly, the extent and reach of global threats is such that national solutions are impossible. Yet, multilateralism, perhaps the only instrument which offers credible prospects of global mechanisms to address transborder threats, is undergoing an existential crisis of faith. This crisis is epitomized by the rise of support for far-right nationalist populism, protectionism and by the declining trust among states, including among traditional allies. While discourse in that vein emphasizes the reinstatement of traditional borders in every sense, the multilateral system was conceived precisely as a model where sovereign states work together to address those issues that expand beyond them. As outlined above, the nature of today's world is such, that compared to a century ago, a large majority of policy issues, including the mitigation of security threats, cease to be contained in the space of traditional borders. The answer should, thus, be more multilateralism.

And yet, for multilateralism to survive, it must adapt and serve the complex international environment we live in. In this vein, actors which support the rules based order, multilateral cooperation and international law should reinforce their effort to work with likeminded partners, but also to construct pragmatic, efficient and appropriate responses together with others. It is also important that they take into account the recalibration of the balance of power; the political dynamics of major powers and their inclination to contribute to a reinforcement of international cooperation – or not.

In this context, the European Union's current recalibration of its foreign policy is interesting to follow. In the first (2020) work programmed of the Von der Leyen Commission, the European Commission stated "Europe will always be committed to upholding, updating and upgrading the rules-based global order to ensure it is fit for today's world. At the same time, Europe needs to be more geopolitical, more united and more effective in the way that it thinks and acts. It needs to invest in alliances and coalitions to advance our values, promote and protect Europe's interests through open and fair trade and strengthen the links between our internal and external policies"[4]. In essence, three interlinked elements are highlighted in this document: the defence of multilateralism, the focus on a geopolitical approach to the world and the construction of targeted partnerships and alliances. The advancement of the EU's values and its interests underpin this triptych.

This approach to EU foreign policy – which some have characterized as a more pragmatic approach – could be viewed as a response to the aforementioned challenge of need to bridge the gap between challenges that transcend traditional borders, without undermining the realities of an environment of growing skepticism towards post-nationalism and a turn of the public opinion towards the support for nationalist populism. As stated by the European Parliament, "the EU's security environment is vulnerable

4 European Commission (2020), Commission Work Programme 2020: A Union that Strives for More, Brussels.

Visão para o futuro: multilateralismo, soberania estratégica e novas parcerias?

Sem dúvida, a extensão e o alcance das ameaças globais são tais que soluções nacionais são impossíveis. No entanto, o multilateralismo, talvez o único instrumento que oferece perspectivas plausíveis de mecanismos globais para enfrentar ameaças transfronteiriças, está passando por uma crise existencial de confiança. Esta crise é sintetizada pelo aumento do apoio ao populismo nacionalista de extrema-direita, do protecionismo e pela queda de confiança entre os Estados, inclusive entre aliados tradicionais. Enquanto o discurso nesse sentido enfatiza o restabelecimento das fronteiras tradicionais em todos os sentidos, o sistema multilateral foi concebido precisamente como um modelo no qual os Estados soberanos trabalham juntos para tratar das questões que transcendem fronteiras. Conforme descrito acima, a natureza do mundo de hoje é tal que, comparada a um século atrás, uma grande maioria de questões políticas, incluindo a mitigação de ameaças à segurança, deixa de estar contida no espaço das fronteiras tradicionais. A resposta deve, portanto, ser mais multilateralismo.

E, no entanto, para que o multilateralismo sobreviva, ele deve se adaptar e atender ao complexo ambiente internacional em que vivemos. Nesse sentido, os atores que apoiam a ordem baseada em regras, a cooperação multilateral e o direito internacional devem reforçar seus esforços para trabalhar com parceiros semelhantes, mas também construir respostas pragmáticas, eficientes e apropriadas coletivamente. Também é importante que eles levem em conta os ajustes do equilíbrio de poder; a dinâmica política das grandes potências e sua inclinação para contribuir para o reforço da cooperação internacional - ou não.

Nesse contexto, é interessante seguir o reajuste atual da política externa da União Europeia. No primeiro trabalho (2020) programado pela Comissão Von der Leyen, a Comissão Europeia declarou que "a Europa estará sempre comprometida em manter, atualizar e modernizar a ordem global baseada em regras para garantir que seja adequada ao mundo de hoje. Ao mesmo tempo, a Europa precisa ser mais geopolítica, mais unida e mais eficaz na maneira como pensa e age. É necessário investir em alianças e coalizões para promover nossos valores, promover e proteger os interesses da Europa por meio do comércio aberto e justo e fortalecer os vínculos entre nossas políticas internas e externas" [4]. Em essência, três elementos interligados são destacados neste documento: a defesa do multilateralismo, o foco em uma abordagem geopolítica do mundo e a construção de parcerias e alianças focadas. O avanço dos valores da UE e seus interesses sustentam este tríptico.

Esta abordagem da política externa da UE - que alguns caracterizaram como uma abordagem mais pragmática - poderia ser vista como uma resposta ao desafio mencionado acima da necessidade de preencher a lacuna entre os desafios que transcendem as fronteiras tradicionais, sem comprometer a realidade de um ambiente de crescente ceticismo em relação ao pós-nacionalismo e um retorno do apoio da opinião pública ao populismo nacionalista. Como afirma o Parlamento Europeu, "o ambiente de segurança da UE

4 European Commission (2020), Commission Work Programme 2020: A Union that Strives for More, Brussels.

to external pressure that prevents the EU from exercising its sovereignty"[5], but the exercise of sovereignty should not contradict but complement international cooperation.

These debates have given rise to the concept of strategic sovereignty, which, in the current environment encompasses a wide range of fields where an actor should be able to act autonomously – ranging from military, to technological and financial. As international actors increasingly fuse economic activity with political and security competition, the hybrid nature of competition reconstructs traditional notions of power and, subsequently, sovereignty. In that context, sovereignty is less about borders, than it is about actorness.

Looking to the future, the pursuit of strategic sovereignty together with multilateralism, may include:

1. Renewed focus on the creation of the multilateral governance in areas such as biodiversity, migration and artificial intelligence;
2. Support for the UN and key multilateral organisations through the 'crisis of multilateralism';
3. Progressing in the reform of the WTO;
4. Upholding multilateral decisions with own laws (such as in the case of the blockage of the Appellate Body of the WTO, or upholding the Paris Agreement through the European Green Deal);
5. Building autonomy in technology and critical equipment;
6. Working with like-minded partners in traditional and new formats;
7. Ensuring effectiveness and accountability of international policies/agreements for the mitigation of global security threats (e.g. accountability of the WHO; state accountability and transparent reporting on the implementation of commitments to the Paris Agreement);

The Covid-19 pandemic has been an eye opener, not only in terms of its global nature, but also as an indicator of the need for more strategic preparedness. Some of the major security challenges of our times, including climate change and global warming, can only be solved through scientific capacity for foresight and anticipation. The capacity to think and prepare for the future can helps states and other actors to navigate, adapt, and shape the future through better policies. International collaboration in the analysis of global trends, and their potential impact, should be a part of global governance if challenges, which extend far beyond traditional borders, are to be tackled today and in the future[6]. ■

5 European Parliament (2020), Resolution of 15 January 2020 on the implementation of the common foreign and security policy – annual report.

6 This section has drawn on the author's unpublished paper 'Promoting the EU's Values and Interests', prepared for the European Parliament's Management Innovation Day, January 2020.

é vulnerável a pressões externas que impedem a UE de exercer sua soberania"[5], mas o exercício da soberania não deve contradizer e sim complementar a cooperação internacional.

Esses debates deram origem ao conceito de soberania estratégica, que, no ambiente atual, abrange uma ampla gama de áreas em que um ator deve ser capaz de agir autonomamente - desde a área militar, até tecnológica e financeira. À medida que os atores internacionais fundem cada vez mais a atividade econômica com a competição política e de segurança, a natureza híbrida da competição reconstrói as noções tradicionais de poder e, subsequentemente, de soberania. Nesse contexto, a soberania tem menos a ver com fronteiras do que com a falta de ação.

Vislumbrando o futuro, a busca pela soberania estratégica em associação ao multilateralismo, pode incluir:

- Foco renovado na criação de governança multilateral em áreas como biodiversidade, migração e inteligência artificial;
- Apoio à ONU e às principais organizações multilaterais durante a 'crise do multilateralismo';
- Avançar na reforma da OMC;
- Apoio a decisões multilaterais com leis próprias (como no caso do bloqueio do Órgão de Apelação da OMC ou reforço do Acordo de Paris por meio do Acordo Verde Europeu);
- Desenvolvimento de autonomia em tecnologia e equipamento crítico;
- Cooperação e trabalho com parceiros de mentalidade similar em formatos tradicionais e novos;
- Garantia da eficácia e da responsabilidade das políticas/acordos internacionais para a mitigação das ameaças à segurança global (por exemplo, responsabilização da OMS; responsabilização do Estado e relatórios transparentes sobre a implementação dos compromissos do Acordo de Paris);

A pandemia de Covid-19 tem sido surpreendente, não apenas em termos de sua natureza global, mas também como um indicador da necessidade de mais preparação estratégica. Alguns dos principais desafios de segurança de nossos dias, incluindo as mudanças climáticas e o aquecimento global, só podem ser resolvidos por meio da capacidade científica de previsão e antecipação. A capacidade de pensar e se preparar para o futuro pode ajudar os Estados e outros atores a navegar, adaptar e moldar o futuro por meio de políticas melhores. A colaboração internacional na análise de tendências globais e seu potencial impacto deve fazer parte da governança global para que os desafios, que se estendem muito além das fronteiras tradicionais, sejam enfrentados hoje e no futuro[6]. ■

5 European Parliament (2020), Resolution of 15 January 2020 on the implementation of the common foreign and security policy – annual report.

6 Esta seção foi baseada no artigo não publicado pela autora 'Promoting the EU's Values and Interests', escrito para o Dia de Inovação em gestão do Parlamento Europeu (the European Parliament's Management Innovation Day), Janeiro 2020.

Daniel Flemes

O Dr. Daniel Flemes é Pesquisador Sênior do Instituto GIGA de Estudos Latino-Americanos em Hamburgo e editor do GIGA Focus América Latina. Ele atuou como pesquisador visitante na Universidade de Georgetown, na Universidade da Cidade do Cabo e na Fundação Getúlio Vargas. Seus livros sobre deslocamentos de poder no sistema internacional foram publicados por editoras de renome internacional, como Ashgate e Palgrave Macmillan. Daniel Flemes publicou várias dezenas de artigos sobre a política externa, de segurança e de defesa de países latino-americanos em revistas especializadas como Third World Quarterly, International Politics, Bulletin of Latin American Research, e Foreign Affairs Latinoamérica. Ele dedica especial interesse ao desenvolvimento político, social e econômico do Brasil. Atualmente ele está pesquisando a política amazônica de países sul-americanos.

Dr. Daniel Flemes is a Senior Research Fellow at the GIGA Institute of Latin American Studies in Hamburg and editor of the GIGA Focus Latin America. He has worked as a visiting scholar at Georgetown University, the University of Cape Town and the Getúlio Vargas Foundation. His books on power shifts in the international system have been published by internationally renowned publishers such as Ashgate and Palgrave Macmillan. Daniel Flemes has published several dozen articles on the foreign, security, and defence policies of Latin American countries in journals such as Third World Quarterly, International Politics, Bulletin of Latin American Research, and Foreign Affairs Latinoamérica. He is particularly interested in Brazil's political, social and economic development. Currently he is researching the Amazon policy of South American states.

Os militares brasileiros como guardiões da Amazônia

Brazil's military as guardian of the Amazon

Daniel Flemes

Pesquisador Sênior do Instituto GIGA de Estudos Latino-Americanos em Hamburgo

Senior Research Fellow at the GIGA Institute of Latin American Studies in Hamburg

Introdução

A influência política dos generais no Brasil tem aumentado fortemente nos últimos tempos. Seja no interior do governo, com militares na ativa ou ex-militares nos cargos de presidente, vice-presidente e ministros; ou sejam as Forças Armadas como instituição nacional e ator social, que desfruta consistentemente de mais confiança entre a população do que instituições políticas como o parlamento e os partidos. É de especial importância o papel das Forças Armadas na Amazônia. Por um lado, o Exército é muitas vezes o único ator que assegura a presença do Estado nessa área de difícil acesso. Por outro lado, os generais sempre se viram como guardiões da soberania nacional e da integridade territorial.

Essa função de guardião não se limita à defesa contra possíveis intervenções de forças estrangeiras, mas há muito tempo inclui também funções policiais (por exemplo, o combate ao tráfico de drogas e de armas), questões energéticas e ambientais (prevenção da exploração ilegal dos recursos naturais), assim como a administração de conflitos entre povos indígenas e atores que exploram o bioma economicamente.

Introduction

The political influence of the generals in Brazil has increased considerably in recent times. Be it within the government, with active or former military personnel as president, vice president and ministers; or be it the armed forces as a national institution and social actor, which consistently enjoys more trust among the population than political institutions such as the parliament and the parties. The military is of particular importance in the Amazon. For one thing, the army is often the only guarantor of state presence in this area of difficult access. On the other hand, the generals have always seen themselves as guardians of national sovereignty and territorial integrity.

This role as guardian is not limited to defence against potential intervention by foreign forces, but has long since included police tasks (e.g. combating drug and arms trafficking), energy and environmental issues (preventing illegal exploitation of natural resources), and dealing with conflicts between indigenous peoples and actors who exploit the biome economically. Illegal resource extraction in particular is often associated with human rights violations against indigenous actors.

In view of these developments, the question that arises is related to the degree of influence of Brazil's generals in the Amazon region in the areas of a) security and defence, b) economic development, and c) environmental and indigenous protection. The aim is to analyse the weight of military decision-makers in comparison with civilian members of the Bolsonaro cabinet with regard to the Amazon policy. This is followed by an assessment of the defence policy and military (academic) cooperation potential between Germany, the EU and Brazil.

The domain of the military: security and defence

The spectrum of security policy challenges in the Amazon region has become more comprehensive and complex in recent years, and the threats themselves less visible and predictable. Interstate conflicts over territorial claims and border demarcations have largely been resolved. The governments of South America agree that the cross-border, non-military threats must be regarded as the real security policy challenge in the region. Drugs and arms trafficking as forms of organised crime have long been common in the region. What is new is their increasing transnationalization. Links of Colombian guerrilla groups and drug gangs to Venezuela and Brazil are just one example of this trend.

Transnational money laundering is one of the many interfaces between different forms of organised crime. The problem acquires a regional dimension when transnational, lawless spaces are created as a result of eroding monopolies of violence, as is the case in the tri-border area between Brazil, Colombia and Venezuela. Criminal gangs are primarily responsible for the precarious security situation in the Amazon region. However, the national police and judicial systems, due to rampant corruption and links to organised crime, are more part of the security problem than help solve it. The dysfunctionality of the police institutions encourages the use of the military in tasks ranging from crime fighting to intelligence gathering about social actors such as non-governmental organisations (NGOs) and indigenous peoples, who, in the view of many generals, are pursuing the "denationalisation" of the Brazilian Amazon.

For instance, the Minister of Institutional Security (GSI) and doyen of the military in Bolsonaro's cabinet, General Augusto Heleno, criticized the demarcation of the indigenous land *Raposa Serra do Sol* in the state of Roraima on the Brazilian border with Venezuela and Guyana, considering it an internal threat to Brazil's sovereignty. Some of the NGOs operating in the Amazon region support indigenous peoples; others fight for biodiversity and are, therefore, associated with biopiracy by the former commander of the Amazon Command. Both groups would, therefore, contribute to the undermining of territorial integrity. The role of the military in domestic politics, which is unusual in democratic systems, is guaranteed by the Constitution in Brazil. The central constitutional enclave is Article 142 (*Garantia da Lei e da Ordem - GLO*), which assigns to the armed forces the role of guardians of the domestic order.

The generals see the territorial integrity of the Brazilian Amazon threatened not only by NGOs and indigenous peoples, but also by the Amazon Synod initiated by Pope

A extração ilegal de recursos, em particular, está frequentemente associada à violação de direitos humanos de integrantes dos povos indígenas.

Em vista dessa evolução, surge a questão de qual é a influência dos generais brasileiros na região amazônica nas áreas de a) segurança e defesa, b) desenvolvimento econômico e, c) proteção ambiental e dos atores indígenas. O objetivo é analisar o peso dos militares como tomadores de decisões em comparação com os integrantes civis do governo Bolsonaro no campo da política relativa à Amazônia. Na seção final apresenta-se uma avaliação do potencial de cooperação nas áreas de política de defesa e militar (acadêmica) entre Alemanha e UE e o Brasil.

O domínio das Forças Armadas: segurança e defesa

O escopo dos desafios da política de segurança na região amazônica tornou-se mais abrangente e complexo nos últimos anos, e as próprias ameaças menos visíveis e previsíveis. Os conflitos entre países quanto a reivindicações territoriais e demarcações de fronteiras foram, em grande parte, resolvidos. Os governos da América do Sul concordam que as ameaças transfronteiriças, não militares, devem ser consideradas como o verdadeiro desafio da política de segurança enfrentado na região. O tráfico de drogas e de armas como formas do crime organizado são comuns há muito tempo na região. O que é novo é sua crescente transnacionalização. Ligações de grupos guerrilheiros colombianos e gangues de drogas com a Venezuela e o Brasil são apenas um exemplo dessa tendência.

A lavagem transnacional de dinheiro é uma das muitas interfaces entre as diferentes formas do crime organizado. Essa problemática adquire uma dimensão regional quando, como resultado da erosão dos monopólios de violência, criam-se espaços transnacionais, sem lei, como é o caso do triângulo fronteiriço entre Brasil, Colômbia e Venezuela. As organizações criminosas são as principais responsáveis pela precária situação de segurança na região amazônica. No entanto, diante da corrupção desenfreada e as ligações com o crime organizado, os sistemas policiais e judiciais nacionais tornam-se mais parte do problema de segurança do que ajudam a resolvê-lo. A disfuncionalidade das instituições policiais incentiva o uso dos militares em tarefas que vão do combate ao crime até a coleta de informações de inteligência sobre atores sociais como organizações não-governamentais (ONGs) e povos indígenas, que, na opinião de muitos generais, estão promovendo a "desnacionalização" da Amazônia brasileira.

O Ministro de Segurança Institucional (GSI) e decano dos militares no governo Bolsonaro, General Augusto Heleno, criticou, por exemplo, a demarcação do território indígena Raposa Serra do Sol no estado de Roraima, na fronteira com a Venezuela e a Guiana, como uma ameaça interna à soberania do Brasil. Algumas das ONGs que operam na região amazônica apoiam os povos indígenas, outras lutam pela biodiversidade e, em razão disso, estão sendo associadas à biopirataria pelo ex-comandante do Comando da Amazônia. Ambos os grupos, portanto, estariam contribuindo para o comprometimento da integridade territorial. O papel dos militares na política interna, que é incomum em sistemas democráticos, é garantido constitucionalmente no Brasil. A âncora constitucional central é o Artigo 142 (Garantia da Lei e da Ordem - GLO), que atribui às Forças Armadas uma função de guardiãs da ordem interna.

Francis. First and foremost, they fear an asymmetric conflict with Colombian guerrilla organisations, which are presumably supported by the Maduro regime in Venezuela. The internal conflicts in Venezuela and Colombia could be carried into Brazil by uncontrolled migration movements. The greatest threat to national sovereignty as regarded by military government circles is China's foreign economic policy, especially since it focuses on Africa, a region rich in raw materials, and finds compliant agents in Cuba and neighbouring Venezuela who are willing to carry out its policies. The generals see the resource-rich Amazon region threatened by Chinese investments, land purchases and migrants from neighbouring countries, which would act as Beijing's fifth column.

