2022

Tensões Geopolíticas Globais e os Desafios de Fortalecimento da Defesa e Segurança Nacional: apontamentos preliminares

Autores | Authors

ANDRÉ CLARK
PAULO SERGIO MELO DE CARVALHO
RONALDO CARMONA

Global Geopolitical Tensions and the Challenges of Strengthening Defense and National Security: preliminary comments

NÚCLEO
DEFESA E SEGURANÇA INTERNACIONAL
DEFENSE AND INTERNATIONAL SECURITY PROGRAM

POLICY PAPERS

CEBRI POLICY PAPERS

Apoio | Partnership

KONRAD ADENAUER STIFTUNG

“As inovações associadas à Quarta Revolução Industrial criam um novo campo de batalha para conflitos e crimes internacionais: o espaço cibernético. A guerra, nos dias atuais, é híbrida, e exige novas medidas para garantir a defesa nacional e minimizar as vulnerabilidades advindas do ciberespaço. O governo brasileiro deve, portanto, estar atento aos crescentes desafios relacionados à digitalização e atuar para que a Estratégia Nacional de Segurança Cibernética seja efetiva na garantia da segurança cibernética no país. Além disso, internacionalmente, o Brasil deve buscar a cooperação com os demais Estados para o estabelecimento de acordos e redes de confiança para lidar com as ameaças cibernéticas.”

The innovation associated with the Fourth Industrial Revolution opens up a new battleground for international conflict and crime: cyberspace. Modern warfare is hybrid. New actions are required to guarantee national defense and to minimize vulnerabilities associated with the cyberspace. The Brazilian government must therefore be mindful of the growing challenges related to digitization and act so that the National Cybersecurity Strategy can effectively ensure Brazil’s cybersecurity. In the international arena, Brazil should cooperate with other States to establish agreements and to build trust networks that can address cyberthreats.

NÚCLEO **DEFESA E SEGURANÇA INTERNACIONAL CEBRI**

O NÚCLEO TRATA DA SEGURANÇA INTERNACIONAL, COM FOCO EM NOVAS AMEAÇAS E FORMAS DE GUERRA, A POLÍTICA E A ESTRATÉGIA BRASILEIRA DE DEFESA, A QUESTÃO AMAZÔNICA, O ATLÂNTICO SUL E A SEGURANÇA CIBERNÉTICA.

CEBRI DEFENSE AND INTERNATIONAL **SECURITY** PROGRAM

THE PROGRAM EXAMINES THE CHALLENGES OF INTERNATIONAL SECURITY, FOCUSING ON TOPICS SUCH AS NEW THREATS AND FORMS OF WAR, CYBERSECURITY, BRAZILIAN DEFENSE POLICY AND STRATEGY AS WELL AS THE ISSUE OF THE AMAZON AND THE SOUTH ATLANTIC.

Especialistas | Experts

ANDRÉ CLARK
Conselheiro do CEBRI, Vice-presidente Sênior para o Hub América Latina da Siemens Energy e General Manager da Siemens Energy Brasil
| Trustee at CEBRI, Senior Vice President for the Siemens Energy hub in Latin America and General Manager of Siemens Energy Brazil

PAULO SERGIO MELO DE CARVALHO
Senior Fellow do CEBRI e Ex-chefe do Centro de Defesa Cibernética do Exército Brasileiro
| Senior Fellow at CEBRI and Former Head of the Brazilian Army's Cyber Defense Center

RONALDO CARMONA
Senior Fellow do CEBRI e Professor da Escola Superior de Guerra (ESG)
| Senior Fellow at CEBRI and Professor at Escola Superior de Guerra (ESG)

2022

NÚCLEO DEFESA E SEGURANÇA INTERNACIONAL

DEFENSE AND INTERNATIONAL SECURITY PROGRAM

POLICY PAPERS

AS OPINIÕES E MANIFESTAÇÕES EXPRESSAS NESTE POLICY PAPER REPRESENTAM EXCLUSIVAMENTE AS OPINIÕES DOS SEUS AUTORES E NÃO, NECESSARIAMENTE, A POSIÇÃO INSTITUCIONAL DO CENTRO BRASILEIRO DE RELAÇÕES INTERNACIONAIS (CEBRI), DOS SEUS INTEGRANTES OU DOS SEUS APOIADORES.

THE OPINIONS AND STATEMENTS EXPRESSED IN THIS POLICY PAPER ARE THOSE OF THE CONTRIBUTING AUTHORS ALONE AND DO NOT NECESSARILY REFLECT THE VIEWS AND POSITIONS OF THE BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS (CEBRI), ITS MEMBERS OR ITS SUPPORTERS.