As a reaction to the complex security situation, the national defence strategy is based on the premise that first and foremost the military deterrent capability must be maintained and expanded. In order to achieve this goal, Defence Minister General Azevedo e Silva has announced a redisposition, structural reform and the modernisation and armament of the military apparatus. Redistribution essentially involves the relocation of units from the Atlantic coast to the Amazonian borders in the country's north and west. Additionally, the structural reform aims to increase mobility so that troops stationed in other parts of the country can be relocated to the Amazon region at short notice if necessary. In recent years, some 27,000 soldiers have been transferred to the Amazon region. Said units were primarily stationed on the borders with Venezuela, Surinam, Colombia, Peru and Bolivia. To this end, 23 new border posts have been set up along the Amazon border.

Armed Forces and economic development of the Amazon region

The objectives of the Bolsonaro administration's economic policy in the Amazon region are expressed in the *Rio Branco* project. The government programme for the development of the Amazon region is currently being prepared by the Secretariat for Strategic Affairs (SAE) of the President's Office under the responsibility of Admiral Flávio Rocha. Government incentives are intended to attract large companies to the Amazon region, which in turn will attract non-indigenous Brazilians from other parts of the country and thus make a significant contribution to increasing economic growth.

In order for the military dictatorship's old dream of non-indigenous settlements in the Amazon region to come true, large investments must be made in the expansion of the infrastructure to connect the Amazon region with the economic centres in the southeast. At the plan's core are three infrastructure projects in the state of Pará: a hydroelectric power plant in Oriximiná, a bridge over the Amazon river in the city of Óbidos, and the extension of the BR-163 highway coming from Rio Grande do Sul to the northern border with Surinam. The main objective of the economic policy is to create conditions for the transportation of soy production in the Midwest. However, government documents do not mention that this would affect a total of 27 constitutionally protected indigenous territories and nature reserves.

Another government bill aims to allow large-scale agriculture (especially soy) by

Os generais veem a integridade territorial da Amazônia brasileira ameaçada não apenas por ONGs e povos indígenas, mas até mesmo pelo Sínodo Amazônico iniciado pelo Papa Francisco. Antes de tudo, eles temem um conflito assimétrico com organizações guerrilheiras colombianas, presumivelmente apoiadas pelo regime Maduro na Venezuela. Os conflitos internos na Venezuela e na Colômbia poderiam ser levados para o Brasil através de movimentos migratórios descontrolados. A maior ameaça à soberania nacional, aos olhos da ala militar do governo, é a política econômica externa da China, uma vez que ela tem como foco a África, uma região rica em matérias-primas, e porque em Cuba e na vizinha Venezuela conta com governos aliados dispostos a implementar suas políticas. Os generais veem a região amazônica, rica em recursos, ameaçada por investimentos chineses, compra de terras e migrantes dos países vizinhos, que estariam agindo como a quinta coluna de Pequim.

Como reação à complexa situação de segurança, a estratégia de defesa nacional baseia-se, em primeiro lugar, na premissa de que é necessário manter e ampliar a capacidade de dissuasão militar. Para atingir esse objetivo, o Ministro da Defesa, General Azevedo e Silva, anunciou uma redistribuição, assim como uma reforma estrutural e a modernização e rearmamento do aparato militar. A redistribuição diz respeito essencialmente à transferência de unidades da costa atlântica para as fronteiras amazônicas no norte e oeste do país. Além disso, a reforma estrutural visa aumentar a mobilidade para que, caso necessário, as tropas estacionadas em outras partes do país possam ser rapidamente deslocadas para a Amazônia. Nos últimos anos, cerca de 27.000 soldados foram transferidos para a região amazônica. As unidades foram estacionadas principalmente nas fronteiras com a Venezuela, Suriname, Colômbia, Peru e Bolívia. Para este fim, foram criados 23 novos postos fronteiriços ao longo da fronteira amazônica.

As Forças Armadas e o desenvolvimento econômico da Amazônia

Os objetivos da política econômica do governo Bolsonaro na Amazônia estão expressos no Projeto Rio Branco. O programa governamental para o desenvolvimento da região amazônica está sendo elaborado atualmente pela Secretaria de Assuntos Estratégicos (SAE) do Gabinete do Presidente, sob a égide do Almirante Flávio Rocha. Com incentivos governamentais pretende-se estabelecer grandes empresas na região amazônica, as quais, por sua vez, deverão atrair brasileiros não-indígenas de outras regiões do país, contribuindo substancialmente para o aumento do crescimento econômico.

Para que o antigo sonho da ditadura militar da colonização não indígena na região amazônica se torne realidade, é preciso antes de tudo investir na expansão da infraestrutura para conectar a região amazônica com os centros econômicos do sudeste. Peça-chave dos planos são três projetos de infraestrutura no estado do Pará: uma usina hidrelétrica em Oriximiná, uma ponte sobre o Rio Amazonas na cidade de Óbidos e a ampliação da rodovia BR-163, que sai do Rio Grande do Sul, até a fronteira norte com o Suriname. O principal objetivo da política econômica é criar condições para que a produção de soja no Centro-Oeste possa ser escoada. Não há qualquer menção nos documentos governamentais sobre o fato de que isso afetaria um total de 27 territórios indígenas e reservas naturais protegidos pela Constituição.

industrialised farms in indigenous lands. The situation is similar with regard to the extraction of natural resources such as wood and gold. The President wants to legalise mining in the indigenous territories. The constitution does not fundamentally prohibit the mining of raw materials in indigenous lands, but it does require a legal framework for it, which does not exist to this day. A government bill to legalise mining in indigenous lands has already been presented to Congress.

Most recently, President Bolsonaro dismembered the National Amazon Council from the Ministry of the Environment, gave it new responsibilities and also placed it under the authority of a retired general, his Vice President Hamilton Mourão. By decree, the Amazon Council is now not only responsible for inter-ministerial coordination, but also for the conduction of control and repression measures in the Amazon region and serve as an intelligence information platform. To implement these responsibilities, a new federal environmental police force (*Força Nacional Ambiental*) will be created, which will also be under the authority of General Mourão. The new police force is to take over the tasks of controlling and sanctioning environmental offences that were previously under the responsibility of the environmental protection agency (Ibama) and the *Instituto Chico Mendes* (ICM).

Ibama and the Funai indigenous authority were excluded from the newly established Amazon Council, as were the governors of the Amazon states. Even among the technical staff of the new, strongly centralized body, which is to shape Amazonian economic growth, there are no experts in indigenous or environmental issues. Mourão's 23 co-workers are four generals, twelve Army and three Air Force officers as well as four Federal Police officers. The body's decision-making process consists of 14 ministers and works as follows: the ministers are allowed to deliberate, but the final decision is up to Vice-President Mourão.

Operations to protect the rainforest and indigenous peoples

Brazil's generals are playing an increasingly active role as environmental and indigenous issues become more virulent. Not least, the positioning of the generals depends on an adjustment of the national concept of sovereignty in the military think tanks. The fact that sovereignty over the Amazon region also entails responsibility for its inhabitants and environmental protection is now recognised by the generals. As a matter of fact, the Ministry of Defence advertises on its website with a colourful image brochure on "Defence and Environment", which describes sustainability, environmental protection and reforestation as military tasks. Nonetheless, for decades the Amazon rainforest has been illegally exploited for gold and other natural resources. The images of mercury-contaminated rivers have become as world-famous as those of the burning rainforest. With Jair Bolsonaro, it is the very first time that a President supports illegal exploiters. The presidential discourse is encouraging more and more soy barons, loggers and gold diggers to continue penetrating nature conservation areas and indigenous lands.

Thus, the livelihoods of the Brazilian indigenous people are increasingly at risk.

Um outro projeto de lei do governo visa permitir a prática da agricultura em larga escala (especialmente da soja) por parte de empreendimentos agrários industrializados nas áreas indígenas. Semelhante situação existe em relação à extração de recursos naturais como a madeira e o ouro. O Presidente quer legalizar a mineração nos territórios indígenas. A Constituição não proíbe expressamente a exploração de matérias primas em áreas indígenas, porém exige um marco legal para tanto, até hoje inexistente. Um projeto de lei do governo para legalizar a mineração em territórios indígenas já foi apresentado ao Congresso.

Mais recentemente, o Presidente Bolsonaro desmembrou o Conselho Nacional da Amazônia do Ministério do Meio Ambiente, conferindo-lhe novas responsabilidades e colocando-o, igualmente, sob a autoridade de um general da reserva, seu Vice Presidente Hamilton Mourão. Por decreto, o Conselho da Amazônia é agora não só responsável pela coordenação interministerial, como também deverá conduzir ações de controle e repressão na região amazônica, além de servir como plataforma de informações de inteligência. Para implementar essas atribuições, será criada uma nova polícia federal ambiental, a Força Nacional Ambiental, que também estará subordinada ao General Mourão. A nova força policial deverá assumir as funções de controle e sanção de infrações ambientais em substituição ao Ibama, a agência de proteção ambiental anteriormente responsável, e ao Instituto Chico Mendes (ICM).

O Ibama e a autoridade indígena Funai foram excluídos do recém estabelecido Conselho da Amazônia, assim como os governadores dos estados amazônicos. Mesmo entre o pessoal técnico do novo órgão, altamente centralizado, que vai estruturar o crescimento econômico da Amazônia, não há especialistas em questões indígenas ou ambientais. Os vinte e três colaboradores do General Mourão são quatro generais, doze oficiais do Exército e três da Aeronáutica, além de quatro membros da Polícia Federal. O processo decisório do órgão composto por 14 ministros é o seguinte: embora os ministros possam deliberar, a decisão final cabe unicamente ao Vice-Presidente Mourão.

Operações para proteger a floresta tropical e os povos indígenas

Os generais do Brasil estão desempenhando um papel cada vez mais ativo à medida que as questões ambientais e indígenas se tornam mais virulentas. Não por último, o posicionamento dos generais depende de um ajuste do conceito nacional de soberania nos laboratórios de ideias dos militares. Que a soberania sobre a região amazônica também implica assumir responsabilidade para seus habitantes e a proteção ambiental é uma noção agora reconhecida pelos generais. Não é por acaso que o Ministério da Defesa promove no seu site, por meio de uma brochura de imagens multicoloridas, o tema "Defesa e Meio Ambiente", que descreve a sustentabilidade, proteção ambiental e reflorestamento como tarefas militares. No entanto, há décadas a floresta amazônica tem sido explorada ilegalmente em busca de ouro e outros recursos naturais. As imagens de rios contaminados com mercúrio tornaram-se tão famosas mundo afora quanto as das queimadas na floresta amazônica. Com Jair Bolsonaro, os exploradores ilegais são apoiados pela primeira vez por um Presidente da República. O discurso presidencial está incentivando cada vez

Contaminated rivers cause nervous diseases and the foreigners bring in infectious diseases such as COVID-19, which are deadly for the indigenous people. In addition to indirect violence, direct violence is also increasing, presumably as a result of the president's degrading rhetoric. In his speech during the last UN General Assembly, President Bolsonaro described the indigenous people as "cavemen". His government's indigenous project is "to enable the natives to become human beings like us". In 2018 and 2019 alone, at least 163 indigenous people were killed in Brazil in conflicts with illegal intruders.

To contain indigenous cultures, the government curtails NGOs and the Funai (National Indigenous Foundation). After taking office, Bolsonaro transferred the Funai from the Ministry of Justice to the Ministry of Agriculture, whose minister Tereza Cristina represents the interests of agribusiness very one-sidedly. In addition, Funai's responsibility for the demarcation of indigenous areas was withdrawn. Following protests by the indigenous associations in Brasília, Congress reversed the decisions, to which the president responded with a provisional legislative measure (*medida provisória*) to revoke Funai's demarcation authority. The provisional law was again lifted by the Supreme Court. Finally, Bolsonaro appointed Marcelo Augusto Xavier da Silva, former federal police officer and representative of the agricultural lobby, as director of the Funai in order to undermine it from within.

The institutional weakening of Funai, Ibama and ICM through budget cuts, withdrawal of responsibilities and dismissals, was followed most recently by the militarization of the indigenous and environmental policy in the Amazon. As part of a Guarantee of Law and Order (GLO) decree, the President sanctioned Operation *Verde Brasil II* in May and June 2020. Around 4,000 military personnel were deployed for 30 days to protect the rainforest. The first edition of Operation *Verde Brasil I* was carried out at the end of 2019, after the Amazon fires had darkened the sky over São Paulo. Even back then, the generals in Bolsonaro's government exerted considerable media pressure because they saw Brazil's international reputation under massive threat, which eventually led the President to send the military to the Amazon region. The significant difference of Operation *Verde Brasil II* is that the environmental authority Ibama, which was actually in charge of the operation and was still leading it last year, only participated in the operation as an auxiliary body under military command.

Apparently, environmental policy objectives are weighted differently within the government. On the one hand, there is President Bolsonaro, who has suspended the execution of sentences for environmental crimes since October 2019, and his Environment Minister Ricardo Salles, who at a cabinet meeting in April 2020 advocated softening environmental protection laws in the shadow of the novel coronavirus crisis. On the other hand, there is the military faction of the government, led by Vice President Mourão. They fear that the counterproductive and irresponsible Amazon policy could call international actors on the scene, who question Brazil's sovereignty over the biome. In May 2020, for example, General Mourão pointed out that the military could not be permanently deployed for environmental protection tasks, but that the civil control capacities of Ibama and ICM would have to be rebuilt.

mais barões da soja, madeireiros e garimpeiros a continuar penetrando em áreas de conservação da natureza e reservas indígenas.

A base de subsistência dos povos indígenas brasileiros, portanto, está cada vez mais ameaçada. Os rios contaminados causam doenças do sistema nervoso e os forasteiros trazem consigo doenças infecciosas como a COVID-19, que são mortais para os povos indígenas. Além da violência indireta, a violência direta também está aumentando, presumivelmente como resultado da retórica degradante do Presidente. Em seu discurso durante a última Assembleia Geral da ONU, o Presidente Bolsonaro descreveu os indígenas como "homens das cavernas". O projeto indígena de seu governo consiste em "permitir que os índios se transformem em seres humanos como nós". Somente em 2018 e 2019, foram mortos no Brasil pelo menos 163 indígenas em conflitos com invasores ilegais.

Para conter as culturas indígenas, o governo restringe as ONGs e a Funai. Depois de tomar posse, Bolsonaro transferiu a Funai do Ministério da Justiça para o Ministério da Agricultura, cuja ministra Tereza Cristina representa os interesses do agronegócio de forma muito unilateral. Além disso, a responsabilidade da Funai pela demarcação de áreas indígenas foi revogada. Após protestos das organizações indígenas em Brasília, o Congresso reverteu as decisões, ao que o Presidente respondeu com uma Medida Provisória revogando a atribuição da Funai relativa à demarcação. Essa lei provisória foi novamente suspensa pelo Supremo Tribunal Federal. Finalmente, Bolsonaro nomeou Marcelo Augusto Xavier da Silva, ex-policial federal e representante do lobby do agronegócio, como diretor da Funai, a fim de esvaziá-la a partir do seu interior.

Ao enfraquecimento institucional da Funai, do Ibama e do ICM por via de cortes orçamentários, retirada de competências e demissões, seguiu-se mais recentemente o avanço da militarização da política indígena e ambiental na Amazônia. Como parte de um decreto da GLO, o Presidente sancionou a Operação Verde Brasil II em maio e junho de 2020. Quatro mil militares foram destacados pelo período de 30 dias para proteger a floresta tropical. A primeira edição da Operação Verde Brasil I foi realizada no final de 2019, depois que os incêndios na Amazônia tinham escurecido o céu sobre São Paulo. Já naquela época, os generais da ala militar do governo Bolsonaro exerceram considerável pressão na mídia, pois viam a reputação internacional do Brasil fortemente ameaçada, o que acabou levando o Presidente a enviar tropas para a Amazônia. A grande diferença da Operação Verde Brasil II é que a autoridade ambiental Ibama, a quem, na verdade, cabia a responsabilidade pela operação e que ainda estava na liderança no ano anterior, só participou da ação como um órgão auxiliar sob comando militar.

Visivelmente, os objetivos da política ambiental possuem pesos diferentes no interior do governo. Por um lado, está o Presidente Bolsonaro, que mandou suspender a execução de sentenças por crimes ambientais desde outubro de 2019, e seu Ministro do Meio Ambiente, Ricardo Salles, que em uma reunião dos ministros em abril de 2020 defendeu a flexibilização das leis de proteção ambiental à sombra da crise do novo coronavírus. Por outro lado, estão os integrantes da ala militar do governo, liderada pelo Vice-Presidente Mourão. Eles temem que a política contraproducente e irresponsável em relação à Amazônia provoque a entrada em cena de atores internacionais, questionando a soberania do Brasil sobre o bioma. Assim, em maio de 2020, por exemplo, o General Mourão assinalou que

Conclusion: General Mourão as Tsar of the Amazon

The security and defence policy is fully under the control of the generals in the Cabinet, including police and intelligence tasks in the Amazon region. And the geopolitical dimension of Brazil's security policy also bears a military signature. Threat scenarios foresee the territorial integrity of the Amazon being undermined by China and migrants from Venezuela as well as by indigenous peoples and NGOs.

The government project for the economic development of the Amazon (*Projeto Rio Branco*) is consistently led by generals. The idea of using the wealth of the rainforest to increase national economic output dates back to the time of the military dictatorship (*Programa Calha Norte*) and has survived to this day in military think tanks such as the Brazilian National War College (*Escola Superior de Guerra - ESG*).

Environmental and indigenous policies are becoming increasingly militarized. Even at the operational level, the already weakened Ibama Environmental Protection Agency has recently been placed under military command. The same applies to the indigenous authority Funai, which has been hollowed out to the point of dysfunction and is now headed by a former police officer who represents the agribusiness lobby. In environmental excesses such as the weakening of the controlling authorities and the extensive fires in the Amazon, the military cabinet wing proves to be a moderating and pragmatic corrective agent in face of the radical and ideological wing around Jair Bolsonaro, Ricardo Salles and Tereza Cristina.

As the powerful chairman of the Amazon Council and head of the *Rio Branco* project, all development and environmental issues in the Amazon region come together under Vice President Mourão. General Mourão can be considered the Amazon Tsar, who, together with President Bolsonaro, General Heleno (GSI) and Admiral Rocha (SAE), weighs up the interests from the above-mentioned policy areas. Civilian cabinet members, social actors and the governors of the Amazon states are left out. The democratic deficits are obvious. There is no way one can say that there is a primacy of politics over the military.

And also the substantive balancing in favour of economic development and at the expense of the legitimate interests of indigenous peoples and the rainforest seems to have already been made. Bolsonaro's generals want to counteract international concern about the biome and its indigenous peoples, not least because they see at the minimum one form of interference in internal affairs in its wake. The primary concern of the military is to protect national sovereignty over the Amazon against alleged economic, ideological and territorial threats from foreign actors. A global flood of images of burning forests and polluted rivers is therefore considered by the generals to be of little use to those aims.

as Forças Armadas não poderiam ser permanentemente usadas para tarefas de proteção ambiental, mas que as capacidades civis de controle do Ibama e do ICM deveriam ser reconstruídas.

Conclusão: o General Mourão como Czar da Amazônia

A política de segurança e defesa está totalmente sob o controle dos generais no governo, incluindo as funções policiais e de inteligência na região amazônica. Assim também, a dimensão geopolítica da política de segurança do Brasil carrega a assinatura militar. Os cenários de ameaças veem a integridade territorial da Amazônia tanto na mira da China e de migrantes da Venezuela como de povos indígenas e ONGs.

O projeto do governo para o desenvolvimento econômico da Amazônia (Projeto Rio Branco) é exclusivamente liderado por generais. Cabe mencionar que a ideia de usar a riqueza da floresta tropical para aumentar o produto nacional remonta à época da ditadura militar (Programa Calha Norte), tendo sobrevivido até hoje nos laboratórios de ideias dos militares, como a Escola Superior de Guerra (ESG).

A política ambiental e indígena está se tornando cada vez mais militarizada. Mesmo no nível operacional, o já enfraquecido órgão de proteção ambiental, o Ibama, foi recentemente colocado sob comando militar. O mesmo se aplica à autoridade indígena Funai, que foi esvaziada até o ponto de se tornar disfuncional e é atualmente dirigida por um ex-policial, representante do lobby agrário. No caso de excessos no âmbito da política ambiental, como o enfraquecimento das autoridades de controle e os incêndios de grande escala na Amazônia, a ala militar do governo mostra-se como um elemento corretivo moderador e pragmático em relação à ala radical e ideológica ao redor de Jair Bolsonaro, Ricardo Salles e Tereza Cristina.

Como poderoso Presidente do Conselho da Amazônia e chefe do projeto Rio Branco, todas as questões sobre desenvolvimento e meio ambiente na região amazônica convergem para o Vice-Presidente Mourão. O General Mourão pode ser considerado o Czar da Amazônia, que, juntamente com o Presidente Bolsonaro, o General Heleno (GSI) e o Almirante Rocha (SAE), pesam os interesses das áreas políticas mencionadas. Membros civis do governo, atores sociais e governadores dos estados amazônicos são deixados de fora. Os déficits democráticos são óbvios. Não se pode, de forma alguma, falar em primazia da política sobre os militares.

E também a avaliação substantiva em favor do desenvolvimento econômico e à custa dos interesses legítimos dos povos indígenas e da floresta tropical parece já ser assunto definido. Não por último os generais de Bolsonaro querem contrarrestar a preocupação internacional com o bioma e seus povos indígenas, visto que no seu rastro estão antecipando, no mínimo, uma forma de interferência em assuntos internos. A principal preocupação dos militares é proteger a soberania nacional sobre a Amazônia contra supostas ameaças econômicas, ideológicas e territoriais por parte de atores externos. Uma avalanche mundial de imagens de florestas em chamas e rios poluídos, portanto, é considerada pelos militares como sendo pouco útil a esses objetivos.

Security policy recommendations for action

Since the former army officer Bolsonaro took office in January 2019, German, European and Brazilian positions on global challenges such as climate change, migration and the protection of minorities could hardly be more different. Bolsonaro's verbal incitement to slash-and-burn in the Amazon rainforest was only the tip of the iceberg. German-Brazilian relations are facing their deepest crisis since the Brazilian military dictatorship. Common goals of Brazil and Germany are limited to the restoration of democracy in Venezuela and soft balancing against China's New Silk Road. With the illegal drug trade, Germany, the EU and Brazil face a common security policy challenge. Brazil is an important transfer country with unclear borders with the producing countries of Peru, Colombia and Bolivia. Since fifty per cent of Latin American drug production now flows into the European market, combating coca cultivation is in the vital interest of the EU. From the point of view of the EU and Mercosur, robust police and intelligence operations combined with substitution programmes that create lucrative incentives for the cultivation of alternative agricultural products seem promising.

Germany is Brazil's fourth largest trading partner and German direct investments totalling more than 20 billion euros lend weight to Berlin's words in Brasília. In addition, Foreign Minister Ernesto Araújo hopes that Germany will support the EU-Mercosur Free Trade Agreement and Brazil's application for OECD membership. A core bilateral interest of Brazil is the transfer of energy and defence technology from Germany. Thyssen Krupp is currently building four high-tech frigates for the Brazilian Navy and transferring the corresponding military technology. Germany's economic interests are aimed at expanding trade relations and promoting and securing German investments in the Amazon region. Brazil is an important exporter of agricultural products in demand in Germany and of raw materials relevant for industrial production. Securing German economic interests must also be seen in the context of the rise of China and India and their hunger for raw materials. Particularly in the Amazon region, there are signs of increased competition for markets and resources.

The overriding goal of all German security policy engagement in the Amazon region should be to make a constructive contribution to containing the numerous transnational security risks and to increase transparency, confidence-building and cooperation in the fields of military and arms policies in the region. The central instrument should be a trusting and critical dialogue at eye level. Especially the increased exchange between officers' academies and think tanks is promising. While the German armed forces (*Bundeswehr*) are firmly rooted in the German constitution (citizens in uniform, internal leadership), authoritarian thinking patterns are still widespread in Brazil's military elite schools. The aim should be to promote more training cooperation (discussion events, personnel exchange) between the military academies of Germany (*Bundeswehr* Command and Staff College, *Bundeswehr* universities) and Brazil (ESG, ECEME, Army Command and Staff School - *Escola de Comando e Estado-Maior do Exército*). The question of what effects changing profile requirements - which would include police tasks such as the fight against drug trafficking and the prevention of illegal exploitation of resources - would have on the constitution of the *Bundeswehr* shows that the exchange would be instructive for both sides.

Recomendações de política de segurança para a ação

Desde que o ex-oficial do exército Bolsonaro tomou posse em janeiro de 2019, as posições alemãs, europeias e brasileiras sobre desafios globais como a mudança climática, a migração e a proteção das minorias dificilmente poderiam ser mais diferentes. A atitude de Bolsonaro, atiçando verbalmente as chamas das queimadas na Amazônia, foi apenas a ponta do iceberg. As relações germano-brasileiras encontram-se na crise mais profunda desde a ditadura militar. Os objetivos comuns do Brasil e da Alemanha limitam-se à redemocratização da Venezuela e ao *Soft Balancing* contra a Nova Rota da Seda da China. Com o comércio ilegal de drogas, a Alemanha, a UE e o Brasil enfrentam um desafio conjunto em termos da política de segurança. O Brasil é um importante país de trânsito com fronteiras difusas com os produtores Peru, Colômbia e Bolívia. Como cinquenta por cento da produção de drogas na América Latina é escoada atualmente para o mercado europeu, o combate ao cultivo da coca é de interesse vital para a UE. Do ponto de vista da UE e do Mercosul, robustas operações policiais e de inteligência em combinação com programas de substituição, que criam incentivos lucrativos para o cultivo de produtos agrícolas alternativos, parecem promissoras.

A Alemanha é o quarto maior parceiro comercial do Brasil e os investimentos diretos alemães ultimamente no valor de mais de 20 bilhões de euros conferem peso às palavras de Berlim em Brasília. Além disso, o Ministro das Relações Exteriores, Ernesto Araújo, espera que a Alemanha apoie o Acordo de Livre Comércio UE-Mercosul e a candidatura do Brasil como membro da OCDE. Um foco de interesse bilateral do Brasil é a transferência de tecnologia nas áreas de energia e defesa por parte da Alemanha. Atualmente, a Thyssen Krupp está construindo quatro fragatas de alta tecnologia para a Marinha brasileira, o que inclui a transferência da respectiva tecnologia militar. Os interesses econômicos da Alemanha visam expandir as relações comerciais e promover e assegurar os investimentos alemães na região amazônica. O Brasil é um importante exportador de produtos agrícolas em demanda na Alemanha e de matérias primas relevantes para a produção industrial. O objetivo de assegurar os interesses econômicos alemães deve ser visto, igualmente, no contexto da ascensão da China e da Índia e de sua fome por matérias primas. Particularmente na região amazônica, há sinais de um aumento da concorrência por mercados e recursos.

O objetivo primordial de todo engajamento da política de segurança alemã na região amazônica deverá consistir em realizar uma contribuição construtiva para conter os inúmeros riscos de segurança transnacional, assim como aumentar a transparência, a confiança e a cooperação nos campos da política militar e de armamento na região. Nesse contexto, um instrumento central deverá ser o diálogo crítico e permeado de confiança, de igual para igual. Especialmente promissor é o crescente intercâmbio entre as academias de oficiais e os *Think Tanks*. Enquanto as Forças Armadas alemãs (*Bundeswehr*) estão firmemente enraizadas na Constituição (cidadãos em uniforme, liderança interna), os padrões de pensamento autoritário ainda estão amplamente difundidos nas escolas de formação da elite militar no Brasil. Seria desejável promover uma maior cooperação na área de formação (eventos de debate, intercâmbio de pessoal) entre as academias militares da Alemanha (*Führungsakademie der Bundeswehr* – Colégio do Estado-Maior, universidades das Forças Armadas) e do Brasil (ESG, ECEME - Escola de Comando e Estado-Maior do Exército). A

The deepening of the defence policy dialogue at the level of defence ministers and supreme commanders would provide an opportunity to better understand the Brazilian generals' development strategy for the Amazon region, exploring economic and technological convergence of interests. Likewise, Brazil should be encouraged to further strengthen its command structures overarching the branches of the armed forces and to introduce "second-degree" confidence-building measures such as mutual force inspections and verification measures. Armaments policy cooperation with Brazil should be directed primarily to the specific requirements of future UN missions (expansion of transport and logistics capacities), as well as placing greater emphasis on the aspect of interoperability. ■

questão sobre os efeitos que uma mudança no perfil de exigências – o que incluiria funções policiais como o combate ao tráfico de drogas e a prevenção da exploração ilegal de recursos - teria sobre a conformação da *Bundeswehr* deixa claro que o intercâmbio seria instrutivo para ambas as partes.

O aprofundamento do diálogo sobre política de defesa em nível dos ministros de defesa e dos comandantes em chefe proporcionaria uma oportunidade para entender melhor a estratégia de desenvolvimento dos generais brasileiros para a região amazônica, assim como para identificar o potencial de convergência dos interesses econômicos e tecnológicos. Da mesma forma, deve-se incentivar o Brasil, nesse contexto, a fortalecer ainda mais suas estruturas de comando transcendendo os ramos das Forças Armadas, além de introduzir iniciativas geradoras de confiança de "segundo grau", tais como inspeções mútuas de tropas e medidas de verificação. A cooperação em matéria de política armamentista com o Brasil deve orientar-se principalmente para as exigências específicas de futuras missões da ONU (expansão das capacidades de transporte e logística), dando maior ênfase que até agora ao critério da interoperabilidade. ■

Juan Battaleme

Juan Battaleme é bacharel em Ciência Política pela Universidade de Buenos Aires; Mestre em Relações Internacionais, Flacso; Mestre em Administração Pública e Ciências do Estado, pela UCEMA. Fellow em Fulbright e Chevening. Professor de Relações Internacionais, Segurança Internacional e Tecnologia Internacional, na Universidade de Buenos Aires, UADE e UCEMA. Professor de Estratégia Naval no Colégio de Guerra Naval da Argentina e de Geopolítica, no Colégio de Guerra da Força Aérea. Secretário Acadêmico do Conselho Argentino de Relações Internacionais (CARI).

Juan Battaleme has a BA in Political Science, Buenos Aires University; MA in International Relations, Flacso; MA in Public Administration and States Sciences, UCEMA University, Fulbright and Chevening Fellow. Professor of International Relations, International Security and Technology, at Buenos Aires University, UADE and UCEMA. Professor of Naval Strategy at the Argentinean Naval War College and Geopolitics, at the Air Force War College. Academic Secretary of the Argentinean Council of International Relations (CARI).

Novas fronteiras na era da geopolítica digital: A interdependência como arma, rivalidade estratégica e recomendação de políticas para Argentina e Brasil

New frontiers in the geopolitical digital era: The weaponization of interdependence, strategic rivalry and policy recommendation for Argentina and Brazil

Juan Battaleme

Secretário Acadêmico do Conselho Argentino de Relações Internacionais (CARI)
Academic Secretary of the Argentinean Council of International Relations (CARI)

Rivalidade estratégica na era da interdependência estrutural

À medida que o século XXI avança, observamos a emergência de ameaças explícitas à governança global em torno de várias questões transnacionais. Ao mesmo tempo, cresce a rivalidade estratégica entre os Estados Unidos e a China. À medida que as grandes potências se veem como uma ameaça para manter ou consolidar seus projetos hegemônicos, a desconfiança aumenta, a ação política para boicotar o crescimento dos concorrentes e as esferas de influência aparecem, enquanto a estrutura da política internacional permanece em um estado de fluxo.

Para manter a clareza dos argumentos do artigo, definiremos rivalidade estratégica como o choque entre superpotências para obter e acessar recursos relacionados às suas necessidades militares e econômicas a fim de garantir seu domínio. O que está em disputa é o poder em um sentido bruto e, para isso, são usados todos os ativos à disposição. O objetivo é tentar obter

Strategic rivalry in the age of structural interdependence

As the XXI century continues to move forward, there are explicit threats to global governance around several transnational issues. At the same time, the strategic rivalry between the United States and China grows. As great powers see each other as a menace to keep or consolidate their hegemonic projects, mistrust ascends, political action to boycott competitors rise and spheres of influence appear, while the structure of international politics remains in a state of flow.

To maintain the clarity of the paper's arguments, we will define strategic rivalry as the clash between superpowers to obtain and access capabilities related to their military and economic necessities in order to secure their dominance. Power - in a rough sense - is in dispute using every asset at their disposal. The objective is to obtain leverage in certain regions, governments, and peoples to command the future. We live in transition times

as we usually say, experiencing the turbulence of gap narrowing and the possibility of the newest gaps with second and third-tier powers. In this environment, technology is a critical factor in the strategic rivalry.

Since complex interdependence became the dominant structure in the international system, there were several discussions about its virtues in terms of progress and benefits along with the existing risks resulting from evident and multiple types of asymmetries both from power and capacities at the political, economic, and military levels. The most crucial asymmetry is related to information because it creates knowledge, and that affects power relations in terms of security and economics.

The paper by Robert Keohane and Joseph Nye, "Power and Interdependence," gives us a good insight into why this is important. First, the multiplicity of political channels and different types of actors participating in a particular grid creates several and dense networks of interest. Even if only a few could be considered significant players, some of them can affect negotiations, perceptions, and political decisions. Major ones set the conditions and limits for those who belong or want to participate in their networks. To access what they offer, they usually ask for a series of concessions, permissions, and, many times, data, and if we do not agree with it, access denial is their action. A slightly similar situation exists in the complex world of international finance and banking: few institutions have many rules to follow before giving access to what they have to offer. We defined power in the XXI century as the capacity to create and to give access, but also to block other competitors' activities or deny access.

Secondly, the issues that are part of the international agenda are more diverse than ever before. Most of the time, the politics of issue linkage using interdependence dimensions of vulnerabilities and sensibilities dimensions as a part of the negotiations, oblige states to consider the security aspects in every part of their strategic agenda. Everything could be considered a security issue, so that is why we say we are living a period of "securitization" of everything.

As an example of the problem, political disagreements about territory have affected the trade relationship between South Korea and Japan, as a part of issue linkage politics starting an escalation of aggressive actions between them. South Korea was removed from Japan's list of trusted exporting partners, creating vulnerability for Seoul[1]. That action forced a process of disarticulation of their value chains, affecting the cooperation in intelligence affairs, security, and stressing their political relations, resorting to nationalism as a way to strengthen their positions.

Europe presents another example. Chinese Huawei Company, looking to gain access to contracts in the UK market, had to accept the creation of a joint laboratory to test its equipment, monitored and controlled by the GCHQ to counteract the security

1 The International Institute for strategic Studies, The Japan-South Korea rift, Strategic Comments, Vol.26, IISS, January 2020. En https://www.iiss.org/publications/strategic-comments/2020/japansouth-korea?, visitado el 15/1/2020.

alavancagem em certas regiões, governos e povos para comandar o futuro. Vivemos tempos de transição, como costumamos chamar, experimentando a turbulência do estreitamento de brechas e a possibilidade de novas brechas com poderes de segundo e terceiro níveis. Nesse ambiente, a tecnologia é um fator crítico na rivalidade estratégica.

Desde que a interdependência complexa se tornou a estrutura dominante no sistema internacional, houve várias discussões sobre suas virtudes em termos de progresso e benefícios, assim como os riscos existentes, resultantes de evidentes e múltiplos tipos de assimetrias, tanto de poder quanto de capacidades políticas, econômicas e militares. A assimetria mais crucial está relacionada à informação, pois cria conhecimento e afeta as relações de poder em termos de segurança e economia.

O trabalho de Robert Keohane e Joseph Nye, "Power and Interdependence" (poder e interdependência), nos dá uma boa ideia de por que isso é importante. Primeiro, a multiplicidade de canais políticos e os diferentes tipos de atores que participam de uma matriz específica criam várias e densas redes de interesse. Mesmo que apenas alguns possam ser considerados atores significativos, vários deles podem afetar negociações, percepções e decisões políticas. Os atores principais estabelecem as condições e limites para aqueles que pertencem ou desejam participar de suas redes. Para acessar o que eles oferecem, geralmente solicitam uma série de concessões, permissões e dados e, na maioria das vezes, quem não concorda com isso, tem seu acesso negado. Uma situação ligeiramente semelhante existe no complexo mundo das finanças e bancos internacionais: poucas instituições têm muitas regras que devem ser seguidas por quem quer acessar o que elas têm a oferecer. Definimos poder no século XXI como a capacidade de criar e dar acesso, mas também de bloquear outras atividades de concorrentes ou negar o acesso.

Em segundo lugar, as questões que fazem parte da agenda internacional nunca foram tão diversas. Na maioria das vezes, a política de vinculação de questões usando dimensões de interdependência de vulnerabilidades e sensibilidade como parte das negociações, obriga os Estados a considerar os aspectos de segurança em todos os componentes de sua agenda estratégica. Tudo pode ser considerado um problema de segurança e é por isso que vivemos um período de "securitização" de tudo.

Um exemplo desse problema são as divergências políticas e territoriais que afetam a relação comercial entre a Coréia do Sul e o Japão, como parte da política de vinculação entre questões e escalada de ações agressivas entre os países. A Coréia do Sul foi removida da lista de parceiros exportadores confiáveis do Japão, criando uma vulnerabilidade para Seul[1]. Essa ação forçou um processo de desarticulação de suas cadeias de valor, afetando a cooperação nos assuntos de inteligência, segurança e enfatizando suas relações políticas, recorrendo ao nacionalismo como forma de fortalecer suas posições.

A Europa apresenta outro exemplo. A empresa chinesa Huawei, buscando obter acesso a contratos no mercado do Reino Unido, teve que aceitar a criação de um laboratório conjunto para testar seus equipamentos e que seria monitorado e controlado pelo GCHQ

1 The International Institute for strategic Studies, The Japan-South Korea rift, Strategic Comments, Vol.26, IISS, January 2020. En https://www.iiss.org/publications/strategic-comments/2020/japansouth-korea?, visitado el 15/1/2020.

concerns that were evident within intelligence community. Fear of data theft from society and the British through Chinese equipment as a new way of espionage drove the 5G considerations in the UK.

Finally, they presented a discussion about the ability to apply coercion through the use of military power in kinetic terms. Some claim that the present political and military situation allows declaring the obsolescence of significant powers wars[2]. The use of Military power remains only against lower-level rivals. However, the growing vision of a "technological peace[3]" is in reality considered a menace as a result of the growing hostility that appears in cyberspace, as digital technology creates opportunities and starts to expand the vulnerabilities window.

There is evidence of the incentives that this area offers in offensive terms[4], making us more willing to use the cyber means to exercise coercion or harm a potential rival. As Stuxnet and other developments proved, it is possible (although expensive) to use cyberspace to affect the real world. The creation of capabilities to defend or to attack adversaries' systems, exploiting vulnerabilities, and looking for those opportunities to take advantage of others' weaknesses while trying to create new digital dependency. The militarization of cyberspace is a present phenomenon, and it is quite impossible to return to the age of "innocence" about the internet. The digital age, based on mobility and connectivity, adds several questions about society's safety and privacy while creating a new security dilemma among states.