SUMÁRIO | TABLE OF CONTENTS

INTRODUÇÃO 3

DESAFIOS 6

PROPOSIÇÕES 15

CONCLUSÃO 21

REFERÊNCIAS 23

INTRODUCTION 25

CHALLENGES 27

PROPOSALS 36

CONCLUSION 42

REFERENCES 44

Tensões Geopolíticas Globais e os Desafios de Fortalecimento da Defesa e Segurança Nacional: apontamentos preliminares

INTRODUÇÃO

O mundo passa, atualmente, por transformações disruptivas na esfera da Segurança Internacional, que tem efeitos não somente conjunturais, mas estruturais e de longo prazo. Nas duas primeiras décadas do século XXI, o aspecto dominante do cenário internacional foi a disputa sistêmica entre os Estados Unidos, potência vitoriosa após o final da Guerra Fria, e a China, potência contestadora que reemerge após mais de quatro décadas de uma exponencial ascensão, em parte, resultante de manobras derivadas da própria geopolítica da Guerra Fria. Essa disputa por hegemonia, que na história contemporânea ocorre em espaço de gerações, apresenta, como seu traço mais fundamental, renovadas ameaças à estabilidade e à segurança internacional, em múltiplas dimensões. Este é, portanto, um primeiro sentido disruptivo no cenário internacional: a efetivação, ou não, de uma disputa por posições no sistema internacional, ou ainda uma solução intermediária, representada por uma guerra prolongada, em múltiplos domínios, por esta posição de liderança.

A partir do ano de 2020, o mundo passou a enfrentar a ameaça causada pelo vírus Sars-Cov-2, que rapidamente se espalhou por todo o planeta e colocou em risco, no limite, a sobrevivência da população humana. O período posterior a eclosão da pandemia de Covid-19 caracterizou-se pela aceleração de algumas tendências anteriores, dentre as quais, a digitalização da economia e da atividade social, a crise da ordem global internacional e do multilateralismo, com o fortalecimento das opções nacionais como

crescente regra sistêmica. Associado a isso, observou-se movimentos ligados ao que tem sido chamado de "desglobalização" e desacoplamento (*decoupling*), com a reversão, ainda que parcial, das cadeias globais, sobretudo as associadas a insumos críticos. Ainda que o processo de vacinação em massa da população mundial tenha minimizado os riscos à saúde global provocados pela Covid-19, os efeitos dessa pandemia na geopolítica internacional continuam relevantes.

Por fim, outro marco recente na conjuntura internacional, mas que influenciará no longo prazo a geopolítica mundial e a arquitetura de segurança consolidada após o final da Segunda Guerra Mundial, é o conflito armado que se desenvolve no território ucraniano desde fevereiro de 2022. A guerra entre a Rússia e a Ucrânia, e o apoio dos países da Organização do Tratado do Atlântico Norte (OTAN) a essa última, oferecem riscos à estabilidade internacional, e aprofundam tendências identificadas anteriormente, como o enfraquecimento do sistema multilateral e a fragmentação de cadeias globais. Essa guerra, os efeitos da pandemia de Covid-19, e a disputa entre Estados Unidos e China, oferecem consequências significativas para a segurança internacional, assim como para a defesa e segurança do Brasil. Em um cenário de confrontação sistêmica, em que a natureza da guerra contemporânea apresenta novas e inéditas facetas, o *Policy Paper* do núcleo de Defesa e Segurança Internacional do CEBRI busca analisar e fazer proposições sobre os principais desafios que se colocam para o Brasil na atualidade.

Cabe ressaltar que o surgimento deste núcleo de Defesa e Segurança Internacional no âmbito do CEBRI, estruturado neste

formato em 2021, busca contribuir para suprimir uma lacuna. A partir de um dos principais *think-thanks* brasileiros e do Hemisfério Sul, objetiva-se constituir um centro de pensamento fora da estrutura de Estado, voltado à produção de conhecimento e análise de assuntos de Defesa e Segurança Internacional, tal como aqueles existentes em outros países, como, por exemplo, modelos de grande porte como a *RAND Corporation* norte-americana ou fundações e institutos europeus.