We build Globalization on two things. One is the development of communications infrastructure. The other is the capacity to maintain flows through a relatively limited and concentrated series of nodes where some of them have higher preeminence than others. The newest race of communications infrastructure, commonly known as the 5G race, is one of the many examples that show us a world of asymmetrical interdependence. The datafication of everything, and the cross-domain databases as a way to obtain advantages create the incentive to compete rather than cooperate.

In a multi-network world, the core nodes are relatively few and linked to each other. Most significant nodes create more political effects than the smaller ones, establishing the entry point to a particular network of interest. The architecture of physical networks -in terms of concentration or distribution of nodes- would impact how we organize our social relations, economies, and policies around them. For most of the analysts, the power exerted over specific networks in terms of construction quickly became apparent. Furthermore, their degree of institutionalization (architecture) opens many possibilities for those who created them.

2 Michael Mandelbaum (2019) Is Major War Still Obsolete?, Survival, 61:5, 65 71,

3 Martin, Felix, Review: Pax technica by Michael Howard, Financial Times, May 20, 2015 en https://www.ft.com/content/035db35e-f3db-11e4-99de-00144feab7de, visitado el 30/1/2020

4 For further reading on the offense defense balance we recommend: Van Evera, Stephen. "Offense, Defense, and the Causes of War." International Security, vol. 22, no. 4, 1998, pp. 5–43. JSTOR, www.jstor.org/stable/2539239. Accessed 30 Jan. 2020. Also, Battaleme, Juan, Un Mundo Ofensivo: El Balance Ofensivo-Defensivo y los conflictos de Kosovo, Afganistán, Irak y Chechenia, 2ed, Ed. Temas, Buenos Aires, 2009. Slayton, Rebecca, What is Cyber Offense and Defense Balance? Conception, Causes and Assesments, International Security, Vol. 41, No. 3 (Winter 2016/17), pp. 72–109, doi:10.1162/ISEC_a_00267.

para combater as preocupações de segurança que eram evidentes na comunidade de inteligência. O medo do roubo de dados da sociedade e dos britânicos através de equipamentos chineses como uma nova maneira de espionagem impulsionou os debates sobre o 5G no Reino Unido.

Por fim, apresentou-se argumento sobre a capacidade de aplicar coerção através do uso do poder militar em termos cinéticos. Alguns afirmam que a atual situação política e militar permite declarar a obsolescência de importantes poderes de guerra[2]. O uso do poder militar permanece apenas contra rivais de nível inferior. No entanto, a crescente visão de uma "paz tecnológica"[3] é, na realidade, considerada uma ameaça resultante da crescente hostilidade que aparece no ciberespaço à medida em que a tecnologia digital cria oportunidades e começa a expandir as janelas de vulnerabilidades.

Há evidências dos incentivos que essa área oferece em termos ofensivos[4] aumentando a disposição de usar os meios cibernéticos para exercer coerção ou prejudicar um potencial rival. O Stuxnet e outros dispositivos provaram que é possível (embora caro) usar o ciberespaço para afetar o mundo real. Criam-se recursos para defender ou atacar os sistemas dos adversários, explorando suas vulnerabilidades e procurando oportunidades para aproveitar as suas fraquezas ao mesmo tempo em que se tenta criar uma nova dependência digital. A militarização do ciberespaço é um fenômeno presente e é impossível voltar à "era da inocência" da internet. A era digital, baseada na mobilidade e conectividade, levanta várias questões a respeito da segurança e da privacidade da sociedade, criando um novo dilema de segurança entre os Estados.

Construímos a globalização sobre dois fundamentos. O primeiro é o desenvolvimento da infraestrutura de comunicação. O segundo é a capacidade de manter fluxos através de uma série de nodos relativamente limitada e concentrada, onde alguns têm maior preeminência do que outros. A mais recente corrida em termos de infraestrutura de comunicação, comumente conhecida como corrida pelo 5G, é um dos muitos exemplos que nos mostram um mundo de interdependência assimétrica. A transformação de tudo em dados, e os bancos de dados cross-domain como forma de obter vantagens incentivam a competição em vez da cooperação.

Em um mundo de múltiplas redes, os nodos centrais são poucos, relativamente, e conectados entre si. Os nodos mais significativos geram mais efeitos políticos do que os menores, estabelecendo o ponto de entrada para uma rede de interesse específica. A arquitetura das redes físicas - em termos de concentração ou distribuição de nodos - afetaria a forma como organizamos nossas relações sociais, economias e políticas. Para a maioria dos analistas, rapidamente ficou clara o poder exercido sobre redes

2 Michael Mandelbaum (2019) Is Major War Still Obsolete?, Survival, 61:5, 65 71,

3 Martin, Felix, Review: Pax technica by Michael Howard, Financial Times, May 20, 2015 en https://www.ft.com/content/035db35e-f3db-11e4-99de-00144feab7de, visitado el 30/1/2020

4 For further reading on the offense defense balance we recommend: Van Evera, Stephen. "Offense, Defense, and the Causes of War." International Security, vol. 22, no. 4, 1998, pp. 5–43. JSTOR, www.jstor.org/stable/2539239. Accessed 30 Jan. 2020. Also, Battaleme, Juan, Un Mundo Ofensivo: El Balance Ofensivo-Defensivo y los conflictos de Kosovo, Afganistán, Irak y Chechenia, 2ed, Ed. Temas, Buenos Aires, 2009. Slayton, Rebecca, What is Cyber Offense and Defense Balance? Conception, Causes and Assesments, International Security, Vol. 41, No. 3 (Winter 2016/17), pp. 72–109, doi:10.1162/ISEC_a_00267.

Adding to what was indicated above, we should be aware of the importance of "power in networks", who is who in certain network and how they allow or limit access of connection to others. The power "over" and "in" networks creates the political environment to access or deny what a country needs to develop.

Henry Farrell and Abraham L. Newman (2019) describe, in a recent work, the existence of two problems that arise with the expansion and centralization of networks in a few central nodes related to networks of communications, financial exchanges and physical production. Networks have an unequal capacity for influence, and they create a differentiated impact, since belonging to a particular network can mean lower benefits than one with more substantial connections. Relative gains remain essential even in a non-zero-sum world.

As networks grow, new nodes attempt to connect to networks with more ties. That situation adds value to networks on top of others. In doing so, they become a "structure," generating a "lock-in" effect on those who are part of it. Once established, they are hard to challenge. 1) they have better access and, 2) a challenging network must prove in advance that it will provide a superior benefit from the preceding one while, at the same time, getting a significant number of actors who want to converge on its network. Easy to enter, easy to deny, hard to get away, hard to build alternative networks.

There are two ways to use interdependence as a weapon. The first is known as a "panopticon effect," which is the ability to observe and collect critical information from the networks' circulating flows. This advantage comes from the ability of a particular group of countries and companies to access the information found on its nodes, both physically and legally, allowing to monitor activities of interest in the public and private spheres, whether they are allies or rivals. Permanent monitoring provides advantages that allow us to understand and therefore operate over intentions and tactics, helping to prevent, deter or derail actions considered dangerous or against specific interests.

The second is the "chokepoint effect," which is based on States' privileges through existing capacities or infrastructure to limit or penalize their use in some areas by third parties. There are critical geographical places, materials, and operating systems onerous and painful to replace. When the permission to access is limited to a handful of actors, anyone who can deny it has a high capacity of coercion. It could entail using it to raise security concerns. Both effects are problems arising from a high degree of connection.

While there is a consensus on the possibilities and opportunities posed by an exponential increase in connections in various areas, there is relatively less awareness of the dangers that a world of greater connections poses, as the two uses of interdependence as a weapon show us. Brazil and Argentina were victims of the great powers' capacities to gain unauthorized access to our sensible networks.

To enlighten the preceding claims for this short policy briefing, we chose three examples. Between 2010 and 2013, the NSA spied political authorities and key companies' directives in Brazil and Mexico in order to gain knowledge on energy production processes, financial aspects, projects and developments of those companies in various

específicas em termos de construção. Além disso, seu grau de institucionalização (arquitetura) abre muitas possibilidades para seus criadores.

Além disso, devemos estar cientes da importância do "poder nas redes", quem é quem em determinada rede e como permitem ou limitam o acesso de outros à conexão. O poder "over" (sobre) e "in" (dentro) nas redes cria o ambiente político para permitir ou negar o acesso ao que um país precisa desenvolver.

Em trabalho recente, Henry Farrell e Abraham L. Newman (2019) descrevem a existência de dois problemas que surgem com a expansão e centralização de redes em alguns nodos centrais relacionados a redes de comunicações, trocas financeiras e produção física. As redes têm uma capacidade desigual de influência e criam um impacto diferenciado, pois pertencer a uma determinada rede pode representar menos benefícios do fazer parte de uma rede com conexões mais substanciais. Ganhos relativos permanecem essenciais mesmo em um mundo que não é de soma zero.

À medida em que as redes crescem, novos nodos tentam se conectar a redes com mais vínculos. Essa situação agrega valor a certas redes em detrimento de outras. Ao fazer isso, tornam-se uma "estrutura", gerando um efeito de "lock-in" (aprisionamento) nos seus integrantes. Uma vez estabelecidos, são difíceis de desafiar. 1) eles têm melhor acesso e, 2) uma rede desafiadora deve provar antecipadamente que proporcionará um benefício superior à anterior e, ao mesmo tempo, deverá obter um número significativo de atores que desejam convergir em sua rede. Facilidade para entrar, facilidade para negar, dificuldade de sair, dificuldade para criar redes alternativas.

Existem duas maneiras de usar a interdependência como arma. A primeira é conhecida como "efeito panóptico", que é a capacidade de observar e coletar informações críticas dos fluxos que circulam nas redes. Essa vantagem vem da capacidade de um grupo específico de países e empresas de acessar as informações encontradas em seus nodos, tanto física quanto legalmente, permitindo monitorar atividades de interesse nas esferas pública e privada, sejam elas de aliados ou de rivais. O monitoramento permanente oferece vantagens que nos permitem entender e, portanto, atuar sobre intenções e táticas, ajudando a prevenir, dissuadir ou inviabilizar ações consideradas perigosas ou contrárias a interesses específicos.

A segunda maneira de usar a interdependência como arma é o "efeito de ponto de estrangulamento" (chokepoint effect), que se baseia nos privilégios dos Estados por meio das capacidades ou infraestrutura existentes para limitar ou penalizar o uso desses em algumas áreas por terceiros. Existem lugares geográficos críticos, materiais e sistemas operacionais de substituição onerosa e difícil. Quando a permissão de acesso é limitada a um punhado de atores, qualquer um que possa negá-la tem uma alta capacidade de coerção. Isso poderia implicar em usar essa capacidade para levantar preocupações de segurança. Ambos os efeitos representam problemas decorrentes de um alto grau de conexão.

Embora exista um consenso sobre as possibilidades e oportunidades geradas por um aumento exponencial nas conexões em várias áreas, há relativamente menos consciência dos perigos que um mundo com mais conexões apresenta, como nos mostram os

locations of the world. Using the Prism and Stellarwind programs, U.S. agencies and interested operators obtained vast amounts of information thanks to their ability to exploit the benefits of policies aimed at promoting freedom of Internet connection. As a consequence, Brazil's former president Dilma Rousseff proposed to build its independent Internet in an attempt to break the dominance on private infrastructure related to the ones from the United States and Europe.

Simultaneously, the GCHQ (the British NSA) deployed a similar program with two objectives: one was to be able to spy on Argentine communication networks. They tried to understand and monitor the information traffic (especially emergency and military comms) as a consequence of the increasing political tension between Argentina and the British government over the Malvinas Islands. The other was to try to influence Argentina's partners that helped the blockade effort promoted by its diplomacy at the regional level. They launched a campaign aimed to affect several different countries' public opinion concerning the controversy over the Islands, known as "Operation Quito."

Finally, there is a growing concern about Maduro's autocratic regime strengthening its political alliance with Russia and China and beginning to develop its 4G network with Russia and China as partners, providing them the opportunity to work directly over Latin American space. Thanks to that, all kinds of surveillance technology, especially on biometric data are being deployed not only in Venezuela but also in other countries. The Chinese also have been the developers of the so-called "Carnet de la Patria," which is the only means for Venezuelan citizens to receive official assistance in the midst of a humanitarian crisis. At least China and Russia will have the opportunity to create their panopticon system in a country with all the resources they need.

From multilateralism to agile governance

Tensions between Huawei Company and Donald Trump's administration over 5G networks have weaponized interdependence and there is a growing will to use it as such. In Latin America, we started to feel the effects of that competition since the two major players are looking for new partners in the region. While 4G infrastructures throughout Latin America are of American or European origin, the recorded reckless use by our powerful partners has opened up some space to consider alternatives in the development of 5G lines or supplementing existing networks.

While the breach of trust due to the discovery of active information monitoring programs put the U.K. and U.S. governments in an awkward diplomatic situation, it was Brazil's and Argentina's governments who had to rebuild the relationship for several reasons. This political advantage begins to fade as China becomes more active in communications and the digital world. Even if we expect similar conduct from that country, it is not clear that the political balance will remain in favor of Western countries. For example, it is highly probable that in the signal communications field, a more substantial Chinese penetration in South America will affect the U.S. information gathering.

dois usos da interdependência como arma. Brasil e Argentina foram vítimas das grandes potências e sua capacidade de obter acesso não autorizado a nossas redes sensíveis.

Para explicitar as reivindicações anteriores neste breve resumo, foram escolhidos três exemplos. Entre 2010 e 2013, a NSA espionou autoridades políticas e lideranças de empresas-chave no Brasil e no México a fim de obter conhecimento sobre processos de produção de energia, aspectos financeiros, projetos e avanços dessas empresas em vários locais do mundo. Usando os programas Prism e Stellarwind, as agências dos EUA e as operadores interessados obtiveram uma grande quantidade de informações graças à sua capacidade de explorar os benefícios de suas políticas destinadas a promover a liberdade de conexão à Internet. Consequentemente, a ex-presidente do Brasil, Dilma Rousseff, propôs construir uma internet independente, na tentativa de quebrar o domínio da infraestrutura privada relacionada aos Estados Unidos e à Europa.

Ao mesmo tempo, o GCHQ (NSA britânica) implantou um programa semelhante com dois objetivos: o primeiro era ser capaz de espionar as redes de comunicação argentinas. Eles tentaram apreender e monitorar o tráfego de informações (especialmente comunicações de emergência e militares) como resultado da crescente tensão política entre a Argentina e o governo britânico sobre as Ilhas Malvinas. O outro era tentar influenciar os parceiros da Argentina que ajudaram o esforço de bloqueio promovido por sua diplomacia em nível regional. Eles lançaram uma campanha destinada a influenciar a opinião pública de vários países a respeito da controvérsia sobre as Ilhas, conhecida como "Operação Quito".

Por último, existe uma preocupação crescente com o regime autocrático de Maduro, que fortaleceu sua aliança política com a Rússia e a China, começando a desenvolver sua rede 4G com a parceria desses dois países e oferecendo a eles a oportunidade de trabalhar diretamente no espaço latino-americano. Graças a isso, todos os tipos de tecnologia de vigilância, especialmente dados biométricos, estão sendo implantados não apenas na Venezuela, mas também em outros países. Os chineses também foram os criadores da chamada "Carnet de la Patria", que é o único meio que os cidadãos venezuelanos possuem para receber assistência oficial em meio a uma crise humanitária. Assim, China e Rússia terão a oportunidade de criar seu sistema de panóptico em um país com todos os recursos necessários.

Do multilateralismo à governança ágil

As tensões entre a Huawei e o governo de Donald Trump sobre as redes 5G criaram o uso da interdependência como arma e a crescente vontade de usá-la como tal. Na América Latina essa competição é constatada, uma vez que os dois principais atores estão procurando novos parceiros na região. Embora as infraestruturas 4G em toda a América Latina sejam de origem americana ou europeia, a observação do uso imprudente por parte de nossos parceiros poderosos abriu espaço para considerar alternativas no desenvolvimento de linhas 5G ou complementar as redes existentes.

Embora a quebra de confiança devida à descoberta de programas ativos de monitoramento de informações coloque os governos do Reino Unido e dos EUA em uma situação diplomática embaraçosa, foram os governos do Brasil e da Argentina que tiveram que reconstruir

Countries of strategic weight resembling Argentina do not have room to build their own networks and, in the end, we must "trust" other potential partners. Therefore, specific reinsurance should be considered to keep them connected to western networks and even strengthen them. If connectivity is going to grow, the strategic restriction should be a political guide; otherwise, we will live in a world of fractured networks competing with each other and will not be able to obtain the benefits achieved so far.

Understanding multiple transformations as their impacts occur, provokes optimistic views about the possibilities of abundance promised by new technologies in the near future; on the other hand, a larger pessimism arises for a scenario that presents itself bleak as a result of the anxiety generated by an awareness of divergent or fractured social transformation. No one knows what is going to happen, and yet we think we have the only solution for both scenarios: Multilateralism.

In this sense, calling for "multilateralism", a growing system of coordinated relations between multiple States following a series of principles of conduct capable of concerted action to achieve specific objectives, is a discourse more related to the twentieth century than to the current one. Multilateralism is rational actors with a similar identity; in this sense, in a world of State prominence, that was the right tool. International governance is not going to go through these kinds of agreements.

Hence the emergence and promotion of "agile governance," which can articulate different logic, objectives, and actions in order to navigate a transition that presents itself atypical compared to others of the past. Solving the problems we face between State actors with decreasing weight, transnational corporate actors with a growing weight in international affairs, and civil society interested in specific niches will demand this new type of hybrid politics.

The governance of "multiple stakeholders," which has been operating for years in the most successful case of hybrid governance (States and private actors), the Internet, gradually becomes relevant. This scheme has allowed cyberspace to grow successfully by demonstrating that actors with different views can work convergently, achieving dynamic governance. The dangers arising from its expansion, such as data manipulation, various criminal uses, and privacy abuses are a reality as demonstrated by various initiatives from the private world involving State actors. Peripheral countries with their technological complexes could find in this type of governance an alternative to protect their interests and those of their private sectors, increasingly connected with external spaces of action.

Multi-party governance is guided by the conceptual approach by which anything not expressly prohibited is permitted. Multilateral governance is different since it assumes that anything that is not expressly permitted is prohibited, in this sense, in its efforts to regulate and control it appears as a defensive tool of States.

Arms control regimes, especially nuclear weapons regimes, were guided by this logic. Asking the world to follow parameters of the last century in the face of the ease with which they proliferate from new developments does not require thinking of frameworks that work under self-restriction logics rather than control or sanctions.

o relacionamento por diversas razões. Essa vantagem política começa a desaparecer à medida em que a China se torna mais ativa nas comunicações e no mundo digital. Mesmo prevendo uma conduta semelhante daquele país, não está claro que o equilíbrio político permaneça a favor dos países ocidentais. Por exemplo, é altamente provável que, no campo das comunicações por sinal, uma penetração chinesa mais substancial na América do Sul afete a coleta de informações norte-americana.

Os países com peso estratégico semelhante à Argentina não têm espaço para construir suas próprias redes e, no final, precisamos "confiar" em outros parceiros potenciais. Portanto, garantias específicas devem ser consideradas para mantê-los conectados às redes ocidentais e até para fortalecê-los. Se a conectividade crescer, a restrição estratégica deve ser um guia político. Caso contrário, viveremos em um mundo de redes fraturadas, competindo entre si e não conseguiremos obter os benefícios alcançados até agora.

Compreender múltiplas transformações à medida que seus impactos ocorrem gera visões otimistas sobre as possibilidades de abundância prometidas pelas novas tecnologias em um futuro próximo. Por outro lado, surge um pessimismo maior com relação a um cenário que se apresenta sombrio como resultado da ansiedade gerada por uma consciência de transformação social divergente ou fraturada. Ninguém sabe o que vai acontecer e, no entanto, achamos que temos a solução única para os dois cenários: o multilateralismo.

Nesse sentido, os apelos ao "multilateralismo", um sistema crescente de relações coordenadas entre múltiplos Estados, seguindo uma série de princípios de conduta capazes de ação concertada para alcançar objetivos específicos, estão mais relacionados ao século XX do que ao atual. O multilateralismo são atores racionais com uma identidade semelhante e, nesse sentido, em um mundo de preeminência estatal, essa era a ferramenta correta. A governança internacional não vai passar por esse tipo de acordo.

Consequentemente, observamos o surgimento e a promoção da "governança ágil", que pode articular diferentes lógicas, objetivos e ações a fim de navegar em uma transição que se apresenta atípica em comparação com outras do passado. Resolver os problemas que enfrentamos entre atores estatais com peso decrescente, atores corporativos transnacionais com peso crescente nos assuntos internacionais e a sociedade civil interessada em nichos específicos exigirá esse novo tipo de política híbrida.

A governança de "stakeholders" múltiplos, observada há anos no caso mais bem-sucedido de governança híbrida (Estados e atores privados), que é a internet, gradualmente se torna relevante. Esse arranjo permitiu que o ciberespaço crescesse com sucesso, demonstrando que atores com visões diferentes podem trabalhar de forma convergente, alcançando uma governança dinâmica. Os perigos decorrentes de sua expansão, como a manipulação de dados, diversos usos criminosos e abusos à privacidade, são uma realidade que é trabalhada em conjunto, como demonstrado por várias iniciativas do mundo privado envolvendo atores estatais. Os países periféricos, com seus complexos tecnológicos, poderiam encontrar nesse tipo de gvernança uma alternativa para proteger seus interesses e os de seus setores privados, cada vez mais conectados a espaços de ação externos.

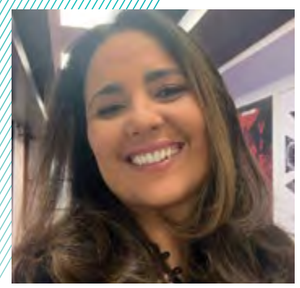
A governança por múltiplas partes é orientada pela abordagem conceitual pela qual

Russia and China push for multilateral agreements, as they have a densely supervised private sphere. At the same time, the West promotes multi-party governance, as its private sphere has greater autonomy and regulations lag behind them. While it may seem contradictory, thinking “big” in the coming years will require more intense work in the diplomatic and security spheres. The agreements will be made between small numbers of actors with shared visions around specific issues. Those agreements will eventually be linked to multiple areas of an issue like the agreement for the ethical use of artificial intelligence promoted by the Vatican, The Cybersecurity Tech Accord, which is supported by Microsoft and IBM. While multilateralism breathes through an artificial respirator, there is possibility for recovery through the emergence of multi-level collaborative agreements. They begin to be structured among those who consider themselves responsible shareholders of the international order under construction. ■

qualquer coisa que não seja expressamente proibida é permitida. A governança multilateral é diferente, pois pressupõe que qualquer coisa que não seja expressamente permitida é proibida. Nesse sentido, seus esforços para regular e controlar parecem ferramentas defensivas dos Estados.

Os regimes de controle de armas, especialmente os de armas nucleares, foram orientados por essa lógica. Pedir ao mundo que siga os parâmetros do século passado, diante da facilidade com que eles proliferam de novos avanços, não requer pensar em estruturas que funcionem sob lógicas de auto-restrição, em vez de controle ou sanções.

Rússia e China pressionam por acordos multilaterais, pois possuem uma esfera privada fortemente monitorada. Ao mesmo tempo, o Ocidente promove a governança por múltiplas partes, pois sua esfera privada tem maior autonomia e os regulamentos ficam obsoletos. Embora possa parecer contraditório, pensar “grande” nos próximos anos exigirá um trabalho mais intenso nas esferas diplomática e de segurança. Os acordos serão celebrado entre um pequeno número de atores com visões compartilhadas sobre questões específicas. Esses acordos acabam vinculados a várias áreas de uma questão, como o acordo para o uso ético da inteligência artificial promovido pelo Vaticano e que tem o apoio da Microsoft e da IBM, The Cybersecurity Tech Accord (Acordo Técnico em Segurança Cibernética). Embora o multilateralismo esteja por um fio, existe a possibilidade de recuperação através de acordos de colaboração em vários níveis. Eles começam a ser estruturados entre aqueles que se consideram stakeholders responsáveis pela ordem internacional em construção. ■



Sabrina Medeiros

Sabrina Evangelista Medeiros é Professora Associada de Relações Internacionais da Escola de Guerra Naval (EGN). Professora do Programa de Pós-Graduação em Estudos Marítimos (PPGEM). Coordenadora de pesquisa no Laboratório de Simulações e Cenários da EGN e de projeto junto ao Pro-Defesa IV/ CAPES-MD. Foi em misssão oficial pelo Ministério da Defesa como membro do Faculty do Colégio Interamericano de Defesa, da Organização dos Estados Americanos, entre 2013 e 2015. Doutora em Ciência Política pelo IUPERJ (IESP), com bolsa sandwish pelo DAAD no WZ-Berlim.

Sabrina Evangelista Medeiros is an Associate Professor of International Relations at the Naval War College (Escola de Guerra Naval - EGN). Professor of the Post-Graduate Program in Maritime Studies (PPGEM). Research coordinator at the Simulations and Scenarios Laboratory at EGN and project coordinator with Pro-Defense IV/CAPES-MD. On official mission by the Ministry of Defense she was member of the Faculty of the Inter-American Defense College, of the Organization of American States, between 2013 and 2015. PhD in Political Science from IUPERJ (IESP), with sandwich scholarship by DAAD at WZ-Berlin.

Danielle Jacon Ayres Pinto

Danielle Jacon Ayres Pinto é Professora Adjunta de Política Internacional e Segurança da Universidade Federal de Santa Catarina. Professora do Programa de Pós-Graduação em Relações Internacionais da UFSC, onde atua também como subcoordenadora. Pós-doutora em Ciências Militares, com ênfase em ciberdefesa e cibersegurança na Escola de Comando e Estado-Maior do Exército - ECEME. Doutora em Ciência Política pela UNICAMP e Mestre em Segurança e Estudos da Paz pela Universidade de Coimbra (UC). Coordenadora do Grupo de Pesquisa em Estudos Estratégicos e Política Internacional Contemporânea - GEPPIC.

Danielle Jacon Ayres Pinto is Assistant Professor of International Policy and Security at the Federal University of Santa Catarina (UFSC). Professor of the Post-Graduate Program in International Relations at UFSC, where she also works as sub-coordinator. Post-doctorate in Military Sciences, with emphasis on cyber defense and cybersecurity at the School of Command and General Staff of the Army - ECEME. PhD in Political Science from UNICAMP and Master in Security and Peace Studies from the University of Coimbra (UC). Coordinator of the Research Group on Strategic Studies and Contemporary International Politics - GEPPIC.

Geopolítica Digital e Segurança da Informação: por um framework multidimensional de políticas de cibersegurança

Digital Geopolitics and Information Security: for a multidimensional cybersecurity policy framework

Sabrina Medeiros

Escola de Guerra Naval

EGN - Brazilian Naval War College

Danielle Jacon Ayres Pinto

UFSC - Universidade Federal de Santa Catarina

UFSC - Santa Catarina Federal University)

A dimensão digital público-privada é cada vez mais híbrida na era da 4ª Revolução Industrial e esse é o principal desafio aos sistemas e subsistemas de defesa e segurança nacionais. A criação, de maneira incremental, de protocolos de compartilhamento de informação e proteção cibernética é, ao mesmo tempo, um obstáculo e um ativo das novas estruturas regulatórias que emergem. O motivo para isso é a progressiva demanda de sistemas mais seguros, ao mesmo tempo em que a velocidade dessas transformações inibe relações mais eficientes e resilientes.

Um caminho para solucionar esse dilema seria a cooperação em ecossistema da internet - que envolve governos, o setor privado, a sociedade civil, a Academia, a comunidade técnica, as organizações internacionais, os usuários - como forma de produzir arranjos variados de governança no setor. Essa cooperação seria mais eficaz ao seguir um modelo de tríplice-hélice, voltado

The public-private digital dimension is increasingly hybrid in the 4th Industrial Revolution era, and represents the main challenge to national defense and security systems and subsystems. The incremental creation of protocols for information sharing and cyber protection is both an obstacle and an asset of the new regulatory structures that are emerging. This is due to the progressive demand for safer systems, while the speed of these transformations inhibits more efficient and resilient relationships.

One way to solve this dilemma would be cooperation in the internet ecosystem - which involves governments, the private sector, civil society, the Academy, the technical community, international organizations and users, as a way to create varied governance arrangements in the sector. Such cooperation would be more effective when following a triple-helix model, directed towards innovation,

with a focus on the elaboration of public policies and strategies for the virtual sector, bringing the public sector, the private sector and civil society (represented by Academy and Non-State Organizations) to the debate.

Our analysis is based on the premise of geopolitical changes and international security brought by new technologies, especially for the field of defense and for the State. Hence, we present a proposal in the form of political dimensions to be achieved, as a way of increasing information security and promoting more stable geopolitical dynamics in the digital space.

In the field of geopolitics, territory, power and sovereignty were central elements of a good defense strategy for States in the international system. The new information and communication technologies (ICTs) and the expansion of cyberspace have redefined new nuances, so that two phenomena can be highlighted: 1) the emergence of new state and non-state players, with capacity for action in the national and international spheres and; 2) the uselessness of traditional resources of power to respond to this environment's new threats.

States with less capacity for traditional power resources now have the possibility of influencing the system, such is the case of Estonia, which now has almost 100% of its systems digitized and has become an efficient model of digital bureaucracy. On the other hand, North Korea, with limited economic resources, has managed to invest in a cyber system capable of harming other agents, as was the case of the attacks on the film "The Interview" (a satire of the North Korean leader Kin Jong-Un) released by Sony Corporation.

However, the most significant phenomenon was the spread of power, caused by the possibility that non-state palyers such as hackers, organized social groups, terrorist groups, etc. have the capacity for global influence. With cheap and easy access to ICTs, these players began to influence the central decision-making processes of the State, such as elections. They also caused damage to critical infrastructure through attacks with malware such as viruses, worms and others. An emblematic example of these attacks was the one perpetrated against Estonia by Russian nationalists in 2007 or the phenomenon of fake news, which redefined the outcome of the BREXIT referendum in 2016.

The virtualization of new cyber resources makes it difficult to determine the source of attacks, due to the redefinition of borders, sovereignty and territory. In addition, it is not possible to turn to the authorities for an answer to this type of crime. With this immateriality in the cyber environment, it became difficult to stop or fight this type of attacks. Traditional resources of power such as bombs, missiles and armies do not deter cyber resources. Thus, the resilience of cyber attack systems is greater than traditional tools allow to assess.

The Internet of Things (IoT), the State's digital bureaucracy, the greater interaction through social media and the highly computerized defense systems, raise the tendency to increase technological vulnerabilities. This does not mean that States should take a step back in their digitalization processes, since this is a one-way movement, but it does make it urgent to reframe their assets to cover these vulnerabilities. Faced with this

para a inovação, com foco na elaboração de política públicas e estratégias para o setor virtual, trazendo para o debate o setor público, o setor privado e a sociedade civil (representada pela Academia e Organizações não estatais).

Nossa análise parte da premissa de mudanças geopolíticas e de segurança internacional que as novas tecnologias trouxeram, em especial para o campo da defesa e para o Estado. Para isso, apresentamos uma proposta na forma de dimensões políticas a serem alcançadas, como forma de incrementar a segurança da informação e promover dinâmicas geopolíticas mais estáveis no espaço digital.

No campo da geopolítica, território, poder e soberania eram elementos centrais de uma boa estratégia de defesa dos Estados no sistema internacional. As novas tecnologias da informação e comunicação (TICs) e a expansão do ciberespaço redefiniram novos matizes, de modo que dois fenômenos podem ser ressaltados: 1) o surgimento de novos atores, estatais e não-estatais, com capacidade de ação na esfera nacional e internacional e; 2) a inutilidade dos tradicionais recursos de poder para responder às novas ameaças desse ambiente.

Estados com menor capacidade de recursos tradicionais de poder passaram a ter possibilidade de influenciar o sistema, como o caso da Estônia, que passou a ter quase 100% dos seus sistemas digitalizados e tornou-se um modelo eficiente de burocracia digital. Por outro lado, a Coréia do Norte, com limitados recursos econômicos, conseguiu investir em sistema cibernético capaz de produzir danos a outros agentes, como no caso dos ataques à empresa Sony Corporation, quando do lançamento do filme "A Entrevista" (sátira contra o líder norte-coreano Kin Jong-Un).

Porém, o fenômeno mais expressivo foi o da difusão do poder, causado pela possibilidade de atores não-estatais - hackers, grupos sociais organizados, grupos terroristas - terem capacidade de influência global. Com acesso barato e fácil sobre as TICs, esses atores passaram a influenciar processos decisórios centrais do Estado, como eleições. Também causaram danos às infraestruturas críticas, por meio de ataques com agentes maliciosos como vírus, worms e outros. Um exemplo emblemático desses ataques foi o perpetrado contra a Estônia por nacionalistas russos em 2007 ou o fenômeno das fake news, que redefiniu o resultado do plebiscito do BREXIT em 2016.

A virtualização dos novos recursos cibernéticos torna difícil determinar a origem de ataques, pela ressignificação das fronteiras, soberania e território. Além disso, não é possível recorrer às autoridades em busca de uma resposta para esse tipo de crime. Com essa imaterialidade no ambiente cibernético, tornou-se difícil barrar ou revidar ataques com esse caráter. Os tradicionais recursos de poder - como bombas, misseis, exércitos - não dissuadem os recursos cibernéticos. Assim, a resiliência de sistemas de ataque cibernético é maior do que as ferramentas tradicionais permitem avaliar.

A Internet das Coisas (IoT), a burocracia estatal digital, a maior interação através das mídias sociais e sistemas de defesa altamente computadorizados, provocam a tendência de ampliação das vulnerabilidades tecnológicas. Isso não significa que os Estados devam recuar em seus processos de digitalização, posto que esse é um movimento sem volta, mas que torna urgente a ressignificação de seus ativos para abrigar essas vulnerabilidades.

scenario of uncertainty, it is necessary to have a renewed understanding of geopolitics in the digital age and how to protect the system of interactions through more efficient regulatory frameworks among the States' structures.

We can say that, in this transition to a post-Westphalian world, new global geopolitical nuances are conditioned by relevant interdependence between players that is intensified by new technologies. A new understanding of traditional concepts will be a key exercise for public policy makers and enforcers in this field. Cooperation between public agents, private players, civil society and the academia seems to be the only effective solution to meet the security demands that lie ahead.

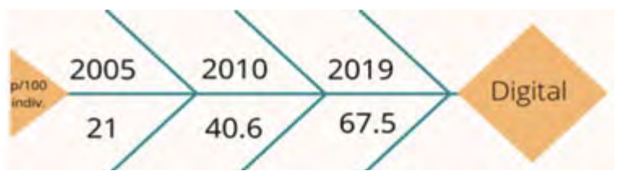
Information Security in Brazil

In the field of cyber defense, systems linked to the Internet of Things (IoT) involve capabilities to increase autonomy and reduce certain risks to human resources. On the other hand, cyber challenges have been addressed by agencies through content blocking and systems with marked access limitations. This situation can be highly damaging in terms of information exchange, as the operating environment is increasingly dependent on interoperability and interagency capabilities.

In other words, it is not possible to establish a governance scheme without considering a public-private, as well as a civil-military framework. While the European Union has developed a group of committees dedicated to the topic in partnership with civil society, this has not happened in any other regional regime. Although the presence of overlapping institutional arrangements can increase the complexity of the matter, the presence of some strategic assumptions can allow the alignment of State objectives with those manifested in the region.

In the Global South, high rates of social and development inequality and poverty have an even more pronounced effect on the need for digitalization. Aspects that weigh on this effect are the insertion in the public administration for the benefit of its own management and security and the participation of the population and its electronic literacy. Since 2005, the population with internet access in Brazil has tripled, guaranteeing access to more people and expanding the opportunities for participation, but also the vulnerabilities of this system have increased.

Figure 1: Number of individuals per 100 inhabitants with internet access, per year



UN Data. Prepared by the author.

Frente a esse cenário de incertezas, prescinde um entendimento renovado de geopolítica na era digital e como proteger o sistema de interações por meio de marcos regulatórios mais eficientes entre as estruturas dos Estados.

Podemos dizer que, nessa transição para um mundo pós-Vestfaliano, novos matizes geopolíticos mundiais são condicionados por relevante interdependência entre atores e, intensificada a partir das novas tecnologias. Novas compreensões de tradicionais conceitos serão exercícios fulcrais para os elaboradores e executores das políticas públicas na matéria. A cooperação entre agentes públicos, agentes privados, sociedade civil e academia parece ser a única solução eficaz para conseguir atender às demandas de segurança que estão por vir.

Segurança da Informação no Brasil

No campo da defesa cibernética, sistemas atrelados à Internet das Coisas (IoT) envolvem capacidades de incremento da autonomia e da diminuição de determinados riscos aos recursos humanos. Por outro lado, os desafios cibernéticos têm sido tratados pelas agências por meio de bloqueios de conteúdo e sistemas com acentuada limitação de acesso. Essa conjuntura pode ser altamente prejudicial em matéria de troca de informações, já que o ambiente operacional é crescentemente dependente de interoperabilidade e capacidades interagências.

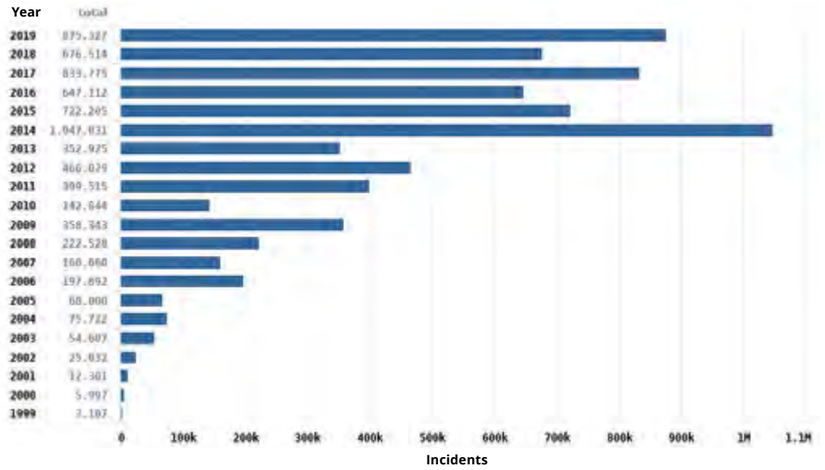
De outro modo, não é possível estabelecer um esquema de governança sem considerar um enquadramento público-privado, assim como, civil-militar. Enquanto a União Europeia desenvolveu um grupo de comitês dedicados ao tema em parceira com a sociedade civil, isso não aconteceu em nenhum outro regime regional. Embora a presença de arranjos institucionais sobrepostos possa ampliar a complexidade da matéria, a presença de alguns pressupostos estratégicos pode permitir alinhavar os objetivos estatais àqueles manifestados na região.

No Sul-Global, os altos padrões de desigualdade social, pobreza e desenvolvimento acarretam um efeito ainda mais acentuado quanto às necessidades de digitalização. Além da inserção na administração pública em benefício de sua própria gestão e segurança, pesam os quesitos de participação e alfabetização eletrônica da população. Desde 2005, o número de habitantes com acesso à internet no Brasil triplicou, garantindo acesso a mais pessoas e ampliando as oportunidades de participação, assim como cresceram as vulnerabilidades desse sistema.