DESAFIOS

A COMPETIÇÃO SISTÊMICA ENTRE SUPERPOTÊNCIAS

O mundo vive atualmente em uma era de competição sistêmica entre superpotências, no qual um polo – a China – busca consolidar sua ascensão e o outro – os Estados Unidos – busca frear a ascensão do poder contestador e, ao mesmo tempo, reverter a perda de poder relativo. A ameaça clássica principal à segurança do sistema internacional é a ocorrência de um confronto militar entre Estados nacionais, em especial entre grandes potências. A competição entre China e Estados Unidos oferece riscos de uma confrontação, sobretudo de forma não cinética e de forma indireta como atualmente ocorre, seja pelo fato de serem potências nuclearmente armadas, seja pela complementaridade econômica entre essas duas economias, que, contudo, recua com o movimento de "*decoupling*". A ameaça de um confronto militar entre Estados é real, como se observa no conflito entre a Rússia e a Ucrânia, em 2022. Para além dos desafios iminentes para a segurança internacional causados pela guerra, essa disputa também afetará no longo prazo a geopolítica internacional e a relação entre as superpotências.

A crise da ordem internacional, e da própria globalização, gera desafios para o Brasil, que tem relações importantes com os Estados Unidos e a China. Essas relações têm amplo aspecto,

incluindo questões culturais, políticas, econômicas, tecnológicas e militares. Nessa competição entre as duas superpotências, o Brasil será cobrado a assumir posições. Não convém, contudo, se mirarmos pelo interesse nacional, tomar posições antagônicas ou agudas, excludentes. O Brasil é tendencialmente uma potência, com uma grande extensão territorial e população, é um grande fornecedor de alimentos para o mundo, tem uma matriz energética limpa, e não tem ameaças militares neste momento à sua segurança – ainda que poderá sofrer antagonismos importantes no futuro breve, como mostram nossos documentos de Defesa.

A própria identificação dos riscos e ameaças à integridade e à soberania do Brasil é um grande desafio posto ao Estado e à sociedade brasileira. As medidas mitigadoras a estes, inclusive de Defesa e Segurança Nacional, têm longo tempo de maturação. Atualizar essa percepção é, portanto, desafio urgente aos brasileiros diante do grave cenário internacional que se apresenta contemporaneamente.

A QUARTA REVOLUÇÃO INDUSTRIAL E A CORRIDA TECNOLÓGICA

A competição entre Estados Unidos e China ocorre em meio a outro fenômeno estrutural, que é a aceleração no desenvolvimento de novas tecnologias. O mundo vive atualmente os primeiros momentos de uma nova revolução tecno-científica – a Quarta Revolução Industrial -, com o amadurecimento de um conjunto de tecnologias, que tem grande impacto sobre a produtividade e sobre o trabalho. Esse conjunto de tecnolo-

gias emergentes – dentre as quais, a inteligência artificial, os algoritmos de *big data* e a multiplicação de sensores de todas as coisas (*Internet of Things* - IoT) – são, por definição, de *natureza dual*. Assim como em Revoluções Industriais anteriores, os países que dominarem a base técnica-tecnológica dessa Quarta Revolução serão os líderes da ordem mundial no século XXI.

Nesse contexto, portanto, o ambiente de concorrência interestatal possivelmente será exponencializado pela realidade de dois "ecossistemas" de tecnologias de informação e comunicação, e de cadeias de produção sensíveis. Esses ecossistemas serão liderados pelos EUA e pela China, em intensa competição tecno-científica. O sistema internacional se caracterizará, portanto, por uma corrida tecnológica entre superpotências em torno da liderança nos padrões que organizarão as forças produtivas em escala global, com o advento da digitalização da economia e de tecnologias como o 5G.

Observa-se um ativismo das grandes potências em torno de novas políticas industriais ancoradas em Ciência, Tecnologia e Inovação (CT&I), que almejam maior autonomia relativa em insumos vitais ou críticos. Isso foi explicitado pela crise da Covid-19, resultando em protecionismo, ruptura de Cadeias Globais de Valores e movimento de "re-shoring". Em síntese, há cada vez mais relação direta entre segurança nacional e política industrial por parte das principais potências mundiais.

Os desafios e riscos para o Brasil nesse cenário se relacionam com a dependência de cadeias globais, em especial daquelas de tecnologias e produtos de defesa. Eventos recentes como a pan-

demia de Covid-19 e a Guerra na Ucrânia demonstram que a dependência de tecnologias estrangeiras na construção de sua estrutura de defesa é um dos principais riscos para a segurança brasileira. Além disso, esse risco se torna especialmente grave em um contexto de conflitos de grandes proporções. A ausência de soluções tecnológicas próprias diminui a autonomia do Brasil no cenário atual, e traz riscos de um alinhamento automático no contexto de competição entre os Estados Unidos e a China.