Figura 1: Relação número de indivíduos por 100 habitantes com acesso à internet, por ano

UN Data. Elaboração própria.

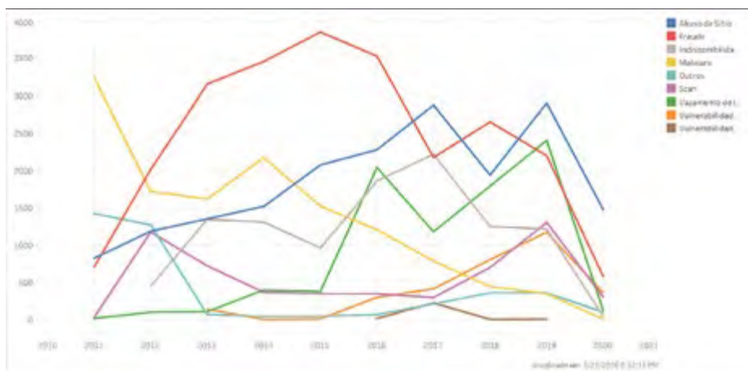
Figure 2: Total incidents reported to CERT.br per Year (CERT - Center for the Study, Response and Treatment of Security Incidents in Brazil)



Cert.br

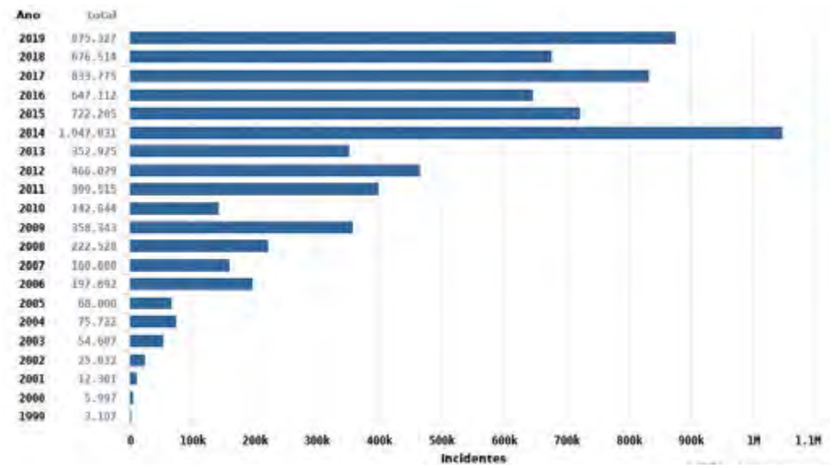
This means that the increase in internet access also increased the number of virtual incidents, which in Brazil are monitored by CERT.br. CERT is one of the agencies responsible for implementing the objectives associated with the Federal Public Administration's Information and Communications Security and Cybersecurity Strategy (Portaria CDN n.14, of May 11, 2015). For the first time, this document consolidated the attributions of Security of Information and Communications (SIC) and Cybersecurity (SegCiber) having as its controlling body the GSI/PR (Institutional Security Office of Brazil, under the President's office). The document's Strategic Map provides that the scope must have a dual purpose: to guarantee the security of State information and to increase awareness about information security and cybersecurity. The implementation of a strategy and respective bodies seems to have eased the pressure revealed in the progressive increase of cases, but which still reached relatively high numbers in 201

Figure 3: Incidents



CERT.br

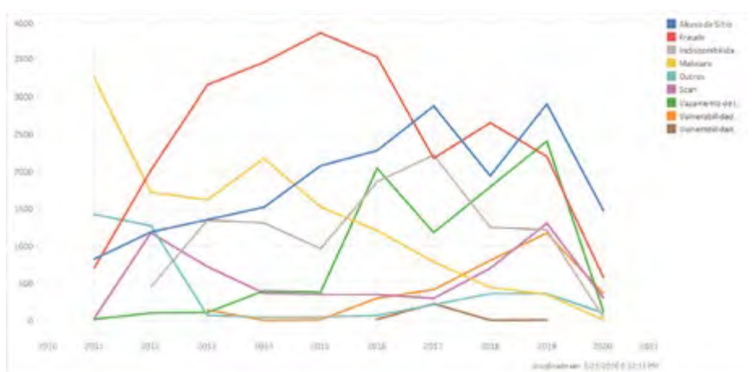
Figura 2: Total de incidentes reportados ao CERT.br por Ano



Cert.br

Ou seja, com o aumento do acesso à internet, também é visível o aumento de incidentes virtuais, que no Brasil é monitorado pelo CERT.br. Essa é uma das agências responsáveis pela implementação dos objetivos associados à Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal (Portaria CDN n.14, de 11 de maio de 2015). O documento consolidou pela primeira vez atribuições de Segurança da Informação e Comunicações (SIC) e de Cibersegurança (SegCiber) tendo como órgão controlador o GSI/PR (Gabinete de Segurança Institucional da Presidência da República). O mapa estratégico do mesmo documento prevê que o alcance deve ter dupla finalidade: garantir a segurança das informações de Estado e ampliar a consciência sobre segurança da informação e segurança cibernética. A implementação de uma estratégica e órgãos respectivos parece ter diminuído a pressão revelada no aumento progressivo de casos, mas que ainda chegaram a números relativamente altos em 2019.

Figura 3: Incidentes

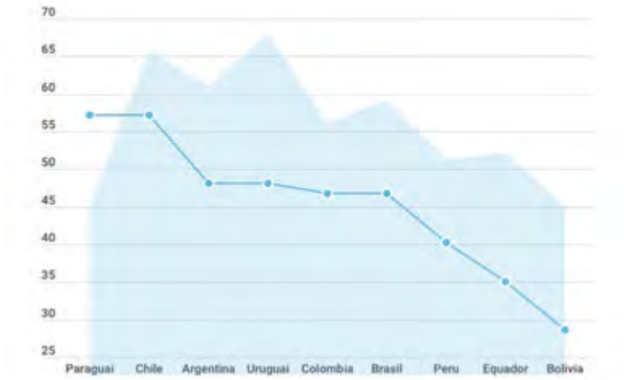


CERT.br

The Information Security Management Committee (CGSI), linked to the Information Security Department (SIC) of the GSI/PR, was created based on Decree 9637, of December 26, 2018, that installed the National Information Security Policy (PNSI), instructing the joint and inter-ministerial development of a National Information Security Strategy. Among the objectives of the PNSI are: the standardization of communication systems, the creation of common guidelines for information security and the increase in electronic access to State services by citizens.

Therefore, it is possible to measure governance in the digital age as manifested by the use of innovation to benefit development. The focus is on demands related to information security for stable political structures, in a free and safe environment. In the graph below, it is possible to comparatively view the state of the art in cybersecurity in South America, based on data collected by the National Cyber Security Index (NCSI).

National Cyber Security Index 2020



Considering three central pillars of threats, each with four criteria, the NCSI determines the degree of cybersecurity in each country. Brazil ranks below countries like Paraguay, Uruguay, Chile and Argentina, which demonstrates the need to improve Brazilian digital governance processes, emphasizing solid public policies that guarantee protection of citizens' data, in addition to greater resilience of the country's critical structures.

For that, some policy options can be presented.

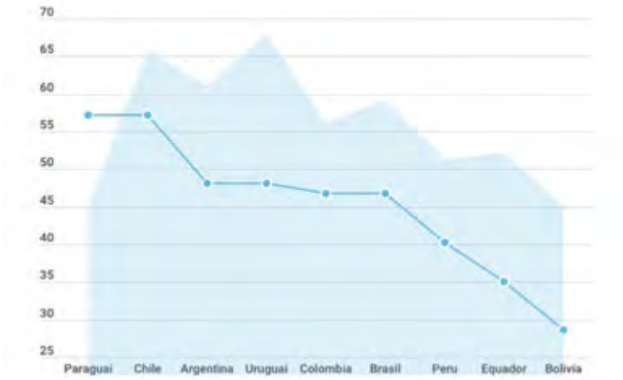
Policy Options

The Global Cybersecurity Index, as part of the International Telecommunications Union (ITU-UN), analyzes the cyber security of member states through 5 pillars: legal, technical, organizational, capacity building, and cooperation. Such pillars invoke the multiple participation of players, so that there are regulatory structures adaptable to the advances necessary to expand the uses of the internet, in its various forms, from defense to citizen participation.

O Comitê Gestor de Segurança da Informação (CGSI), vinculado ao Departamento de Segurança da Informação (SIC) do GSI/PR, foi criado a partir do Decreto 9637, de 26 de dezembro de 2018, pelo qual se instituiu a Política Nacional de Segurança da Informação (PNSI), dando instruções para a elaboração conjunta e interministerial de uma Estratégia Nacional de Segurança da Informação. Dentre os objetivos da PNSI estão: a padronização de sistemas de comunicação, a criação de diretrizes comuns para a segurança da informação, e o aumento do acesso eletrônico a serviços do Estado pelos cidadãos.

Portanto, é possível dimensionar a questão da governança na era digital como manifestada pelo alinhamento dos usos da inovação em benefício do desenvolvimento. O foco está direcionado às demandas afetas à segurança da informação para estruturas políticas estáveis, em ambiente livre e seguro. No gráfico a seguir é possível visualizar comparativamente o estado da arte em cibersegurnaça na região da América do Sul, a partir dos dados coletados pelo National Cyber Security Index (NCSI).

National Cyber Security Index 2020



Considerando três pilares centrais de ameaças, cada um com quatro critérios, o NCSI determina o grau de segurança cibernética de cada país. O Brasil está atrás de países como o Paraguai, o Uruguai, o Chile e a Argentina, o que demonstra a necessidade de aprimorar os processos de governança digitais brasileiros, dando ênfase a políticas públicas sólidas que garantam proteção dos dados dos cidadãos, além de maior capacidade de resilência das estruturas críticas do país.

Para isso, algumas opções políticas podem ser apresentadas.

Opções Políticas

O Global Cybersecurity Index, como parte do *International Telecommunications Union (ITU - UN)* tem como método de análise da cibersegurança de Estados-membros a avaliação por meio de 5 pilares: o legal; o técnico; o organizacional; o desenvolvimento de capacidades; e a cooperação. Tais pilares invocam a participação múltipla de atores, de modo que haja estruturas regulatórias adaptáveis aos avanços necessários para a ampliação dos usos da internet, em suas variadas formas, desde a defesa até a participação cidadã.

Below, we present some of the possible ways for Brazil to participate in this arena with ease, in order to have the above mentioned pillars as a priority in each of the proposed dimensions:

Figure 4: Cyber Policies' Dimensions

Prepared by the author

1) International Regimes: reinforcement of regional, interregional and international arrangements. The ability to demonstrate trust can increase the chances of participating in regimes that strengthen human resources, share tools and systems of surveillance and combat, both of civil and military character. In addition, access to funds and financing from these regimes can expand economic opportunities for the innovation sector.

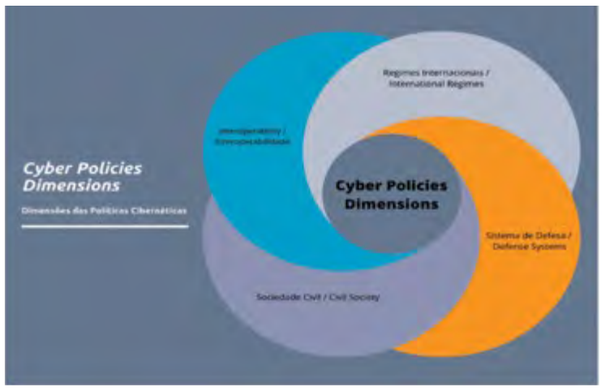
2)Defense Systems: division between defense systems, critical infrastructure and social systems (public services and public-private partnerships). The division of duties within the federal and federative system between separate control and protection structures can benefit the efficiency of the processes provided for in the relevant policies. This way, it is possible to coordinate tasks that may include companies certified for good practices such as "data ownership respectful", enabling to compose subsystems of control and access to citizens and protection of services.

3) Civil Society: expansion of civil society participation committees. Hierarchical structures do not always offer conditions for models of civil society participation. When national security does not allow the participation of organizations and interest groups associated with cybersecurity, it is necessary to create State councils to increase policies and legal frameworks. In addition, a sector-based reporting system can enhance the ability of governments to analyze potential crises and risks to society, despite the government's role of protection, including regulations on the protection of personal data.

4) Interoperability: Interoperability and inter-agency relationships. The use of common protocols, the adaptation of internal regulatory mechanisms and the standardization of parameters and associated policies can increase resilience, especially

Apresentemos, pois, alguns dos caminhos possíveis para que o Brasil participe dessa arena com desenvoltura, de modo a ter os pilares acima mencionados como prioridade em cada uma das dimensões propostas:

Figura 4: Dimensões das Políticas Cibernéticas



Elaboração Própria

1) Regimes Internacionais: reforço aos arranjos regionais, interregionais e internacionais. A capacidade dos atores de demonstrarem confiança pode aumentar as chances de participação em regimes que fortaleçam recursos humanos, compartilhem ferramentas e sistemas de vigilância e combate, de caráter civil e militar. Além disso, o acesso aos fundos e financiamentos desses regimes pode ampliar oportunidades econômicas para o setor de inovação.

2) Sistemas de Defesa: divisão entre os sistemas de defesa, infraestruturas críticas e sistemas sociais (serviços públicos e parcerias público-privadas). A divisão de atribuições dentro do sistema federal e federativo entre estruturas de controle e de proteção separadas pode beneficiar a eficiência dos processos previstos nas políticas pertinentes. Desse modo, é possível coordenar os trabalhos que incluam empresas certificadas por boas práticas de "data ownership respectful", podendo compor subsistemas de controle, acesso ao cidadão e proteção de serviços.

3) Sociedade Civil: ampliação de comitês de participação da sociedade civil. As estruturas hierárquicas nem sempre oferecem condições de abrigar modelos de participação da sociedade civil. Quando a segurança nacional não permite a participação de organizações e grupos de interesse associados à segurança cibernética, é preciso criar nas instituições do Estado conselhos próprios para incremento de políticas e marcos legais. Além disso, um sistema de reporte setorizado pode ampliar a capacidade dos governos de analisar potenciais crises e riscos à sociedade, em que pese o papel do governo de proteger, incluindo as regulamentações quanto à proteção de dados pessoais.

4) Interoperabilidade: Interoperabilidade e relações interagência. A utilização de protocolos comuns, a adaptação de mecanismos regulatórios internos e a normatização

based on the registration and sharing of good practices. In addition, it is possible to optimize joint command and control centers for the centralization of information and response actions when the matter reaches different entities - as is the case with attacks on critical infrastructures.

These dimensions of cybersecurity policies are regulatory, organizational, cooperative and techno-operative contributions necessary to create a resilient governance system connected to the wide capillarity of the problem at hand, which defines a new era.

The goals associated with privacy-enhancement e-government systems are critical and deserve special attention and significant external controls. In the case of Brazil, the General Data Protection Law (LGPD) is expected to come into effect in 2021, due to political reasons. The creation of previous regulatory frameworks in Germany (Bundesdatenschutzgesetz - BDSG) and in the European Union, places Brazil as a potential partner in the matter, given that companies and human resources will have to be certified.

Within this approach, an initiative aimed at improving the Brazilian cybersecurity system could be carried out with the European Union and Member States. Through ENISA, one of the priority objectives of the European Union is the support of States in the development of capacities and guidance of policies related to information security systems. Some of the guidelines in progress may help Brazil raise the level of its participation in collaborative networks, its access to specific funds and the qualifiers of trust of its institutions and processes.

Conclusions

The criteria associated with the proposed scheme provoke some essential conditions for this synergy between the four dimensions. The first of these is "openness", in which values aimed at an open network are generated from universal technical standards, free communication, open markets and internet governance through institutions open to participation.

Other values such as pluralism, the multiplicity of players and the public interest prevail in the overlapping frameworks, between the UN and related regimes. This set of shared values ends up fine-tuning the conceptual elements that govern the operating social system, even if invisibly, such as the principle of neutrality, in which the system should not allow discrimination of content.

In addition to operating social systems, the incorporation of new 5G systems, IoT, public-private interdependence relationships, must take into account the strategic options available, associating the possible risks related to dependency and sovereignty, with the possibility of making systems more vulnerable due to obsolescence.

Thus, the reliability of partners, the development of stable collaboration networks and the integrated technological improvement, are assets that will distance those who remain isolated. Otherwise, economies with less regulatory power will be potential

de parâmetros e políticas associadas pode aumentar a resiliência, sobretudo a partir do registro e compartilhamento de boas práticas. Além disso, é possível otimizar centros de comando e controle conjuntos na centralização de informações e nas ações de resposta quando a matéria alcançar diversos entes – como é o caso de ataques às infraestruturas críticas.

Essas, que aqui caracterizamos como dimensões das políticas de cibersegurança, são aportes regulatórios, organizacionais, cooperativos e tecno-operativos necessários à criação de um sistema de governança resiliente e com conexão à ampla capilaridade do problema em lide, que define uma nova era.

As metas associadas aos sistemas de "privacy-enhancement e-government" são críticas e merecem também atenção especial e controles externos significativos. No caso do Brasil, a Lei Geral de Proteção de Dados (LGPD), tem vigência prevista para 2021, devido a motivações políticas. A criação de marcos regulatórios anteriores na Alemanha (Bundesdatenschutzgesetz – BDSG) e na União Europeia, colocam o Brasil como potencial parceiro na questão, dado que empresas e recursos humanos terão que certificar-se.

Dentro dessa abordagem, uma iniciativa voltada ao aprimoramento do sistema brasileiro de cibersegurança poderia ser feita com a União Europeia e seus Estados-mebros. Por meio da ENISA, um dos objetivos prioritários da União Europeia é o apoio de Estados terceiros no desenvolvimento de capacidades e orientacão de políticas afetas aos sistemas de segurança de informação. Algumas das pautas em curso podem auxiliar o Brasil a elevar o patamar de sua participação em redes colaborativas e no acesso a fundos específicos, qualificadores de confiança de suas instituições e processos.

Conclusões

Os critérios associados ao esquema proposto provocam algumas condições essenciais para essa sinergia entre as quatro dimensões. A primeira delas é a "abertura" (ou openness), em que valores voltados a uma rede aberta são gerados a partir de padrões técnicos universais, comunicação livre, mercados abertos e governança da internet por meio de instituições abertas à participação.

Outros valores como o pluralismo, a multiplicidade de atores e o interesse público vigoram nos *frameworks* sobrepostos, entre a ONU e regimes conexos. Esse conjunto de valores compartilhados acaba for afinar os elementos conceituais que regem o sistema social em operação, ainda que invisível, como o princípio da neutralidade, em que o sistema não deve permitir discriminação de conteúdos.

Para além de sistemas sociais em operação, a incorporação de sistemas novos de 5G, de IoT, de relações de interdependência público-privadas, deve levar em conta as opções estratégicas disponíveis, relacionando os riscos eventuais afetos à dependência e soberania, com a possibilidade de deixar que sistemas sejam ainda mais vulneráveis pela obsolescência.

Assim, a confiabilidade de parceiros, o desenvolvimento de redes de colaboração estáveis

sources of instability and change in the geopolitical locus, since the forces active in dispute processes in the cybersecurity scenario are not necessarily those whose power variables are known. Nevertheless, the march towards the virtualization of societies cannot be interrupted and the goal for domestic knowledge will continue to be the paradigm to be pursued. ■

References

Ayres Pinto Danielle Jacon; Freitas, Riva Sobrado de; Pagliari, Graciela de Conti, **Fronteiras Virtuais: um debate em segurança e soberania do Estado**. In Maria Raquel Freire., Danielle Jacon Ayres Pinto e Daniel Chaves (org.) Fronteiras Contemporâneas comparadas: Desenvolvimento, Segurança e Cidadania. Amapá: Editora UNIFAP, 2018, p. 39-52.

Brasil, **Doutrina Militar de Defesa Cibernética**. Ministério da Defesa: Brasília, 1ª Edição, 2014. In: https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_ cibernetica_1_2014.pdf (Accessed 20May20)

Brasil. **Decreto presidencial n.9.637 de 26 de dezembro de 2018**. (Brasília: Presidência da República, 2018. In: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/ Decreto/D9637.htm (Accessed 20May20)

Cavelty, Mirian. **The Militarization of Cyber Security as a Source of Global Tension**. Strategic Trends 2012: Key Developments in Global Affairs. In Andrea Baumann e Daniel Prem Mahadevan Möckly. Zurique: Center for Security Studies (CSS), 2012. (Accessed 20May20)

CERT - **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil Estatísticas de Incidentes.** In: https://cert.br/stats/ (Accessed 20May20)

ENISA - EUROPEAN UNION AGENCY FOR CYBERSECURITY. **ENISA Programming Document 2020–2022**. November, 2019. In: https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-202020132022 (Accessed 20May20)

Huriel, Louise M.; Lobato, Luiza. **A Strategy for Cybersecurity Governance in Brazil** Instituto Igarapé. 2018. In: https://igarape.org.br/wp-content/uploads/2019/01/A-Strategy-for-Cybersecurity-Governance-in-Brazil.pdf (Accessed 20May20)

Andress, Jason; Winterfeld, Steve. **Cyber Warfare Techniques, Tactics and Tools**. Waltham: Elsevier, 2011.

Kurbalija, Jovan . **Introducción a la gobernanza de la Internet**. Malta: DiploFondation. 7ª edição, 2016.

Mendes, Cintiene; Paiva, Ana Luiza B; Medeiros, Sabrina. **Policy Diffusion by means of Defense and Security Simulations and the uses of agent-based modelling**. Revista da EGN. v.26, n.1, 2020.

Menezes, Karina. **LGPD em vigor ainda em 2020?** IdBlog. Compliance. 25/05/2020. In: https://blog.idwall.co/category/outros/compliance/ (Accessed 26May20)

e o aprimoramento tecnológico integrado, são ativos que distanciarão aqueles que permanecerem isolados. De outro modo, economias com menor poder de regulação serão potencialmente fontes de instabilidade e mudança de lócus geopolítico, posto que as forças ativas em processos de disputa no cenário de cibersegurança não são necessariamente aquelas cujas variáveis de poder são conhecidas. Não obstante, a marcha em direção à virtualização de sociedades não poderá ser interrompida e a meta por conhecimentos autóctones continuará a ser o paradigma a ser buscado. ■

Referências

Ayres Pinto Danielle Jacon; Freitas, Riva Sobrado de; Pagliari, Graciela de Conti, **Fronteiras Virtuais: um debate em segurança e soberania do Estado**. In Maria Raquel Freire., Danielle Jacon Ayres Pinto e Daniel Chaves (org.) Fronteiras Contemporâneas comparadas: Desenvolvimento, Segurança e Cidadania. Amapá: Editora UNIFAP, 2018, p. 39-52.

Brasil, **Doutrina Militar de Defesa Cibernética**. Ministério da Defesa: Brasília, 1ª Edição, 2014. In: https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/ doutrina/md31_m_07_defesa_ cibernetica_1_2014.pdf (Accessed 20May20)

Brasil. **Decreto presidencial n.9.637 de 26 de dezembro de 2018**. (Brasília: Presidência da República, 2018. In: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/ Decreto/D9637.htm (Accessed 20May20)

Cavelty, Mirian. **The Militarization of Cyber Security as a Source of Global Tension**. Strategic Trends 2012: Key Developments in Global Affairs. In Andrea Baumann e Daniel Prem Mahadevan Möckly. Zurique: Center for Security Studies (CSS), 2012. (Accessed 20May20)

CERT - **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil Estatísticas de Incidentes.** In: https://cert.br/stats/ (Accessed 20May20)

ENISA - EUROPEAN UNION AGENCY FOR CYBERSECURITY. **ENISA Programming Document 2020–2022**. November, 2019. In: https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-202020132022 (Accessed 20May20)

Huriel, Louise M.; Lobato, Luiza. **A Strategy for Cybersecurity Governance in Brazil** Instituto Igarapé. 2018. In: https://igarape.org.br/wp-content/uploads/2019/01/A-Strategy-for-Cybersecurity-Governance-in-Brazil.pdf (Accessed 20May20)

Andress, Jason; Winterfeld, Steve. **Cyber Warfare Techniques, Tactics and Tools**. Waltham: Elsevier, 2011.

Kurbalija, Jovan . **Introducción a la gobernanza de la Internet**. Malta: DiploFondation. 7ª edição, 2016.

Mendes, Cintiene; Paiva, Ana Luiza B; Medeiros, Sabrina. **Policy Diffusion by means of Defense and Security Simulations and the uses of agent-based modelling**. Revista da EGN. v.26, n.1, 2020.

Pagliari, G.D.C.; Ayres Pinto, D. J; Viggiano, J. **Mobilização nacional, ameaças cibernéticas e redes de interação num modelo de tríplice hélice estratética: um estudo prospectivo.** In.: OLIVEIRA, M.G. (Org.) Defesa Cibernética e Mobilização Nacional. Recife: Editora UFPE, 2020, p. 135-174.

National Cyber Security Index (NCSI). https://ncsi.ega.ee/compare/ (Accessed 19May20)

Tosi, Scott J. **O apoio cibernético nas operações de combate da Coreia do Norte**. Military Review. Army University Press. v.1, n. 2018, p. 31-40. https://www.armyupress.army.mil/Journals/Edicao-Brasileira/Arquivos/Primeiro-Trimestre-2018/O-Apoio-Cibernetico-nas-Operacoes-de-Combate-da-Coreia-do-Norte/ (Accessed 18May20)

UN. **DATA per country.** http://data.un.org/en/iso/br.html (Accessed 20May20)

UNESCO. Glossary – Internet Governance. https://en.unesco.org/glossaries/igg/groups/1.%20Internet%20governance%20general (Accessed 26May20)

Menezes, Karina. **LGPD em vigor ainda em 2020?** IdBlog. Compliance. 25/05/2020. In: https://blog.idwall.co/category/outros/compliance/ (Accessed 26May20)

Pagliari, G.D.C.; Ayres Pinto, D. J; Viggiano, J. **Mobilização nacional, ameaças cibernéticas e redes de interação num modelo de tríplice hélice estratética: um estudo prospectivo.** In.: OLIVEIRA, M.G. (Org.) Defesa Cibernética e Mobilização Nacional. Recife: Editora UFPE, 2020, p. 135-174.

National Cyber Security Index (NCSI). https://ncsi.ega.ee/compare/ (Accessed 19May20)

Tosi, Scott J. **O apoio cibernético nas operações de combate da Coreia do Norte**. Military Review. Army University Press. v.1, n. 2018, p. 31-40. https://www.armyupress.army.mil/Journals/Edicao-Brasileira/Arquivos/Primeiro-Trimestre-2018/O-Apoio-Cibernetico-nas-Operacoes-de-Combate-da-Coreia-do-Norte/ (Accessed 18May20)

UN. **DATA per country.** http://data.un.org/en/iso/br.html (Accessed 20May20)

UNESCO. Glossary – Internet Governance. https://en.unesco.org/glossaries/igg/groups/1.%20Internet%20governance%20general (Accessed 26May20)

Eduardo Magrani

Doutor (Ph.D.) Eduardo Magrani é, atualmente, fellow da Fundação Konrad Adenauer. Professor de Direito e Tecnologia e Propriedade Intelectual. Presidente do Instituto Nacional de Proteção de Dados do Brasil. Autor da Trilogia da Cultura Digital "Democracia, Hiperconectividade e Ética: uma trilogia sobre cultura digital".

Ph.D. Eduardo Magrani is currently Fellow at the Konrad Adenauer Stiftung. Professor of Law and Technology and Intellectual Property. President of the National Institute for Data Protection in Brazil. Author of the Digital Culture Trilogy "Democracy, Hyperconnectivity and Ethics: a trilogy on digital culture".

Ameaças da internet das coisas (iot) em uma sociedade tecnorregulada - o novo desafio jurídico da revolução da informação

Threats of the internet of things in a techno-regulated society – a new legal challenge of the information revolution

Eduardo Magrani

Fellow da Fundação Konrad Adenauer

Fellow at the Konrad Adenauer Stiftung

Introdução

A tecnologia tem mudado rapidamente a maneira como interagimos com o mundo ao nosso redor. As empresas, com o objetivo de atender às novas demandas dos consumidores, estão desenvolvendo produtos com interfaces tecnológicas que seriam inimagináveis dez anos atrás.

Sistemas automatizados acendem luzes e aquecem refeições enquanto você está a caminho de casa, pulseiras e palmilhas inteligentes compartilham com seus amigos a distância que você percorreu a pé ou de bicicleta (Nike Running, 2012); sensores avisam automaticamente os agricultores quando um animal está doente ou prenha (Computer Science Zone, 2015). Estes exemplos são todas manifestações associadas ao conceito de "Internet das Coisas" ("IoT").

Não há consenso sobre o que a Internet das Coisas (IoT) representa e não existe um conceito bem definido e unânime para a IoT. Genericamente, pode ser entendida como

Introduction

Technology has been rapidly changing the way we interact with the world around us. Companies, aiming to meet new consumer demands, are developing products with technological interfaces that would have been unimaginable a decade ago.

Automated systems turn on lights and warm meals as you leave your work, intelligent bracelets and insoles share with your friends how much you have walked on foot or ridden on a bike (Nike Running, 2012); sensors that automatically warn farmers when an animal is sick or pregnant (Computer Science Zone, 2015). These examples are all manifestations associated with the concept of "Internet of Things" ("IoT").

There are strong disagreements regarding what IoT stands for. There is no such thing as a unanimously well-defined concept for IoT. More broadly, it can be understood as an interconnected environment of physical objects linked to the Internet through

small built-in sensors, that creates a computer-based ubiquitous ecosystem, in order to facilitate and introduce functional solutions for daily routines and activities (Federal Trade Commission, 2015; NIC.br, 2014).

Even though it might resemble a futuristic scenario, this kind of technology is already part of the present. Bracelet computers, smart watches, health devices, smart houses, cars and smart cities, are all manifestations of the "Internet of Things" (Federal Trade Commission, 2015).

However, despite the present context, it is still a fairly recent culture based on the new relations we are forging with machines and interconnected devices. It is estimated that the number of "things" connected to the Internet have surpassed the number of people, what further confirms this new human-machine relationship. Estimations (Barker, 2014) tell that in 2020 the quantity of interconnected objects will overcome 25 billion, being able to reach the mark of 50 billion smart devices.

All this hyperconnectivity and continuous interaction between gadgets, sensors and people, points to the rise of data and logs being produced, stored and processed both virtually and physically. On one hand, this may produce innumerous benefits to consumers. Interconnected health devices allow constant and efficient monitoring as well as greater interaction between doctor and patient. Residential automated systems will enable users to send messages to their home devices even before they arrive, performing actions such as opening the garage door, turning off alarms, turning on the lights, preparing a hot bath, cooking dinner, playing that special song, and even shifting the rooms` temperature. Moreover, what the future holds for IoT is yet to be discovered.

On the other hand, the large amount of connected apparatuses will accompany us daily and regularly in our everyday life, and therefore collecting, transmitting, storing and sharing an enormous amount of data – most of it strictly private and even intimate.

With the exponential rise of such devices, we should also pay attention to the potential risks and challenges that this increase may bring to fundamental rights. Those challenges can be investigated through a wide variety of lenses. For example, the new technological scenario is occasioning several changes on regulation and in jurisprudence of consumer's law. Nevertheless, despite the variety of areas covered by this discussion, the analysis intended in this paper will try to investigate those challenges especially through the lens of privacy, freedom of expression and protection of personal data.

Although some of the threats and risks of the IoT scenario do not seem novel, considering how recent this context of hyperconnectivity is, we are not yet fully conscious of the possible damages that are dramatically enhanced in an IoT environment nor do we have sufficient legal regulation to avoid losses that could arise from the unclear processes of storage, treatment and sharing of our personal data in the context of IoT.

um ambiente interconectado de objetos físicos vinculados à internet por meio de pequenos sensores embutidos, que cria um ecossistema informatizado e onipresente para facilitar e introduzir soluções funcionais para rotinas e atividades diárias (Federal Trade Comissão, 2015; NIC.br, 2014).

Embora possa parecer um cenário futurista, esse tipo de tecnologia já faz parte da atualidade. Pulseiras computadorizadas, relógios inteligentes, dispositivos de saúde, casas inteligentes, carros inteligentes e cidades inteligentes são manifestações da "Internet das Coisas" (Federal Trade Commission, 2015).

No entanto, apesar do contexto atual, ainda é uma cultura relativamente recente baseada nas novas relações que estamos criando com máquinas e dispositivos interconectados. Estima-se que o número de "coisas" conectadas à internet superou o número de pessoas, o que confirma ainda mais essa nova relação homem-máquina. Estimativas (Barker, 2014) predizem que em 2020 a quantidade de objetos interconectados superará 25 bilhões, podendo atingir a marca de 50 bilhões de dispositivos inteligentes.

Toda essa hiperconectividade e interação contínua entre dispositivos, sensores e pessoas, aponta para o aumento de dados e logs sendo produzidos, armazenados e processados virtualmente e fisicamente. Por um lado, isso pode produzir inúmeros benefícios para os consumidores. Dispositivos de saúde interconectados permitem monitoramento constante e eficiente, além de maior interação entre médico e paciente. Os sistemas automatizados residenciais permitirão que os usuários enviem mensagens para seus dispositivos domésticos antes mesmo de chegarem em casa, realizando ações como abrir a porta da garagem, desligar alarmes, acender as luzes, preparar um banho quente, preparar o jantar, tocar aquela música especial e até mesmo alterar a temperatura dos cômodos. No entanto, ainda há muito a descobrir sobre o que o futuro reserva para a IoT.

Por outro lado, a grande quantidade de aparelhos conectados nos acompanhará diariamente e regularmente em nossa vida cotidiana, coletando, transmitindo, armazenando e compartilhando uma enorme quantidade de dados - a maioria estritamente privada e até íntima.

Com o crescimento exponencial de tais dispositivos, devemos também prestar atenção aos possíveis riscos e desafios que esse aumento pode trazer para os direitos fundamentais. Esses desafios podem ser apurados através de uma ampla variedade de lentes. Por exemplo, o novo cenário tecnológico está ocasionando várias mudanças na regulamentação e na jurisprudência do direito do consumidor. No entanto, apesar da variedade de áreas cobertas por esta discussão, a análise pretendida neste artigo tentará avaliar esses desafios, especificamente através das lentes da privacidade, liberdade de expressão e proteção de dados pessoais.

Embora algumas das ameaças e riscos do cenário de IoT não sejam novidade, devemos considerar quão recente é esse contexto de hiperconectividade e que ainda não estamos totalmente cientes dos possíveis danos que são dramaticamente aumentados em um ambiente de IoT. Tampouco temos regulamentação legal suficiente para evitar perdas que possam surgir dos processos incertos de armazenamento, tratamento e compartilhamento de nossos dados pessoais no contexto da IoT.

Besides, while we are failing on having an adequate regulatory framework upheld by the law, we are experiencing a strong auto-regulation from the market, a regulation that, many times, is made through code design[1], what we may call a techno-regulation[2]. It is crucial to analyze what the new legal challenges are in this context that forces us to think about an adequate legal framework to respond to those challenges.

Based on a theoretical and constitutional approach to current technological evolution with particular regard to the Internet of Things and its privacy dimension, the purpose of this preliminary effort is to trigger further reflections about the regulatory challenges posed by greater (inter)connectivity.

A techno-regulated society

Considering the characteristics pointed out by cyber-optimistic scholars such as Manuel Castells and Yochai Benkler, we may say that new information and communication technologies have been seen as the great promise for several different areas. Nonetheless, this potential can be considerably reduced depending on how new technological layers are built upon certain infrastructures, therefore allowing users to explore more or less actions and depending on criteria for access and content filtering by algorithms[3]. Besides, private companies are developing technology without paying adequate attention to fundamental rights such as privacy and security. Without proper care, this procedure can bring serious risks to consumers (Almeida, Doneda, & Monteiro, 2015).

We are living a moment of intense techno-regulation, commodification of personal data, and no strong legal apparatus to protect human and fundamental rights such as privacy protection. It is crucial that we stop to think about the role that the law should play in this context, especially in countries like Brazil that, for example, still don't have a solid and comprehensive data protection law (Pagallo, 2013).

Only recently has Internet diffusion become part of the Brazilian context. According to "CETIC Domicílios" report, 51% (85,9 million) of Brazilians are Internet users and within that statistics, 77% of them range from 16 to 24 years old (Center for Educational Computing, 2009). The current Brazilian legislation has already contemplated some aspects of Internet access and uses.

Even though Internet-related regulations such as the Marco Civil da Internet try to uphold the value and potential of the Internet as well as stipulate practices that seek to protect constitutional rights, the current autoregulation based on code design[4] has

1 https://www.orbit-rri.org/journal/volume-one/issue-1/threats-internet-things-techno-regulated-society-new-legal-challenge-information-revolution/#post-3450-footnote-7
2 https://www.orbit-rri.org/journal/volume-one/issue-1/threats-internet-things-techno-regulated-society-new-legal-challenge-information-revolution/#post-3450-footnote-8
3 https://www.orbit-rri.org/journal/volume-one/issue-1/threats-internet-things-techno-regulated-society-new-legal-challenge-information-revolution/#post-3450-footnote-27
4 https://www.orbit-rri.org/journal/volume-one/issue-1/threats-internet-things-techno-regulated-society-new-legal-challenge-information-revolution/#post-3450-footnote-37

Além disso, embora não consigamos manter uma estrutura regulatória adequada garantida por lei, estamos vivenciando uma forte autorregulação do mercado, uma regulamentação que, muitas vezes, é feita através do design de código[1] e que podemos chamar de uma *tecnorregulação*[2]. É crucial analisar quais são os novos desafios legais nesse contexto que nos obriga a pensar em uma estrutura jurídica adequada para responder a esses desafios.

Com base em uma abordagem teórica e constitucional da atual evolução tecnológica, com especial atenção à Internet das Coisas e sua dimensão relacionada à privacidade, o objetivo desse esforço preliminar é desencadear novas reflexões sobre os desafios regulatórios impostos por uma maior (inter) conectividade.

Uma sociedade tecnorregulada

Considerando as características apontadas por estudiosos ciberotimistas, como Manuel Castells e Yochai Benkler, podemos dizer que novas tecnologias de informação e comunicação são consideradas a grande promessa de diversas áreas. No entanto, esse potencial pode ser consideravelmente reduzido dependendo de como novas camadas tecnológicas são construídas sobre certas infraestruturas, permitindo que os usuários explorem mais ou menos ações e dependendo dos critérios de acesso e filtragem de conteúdo por algoritmos[3]. Além disso, empresas privadas estão desenvolvendo tecnologia sem prestar atenção adequada a direitos fundamentais como privacidade e segurança. Sem o devido cuidado, esse procedimento pode trazer sérios riscos aos consumidores (Almeida, Doneda & Monteiro, 2015).