A GUERRA HÍBRIDA E A CIBERSEGURANÇA

As novas tecnologias e as disrupções decorrentes dessas inovações afetam diretamente a estabilidade de países e do sistema internacional. Nesse sentido, a guerra contemporânea é marcada por seu caráter híbrido, em que novas tecnologias abrem possibilidades de quebra da coesão nacional do oponente. O controle dos metadados, gerados por 2/3 da humanidade diariamente conectado à internet permite novas manobras estratégicas no sentido da desestabilização do oponente, e de forma cada vez mais dissimulada. A guerra contemporânea ocorre de forma permanente, sob a aparência de paz, com campanhas de desinformação e operações psicológicas voltadas às grandes massas.

Os novos padrões sociais, resultantes da massificação da internet e do advento das redes sociais, criam vulnerabilidades altamente críticas à coesão nacional e ao próprio regime democrático. Ações em redes sociais, como a disseminação de informações falsas e rumores, a exposição de líderes políticos, o estímulo à descrença nas instituições, e a interferência nos

processos eleitorais, podem afetar a coesão social de Estados. Mais além, a guerra no ambiente cibernético está ao alcance de um maior número de países, assim como de organizações criminosas transnacionais.

As sociedades hoje são altamente dependentes de serviços sendo, portanto, altamente vulneráveis a ataques contra infraestruturas críticas. A guerra híbrida, por fim, borra os limites entre o público e o privado, com ataques ocorrendo a empresas e infraestruturas privadas. Há um conjunto de ações sendo desenhado por parte das grandes potências para a mitigação destas vulnerabilidades, que vai de medidas legais a contramedidas na área de inteligência. Nesse contexto, se faz necessário analisar quais são as estruturas necessárias para enfrentar esse tipo de ameaça. Mais além, essa estrutura exigirá cooperação internacional, pois ataques partem de atores transnacionais.

Tecnologias da informação e das comunicações se tornaram indispensáveis para o pleno funcionamento do Estado, da economia e da vida em sociedade. A aceleração do processo de digitalização do trabalho, da política e da vida em sociedade gerou oportunidades, mas também desafios. Neste particular, há largo esforço para que o espaço cibernético se mantenha aberto, livre e seguro. *Aberto*, para que permita a promoção de acesso à internet universal, acessível e igual, em particular para que permita crescimento econômico e inovação, e gere desenvolvimento político, social e econômico no mundo todo. *Livre*, para que seja possível a promoção e proteção dos direitos humanos e liberdades fundamentais, incluindo a liberdade de expressão, acesso à informação, direito de reunião e associação, privacidade e julgamento justo. *Seguro*, para que permita melhor coope-

ração e luta contra crimes cibernéticos, especialmente por meio do uso de instrumentos diplomáticos e legais e na construção de resiliência contra ataques cibernéticos.

Os ataques cibernéticos podem causar sérios danos às instalações, serviços e bens das empresas de setores estratégicos – como o setor energético – que, se forem interrompidos ou destruídos, provocarão grandes impactos sociais, econômicos, políticos e de segurança. A crescente digitalização e automação da gestão do setor de energia impõe a necessidade de um controle avançado nas pontas e nas diversas camadas dos seus sistemas, o que implica a adoção de medidas bem definidas e uma gestão rígida da governança dos seus ativos de informação, facilitando a operação dos diversos sistemas da empresa. Igualmente, essa transformação digital torna indispensável a adoção de políticas de segurança cibernética pelos órgãos governamentais para proteger as infraestruturas críticas da área de energia, dentre outras.

Após a aprovação da Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal em 2015 e da Política Nacional de Segurança da Informação em 2018, o governo brasileiro lançou, no começo de 2020, a Estratégia Nacional de Segurança Cibernética - E-Ciber. O documento está vinculado ao arcabouço mais amplo de planejamento estratégico geral do Estado brasileiro e representa o primeiro eixo da Estratégia Nacional de Segurança da Informação que, em cumprimento ao estabelecido na política declaratória de 2018, será construída em módulos temáticos. A Estratégia tem o objetivo de buscar as melhores práticas em segurança cibernética, além de estabelecer as principais metas e

objetivos estratégicos para os próximos quatro anos, que deverão inspirar e guiar ações futuras. Nesse sentido, faz-se oportuno analisar a visão estratégica do governo brasileiro para manter o espaço cibernético nacional seguro, assim como refletir sobre as iniciativas indispensáveis para que a E-Ciber evolua de uma política declaratória para uma estratégia efetiva de segurança cibernética. Igualmente, é pertinente refletir sobre a adequação das versões originais e das revisões periódicas do Livro Branco da Defesa Nacional; da Estratégia Nacional e da Política Nacional de Defesa para tornar a sociedade brasileira mais consciente acerca dos riscos apresentados pela dimensão cibernética da segurança para a defesa nacional.