Estamos vivendo um momento de intensa regulamentação tecnológica, mercantilização de dados pessoais e nenhum aparato jurídico robusto para proteger direitos humanos e fundamentais, como proteção da privacidade. É crucial pararmos para pensar sobre o papel que a lei deve desempenhar nesse contexto, especialmente em países como o Brasil que ainda não possuem uma lei sólida e abrangente de proteção de dados (Pagallo, 2013).

A difusão da internet se tornou parte do contexto brasileiro apenas recentemente. Segundo o relatório "CETIC Domicílios", 51% (85,9 milhões) da população é usuária da internet e, dentro dessas estatísticas, 77% dessas pessoas têm entre 16 e 24 anos de idade (Center for Educational Computing, 2009). A legislação brasileira atual já contempla alguns aspectos do acesso e do uso da internet.

Embora regulamentações relacionadas à internet, como o Marco Civil da Internet, tentem resguardar o valor e o potencial da internet ao mesmo tempo em que buscam estabelecer práticas para proteger os direitos constitucionais, a atual autorregulamentação baseada

1 https://www.orbit-rri.org/journal/volume-one/issue-1/threats-internet-things-techno-regulated-society-new-legal-challenge-information-revolution/#post-3450-footnote-7
2 https://www.orbit-rri.org/journal/volume-one/issue-1/threats-internet-things-techno-regulated-society-new-legal-challenge-information-revolution/#post-3450-footnote-8
3 https://www.orbit-rri.org/journal/volume-one/issue-1/threats-internet-things-techno-regulated-society-new-legal-challenge-information-revolution/#post-3450-footnote-27

proven to be able to overlap the rule of law reflected in these regulations. This auto-regulation can subvert the traditional legal logic of "ought to" that safeguards citizens' free will, establishing a binary logic of "can/can't", therefore leaving no alternative to citizens or governments' actions (Pagallo, 2015).

Harvard professor Lawrence Lessig called attention to the fact that the very architecture of the Internet, that is, the hardware and software that make it up with technical structure and codes governing its functioning, are also ways to regulate human behavior. According to professor Lessig, regulation through architecture is sometimes even more effective than other more familiar forms such as law, economics (market) and social norms. That's why he coined the well known phrase "Code is Law"(Lessig, 2000), since the very architecture of the sites makes us hostage of the algorithms[5], regulating our behavior as well as the law and creating serious obstacles to access to information, individual autonomy, privacy and freedom of expression (Lessig, 2006).

The Internet is plastic and changeable and the fact that we are unwittingly becoming hostages of the algorithms that insert us on these bubbles, seeking the promise of hyperconnectivity and its facilities, has been seen as one of the most drastic changes, and subtle, because it is often unnoticeable.[6] In a techno-regulated context ruled by algorithms' binary logic of "can/can't", the democratic potential of the connected public sphere and even the influence of the rule of law can be dramatically reduced.

The concept of rule of law is not easy to tackle. Tom Bingham (Bingham, 2010) brings a huge effort to describe the evolution of the concept and its meaning nowadays. According to Bingham, although we have an abstract idea of what it means as a "law-governed state" and "the laws of the land" and its importance for contemporary societies, it is hard to achieve a consensus about a closed concept.

Nevertheless, for the purposes of this article, we draw on Bingham`s position, considering rule of law as the foundation of a civilized society that embodies a series of important interrelated ideas, as follows: First, it is responsible for limiting the power of the state. A government exercises its authority through publicly disclosed laws that are adopted and enforced by an independent judiciary in accordance with established and accepted procedures. Secondly, no one is above the law; there is equality before the law. Thirdly, there must be protection of the rights of the individual. Finally, the law must apply equally to the government and individual citizens (Bingham, 2010).

Although Bingham considers the concept an ideal, the author agrees that it is an ideal worth striving for and envisions the connection of the rule of law with the concretion of fundamental and human rights. In that sense, we have a discrepancy between the role that the rule of law should represent in contemporary societies and the frequent disregard by private companies such as Facebook and YouTube through techno-regulation on the conduction of their platforms (Bingham, 2010).

5 https://www.orbit-rri.org/journal/volume-one/issue-1/threats-internet-things-techno-regulated-society-new-legal-challenge-information-revolution/#post-3450-footnote-40

6 https://www.orbit-rri.org/journal/volume-one/issue-1/threats-internet-things-techno-regulated-society-new-legal-challenge-information-revolution/#post-3450-footnote-42

no design de códigos[4] provou ser capaz de se sobrepor ao Estado de Direito refletido nestes regulamentos. Essa autorregulação pode subverter a tradicional lógica legal de "deveria fazer" que protege o livre arbítrio dos cidadãos, ao estabelecer uma lógica binária de "pode/não pode", não deixando portanto alternativa às ações dos cidadãos ou governos (Pagallo, 2015).

O professor de Harvard, Lawrence Lessig, chamou a atenção para o fato de que a própria arquitetura da internet, isto é, o hardware e o software que compõem a sua estrutura técnica e os códigos que regem seu funcionamento, também são formas de regular o comportamento humano. Segundo o professor Lessig, a regulação através da arquitetura, é, muitas vezes, mais eficaz do que outras formas mais comuns, como direito, economia (mercado) e normas sociais. Foi por isso que ele cunhou a conhecida frase "O Código é a Lei" (Code is Law) (Lessig, 2000), uma vez que a própria arquitetura dos sites nos torna reféns dos algoritmos[5], regulando nosso comportamento, bem como a lei e criando sérios obstáculos ao acesso. à informação, autonomia individual, privacidade e liberdade de expressão (Lessig, 2006).

A internet é adaptável e mutável, e o fato de estarmos inconscientemente nos tornando reféns dos algoritmos que nos inserem nessas bolhas em nossa busca pela promessa de hiperconectividade e sua conveniência, é visto como uma das mudanças mais drásticas e sutis, porque geralmente é imperceptível[6]. Em um contexto tecnorregulado regido pela lógica binária do algoritmo "pode/não pode", o potencial democrático da esfera pública conectada e até mesmo a influência do Estado de Direito podem ser drasticamente reduzidos.

O conceito de Estado de Direito não é fácil de abordar. Tom Bingham (Bingham, 2010) faz um grande esforço para descrever a evolução do conceito e seu significado hoje em dia. Segundo Bingham, embora tenhamos uma ideia abstrata do que significa um "Estado governado por leis" e "leis da terra" e sua importância para as sociedades contemporâneas, é difícil obter um consenso sobre um conceito fechado.

No entanto, para os fins deste artigo, baseamo-nos na posição de Bingham, considerando o Estado de Direito como o fundamento de uma sociedade civilizada que incorpora uma série de ideias inter-relacionadas e importantes, como vemos a seguir: Em primeiro lugar, ele é responsável por limitar o poder do Estado. Um governo exerce sua autoridade através de leis divulgadas publicamente que são adotadas e aplicadas por um judiciário independente de acordo com os procedimentos estabelecidos e aceitos. Em segundo lugar, ninguém está acima da lei e existe igualdade perante a lei. Em terceiro lugar, deve haver proteção dos direitos do indivíduo e, finalmente, a lei deve aplicar-se igualmente ao governo e aos cidadãos (Bingham, 2010).

4 https://www.orbit-rri.org/journal/volume-one/issue-1/threats-internet-things-techno-regulated-society-new-legal-challenge-information-revolution/#post-3450-footnote-37

5 https://www.orbit-rri.org/journal/volume-one/issue-1/threats-internet-things-techno-regulated-society-new-legal-challenge-information-revolution/#post-3450-footnote-40

6 https://www.orbit-rri.org/journal/volume-one/issue-1/threats-internet-things-techno-regulated-society-new-legal-challenge-information-revolution/#post-3450-footnote-42

In 2004, UN Secretary-General Kofi Annan provided an expansive definition of the rule of law 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. It requires, as well, measures to ensure adherence to the principles of supremacy of law, equality before the law, accountability to the law, fairness in the application of the law, separation of powers, participation in decision-making, legal certainty, avoidance of arbitrariness and procedural and legal transparency" (United Nations Security Council, 2004).

Algorithmic regulation of devices and platforms restricts the user to what has already been programmed. Furthermore, when it comes to algorithms and content providers, content filtering and withdrawal are commonly automatized, rather invisible, and can even execute illegal (and demotivated) censorship without being held accountable to the user. Even though these kinds of practices occur daily, private tech companies do not suffer any penalty. It is the techno-regulation overlapping the rule of law.

According to Ugo Pagallo, "where non-normative instruments dominate the regulatory environment, we seem to be subject to the rule of technology rather than the rule of law. It may be time to realize the fact that increases in efficiency do not always result in effective solutions. `To prevent becoming merely the cognitive resource for these environments we must figure out how they are anticipating us'. In a techno-regulatory setting, rules no longer embody the politics that they are based on, but they simply dictate them. Law and politics do not operate as two exclusive axioms namely, `politics is the field of power relations and contestations; and law is the sphere of truth and justice governed by the rule of law.' Techno-regulation signals the demise of our capacity to reason against and resist, and thus it may result with a further deviation from the values that make us "human" (Pagallo, 2015).

It is important to assert that it must not be the intent of the law to govern this process in a way that hinders the advance of technology. Differently, we must be conscious that if techno-regulation by code is growing faster than our ability to guarantee safety and privacy for users and we are already failing to have an adequate regulatory framework upheld by the law, an adequate legal framework is necessary to respond to those new legal challenges. Moreover, a deep reflection is necessary about to what extent the normative side of the law should be transferred from the traditional "ought to" of legal systems to automatic techniques through mechanisms of design, codes, and architectures (Pagallo, 2012).

The lack of specific regulation, in Brazil for instance, safeguarding personal data, makes it an even worse scenario, facilitating companies to close deals based on online information produced by its clients (users) using their services. This feeds the economic force of private companies, further simulating unclear and unfair relationships that involve practices that are challenging to track – treating data that, most of the times, is beyond the scope of their services and products.

Even though public policy makers and citizens in Brazil appear to be more conscious

Embora Bingham considere o conceito um ideal, o autor concorda que é um ideal pelo qual vale a pena lutar e prevê a conexão entre o Estado de Direito e a efetivação dos direitos humanos e fundamentais. Nesse sentido, há uma discrepância entre o papel que o Estado de Direito deve representar nas sociedades contemporâneas e sua frequente desconsideração por empresas privadas como o Facebook e o Youtube, por meio da tecnorregulação na condução de suas plataformas (Bingham, 2010).

Em 2004, o Secretário Geral da ONU, Kofi Annan, forneceu uma definição abrangente do Estado de Direito como "um princípio de governança no qual todas as pessoas, instituições e entidades, públicas e privadas, incluindo o próprio Estado, são responsáveis perante leis publicamente promulgadas, aplicadas com equidade e adjudicadas de maneira independente, e que sejam consistentes com as normas e padrões internacionais de direitos humanos. Também são exigidas medidas para garantir a aderência aos princípios da supremacia da lei, igualdade perante a lei, responsabilidade perante a lei, justiça na aplicação da lei, separação de poderes, participação na tomada de decisões, segurança jurídica, prevenção de arbitrariedades e transparência processual e legal" (Conselho de Segurança das Nações Unidas, 2004).

A regulação algorítmica de dispositivos e plataformas restringe o usuário ao que já foi programado. Além disso, quando se trata de algoritmos e provedores de conteúdo, a filtragem e a retirada de conteúdo são geralmente automatizadas, feitas de maneira oculta e podem até executar censura ilegal (e desmotivada) sem compromisso com o usuário. Embora esse tipo de prática ocorra diariamente, as empresas privadas de tecnologia não sofrem nenhuma penalidade. É a tecnorregulação sobrepondo-se ao Estado de Direito.

De acordo com Ugo Pagallo, "onde instrumentos não normativos dominam o ambiente regulatório, parece que estamos mais sujeitos ao Estado da tecnologia do que ao Estado de Direito. Talvez seja hora de perceber que o aumento da eficiência nem sempre resulta em soluções eficazes. `Para evitar nos tornarmos apenas o recurso cognitivo desses ambientes, precisamos descobrir como eles estão nos antecipando'. Em um cenário tecnorregulatório, as regras não incorporam mais a política em que se baseiam, mas simplesmente a ditam. Direito e política não operam como dois axiomas exclusivos, a saber: `política é o campo da contestação e das relações de poder; e a lei é a esfera da verdade e da justiça governada pelo Estado de Direito." A tecnorregulação sinaliza o fim de nossa capacidade de raciocinar de maneira contrária e resistir, e, portanto, pode resultar em um desvio adicional dos valores que nos tornam "humanos". (Pagallo, 2015).

É importante ressaltar que não deve ser a intenção da lei reger esse processo de maneira a impedir o avanço da tecnologia. Pelo contrário, devemos estar conscientes de que, se a tecnorregulação por código estiver crescendo mais rapidamente do que nossa capacidade de garantir segurança e privacidade para os usuários - e já estamos falhando em ter uma estrutura regulatória adequada confirmada por lei -, uma estrutura legal adequada é necessária para responder a esses novos desafios jurídicos. Além disso, é necessária uma profunda reflexão sobre até que ponto o lado normativo da lei deve ser transferido do tradicional "dever fazer" dos sistemas jurídicos para as técnicas automáticas por meio de mecanismos de design, códigos e arquiteturas (Pagallo, 2012).

of the Internet's economic and social potential, they are not sufficiently aware of the risks that may arise from private companies' practices or the enhanced risks to fundamental rights imposed by big and open data and the enlargement of the IoT environment.

Besides the urgent necessity of developing a specific legislation about personal data and privacy protection to avoid unconstitutional techno-regulation or personal data treatment, we should seek more broadly an efficient regulation of these technologies through a meta-technological perspective of the law.

The legal order and the rule of law, differently from other social orders, regulate human behavior by means of a specific technique. Once such technique regulates other techniques, that orients behaviors and, beyond that, processes of technological innovation, we may accordingly conceive the law as a meta-technology (Pagallo, 2013).

According to Pagallo and Durante (2016), "the different and even opposite ways in which we can grasp the normative purposes of the law as a meta-technology recommend expanding our view. We propose four steps of analysis. First, a meta-regulatory approach to the field of legal automation should allow us to determine whether, and to what extent, lawmakers shall not (or cannot) delegate decisions to automated systems. Second, focus should be on the impact of technology on the formalisms of the law, and how the latter competes with further regulatory systems. Third, we have to pay attention to the principles and values, which are at stake with the delegation of decisions to automated systems, namely the institutional dimension of the law with matters of interpretation and deliberation. Fourth, the distinction between automatic and non-automatic decisions of the law, and their legitimacy, may entail a class of legal problems, i.e. the hard cases of the law (...)."

Bearing in mind the importance of the law as an effective system for regulating behavior and actions, as well as considering that its criterions also take into account the need to guarantee constitutional rights while concomitantly preserving human autonomy, the rule of law has to guide technology and not the opposite. As Lawrence Lessig once stated, the threat is that "controls over access to content will not be controls that are ratified by courts; the controls over access to content will be controls that are coded by programmers" (Lessig, 2004).

Therefore, in face of the enhanced risks imposed by the advancement of techno-regulation and amplified by the spread of the IoT environment, the rule of law must be seen as the premise for developing technology, or as a meta-technology, that should guide behavioral technological regulation and not the contrary – often resulting in the violation of rights.

No one knows for sure how the Internet of Things will affect our lives in the future. Integrated, related, targeted and combined data collected from smart devices, providing numerous opportunities for analysis of this information and converting each information in a relevant piece of information to be combined and analyzed. Whether

A falta de regulamentação específica, no Brasil, por exemplo, para salvaguardar dados pessoais, torna o cenário ainda pior, facilitando as empresas a fechar negócios com base em informações produzidas online pelos clientes (usuários) que utilizam seus serviços. Isso alimenta a força econômica das empresas privadas, simulando relações pouco claras e injustas que envolvem práticas difíceis de rastrear - processando dados que, na maioria das vezes, estão além do escopo de seus serviços e produtos.

Embora os formuladores de políticas públicas e cidadãos no Brasil pareçam estar mais conscientes do potencial econômico e social da internet, eles não estão suficientemente cientes dos riscos que podem surgir das práticas de empresas privadas ou do aumento dos riscos para os direitos fundamentais impostos por dados abertos e big data e a ampliação do ambiente da IoT.

Além da necessidade urgente de desenvolver uma legislação específica sobre a proteção de dados pessoais e da privacidade para evitar a tecnorregulação inconstitucional ou o processamento de dados pessoais, devemos buscar uma regulamentação mais eficiente dessas tecnologias por meio de uma perspectiva metatecnológica da lei.

A ordem legal e o Estado de Direito, diferentemente de outras ordens sociais, regulam o comportamento humano por meio de uma técnica específica. Uma vez que essa técnica regula outras técnicas que orientam comportamentos e processos de inovação tecnológica, podemos conceber a lei como uma metatecnologia (Pagallo, 2013).

Segundo Pagallo e Durante (2016), "as maneiras diversas e até opostas pelas quais podemos apreender os propósitos normativos da lei como metatecnologia recomendam expandir nossa visão. Propomos quatro etapas de análise. Primeiro, uma abordagem metarreguladora do campo da automação legal deve permitir-nos determinar se, e em que medida, os legisladores não devem (ou não podem) delegar decisões a sistemas automatizados. Segundo, o foco deve estar no impacto da tecnologia nos formalismos da lei e em como esta compete com outros sistemas reguladores. Terceiro, devemos prestar atenção aos princípios e valores que estão em jogo com a delegação de decisões a sistemas automatizados, especialmente, a dimensão institucional da lei com questões de interpretação e deliberação. Quarto, a distinção entre decisões automáticas e não automáticas da lei e sua legitimidade pode acarretar uma classe de problemas jurídicos, ou seja, os casos difíceis (*hard cases*) da lei (...). "

Levando em conta a importância da lei como um sistema eficaz para regular comportamentos e ações, bem como considerando que seus critérios também levam em consideração a necessidade de garantir direitos constitucionais e, ao mesmo tempo, preservar a autonomia humana, o Estado de Direito deve orientar a tecnologia e não o contrário. Como Lawrence Lessig afirmou uma vez, a ameaça é que "os controles sobre o acesso a conteúdo não serão ratificados pelos tribunais; os controles sobre o acesso a conteúdo serão controles codificados pelos programadores "(Lessig, 2004).

Portanto, perante os grandes riscos impostos pelo avanço da tecnorregulação ampliada pela disseminação do ambiente da IoT, o Estado de Direito deve ser visto como a premissa para o desenvolvimento de tecnologia, ou como uma metatecnologia, que deve orientar a regulação tecnológica comportamental e não o contrário que geralmente resulta na violação de direitos.

or not, the way we interact with machines and algorithms tends to be more and more intense. In this context Internet of Things, governance and data security will be key. Businesses and consumers should weigh benefits and risks cautiously. Moreover, the law should be aware of its role in this context aiming to, on one side, not excessively hamper the economic and technological development in progress, and, on the other, regulate effectively these practices in order to curb abuses and protect the existing constitutional rights. ■

Ninguém sabe ao certo como a Internet das Coisas afetará nossa vida no futuro. Dados integrados, relacionados, direcionados e combinados coletados de dispositivos inteligentes, fornecendo inúmeras oportunidades para análise dessas informações e convertendo cada informação em uma informação relevante a ser combinada e analisada. Seja como for, a maneira como interagimos com máquinas e algoritmos tende a ser cada vez mais intensa. Nesse contexto, a Internet das Coisas, governança e segurança de dados serão fundamentais. As empresas e os consumidores devem avaliar os benefícios e os riscos com cautela. Além disso, a lei deve estar ciente de seu papel nesse contexto, visando, por um lado, não prejudicar excessivamente o desenvolvimento econômico e tecnológico em andamento, e, por outro, regular efetivamente essas práticas, a fim de coibir abusos e proteger os direitos constitucionais existentes. ■

ISSN 2176-297X