Além da Estratégia Nacional de Segurança Cibernética, outro marco importante para a cibersegurança brasileira foi a aprovação, em 2018, da Lei Geral de Proteção de Dados Pessoais (LGPD). Essa Lei estabelece regras sobre a coleta, armazenamento, tratamento e compartilhamento de dados pessoais visando proteger operações de tratamento de informações relacionadas a pessoa natural identificada ou identificável e assim assegurar o direito constitucional à privacidade. Criada pela LGPD, foi ativada, em outubro de 2020, pelo Senado brasileiro a Autoridade Nacional de Proteção de Dados (ANPD). A ANPD tem a atribuição de zelar pela proteção dos dados pessoais, assegurar a observância de segredos comerciais e industriais e punir eventuais descumprimentos à legislação. Em que pese os avanços dessas iniciativas para promoção da segurança cibernética com foco na privacidade dos indivíduos, a LGPD e a ANPD não são suficientes para promover de forma objetiva e específica a segurança da informação que, por sua vez, compreende a proteção das informações, sistemas, recur-

sos e demais ativos contra desastres, erros e manipulação não autorizada, com o objetivo de reduzir a probabilidade e o impacto de incidentes de segurança cibernética. Nesse sentido, é necessário refletir sobre estratégias de redução dos riscos e dos danos causados por ataques cibernéticos à segurança da informação de empresas e do governo, assim como os limites e possibilidades da criptografia para assegurar a segurança da informação e a proteção de dados nos poderes da República e nas empresas do país.

A DEFESA E A SEGURANÇA NACIONAL DO BRASIL

Os riscos e ameaças resultantes do agravamento do ambiente de segurança internacional contemporâneo apresenta evidentes consequências para a Defesa Nacional, e vista de forma mais ampla, para a Segurança Nacional. O Brasil tem características que o colocam como um ator relevante no sistema internacional: está entre os maiores países do mundo em termos de território e população, e é uma potência em sua região, fazendo fronteira com quase todos os países sul-americanos e tendo quase 17 mil quilômetros de fronteira terrestre. Assim, se faz necessário que o país tenha relevância em termos militares, para garantir a sua segurança. Mais além, as disputas que ocorrem no sistema internacional também têm reflexos na América do Sul, sendo necessário que o Brasil tenha poder militar para garantir a paz na região e sua segurança. Urge, por exemplo, relançar uma política e uma estratégia brasileira para a América do Sul, e de forma mais ampla, para seu entorno estratégico, que inclui o Atlântico Sul e a África.

A segurança brasileira, conjunturalmente e circunstancialmente, não é ameaçada diretamente por outros Estados, sobretudo pelo fato de o país estar inserido em uma região sem grandes conflitos interestatais. Contudo, vislumbram-se possíveis alterações dessa realidade, como demonstra, por exemplo, a securitização da questão ambiental por parte da OTAN, em sua recente atualização estratégica. Em nosso entorno sul-americano, chama atenção as ações de atores não estatais, e, em especial, aquelas ligadas a atividades de narcotráfico. É um desafio para o Brasil a questão da violência em seu território, e a garantia de segurança nas suas fronteiras. Medidas para enfrentar esses problemas exigem ampla reflexão e discussão pela sociedade.

Por fim, no contexto de sua Política e Estratégica Nacional de Defesa e de uma possível nova Estratégia de Segurança Nacional, é um desafio para o Brasil identificar necessidades atinentes à modernização e reequipamento de sua estrutura de defesa. Nesse contexto, ajustes institucionais e reversão de instabilidades orçamentárias – cuja consequência é a impossibilidade de planejar gastos de médio e longo prazo - são alguns dos desafios para estruturação de Forças Armadas e de uma base industrial de defesa no Brasil que sejam compatíveis com as necessidades e a importância do país no sistema internacional.

PROPOSIÇÕES

A COMPETIÇÃO SISTÊMICA ENTRE SUPERPOTÊNCIAS

No contexto da rivalidade geopolítica entre as duas grandes potências, Estados Unidos e China, o Brasil precisa **considerar os riscos atinentes à associação a um ou a outro projeto**, o que tornam essas opções altamente desaconselhavéis, tendo em vista nosso interesse nacional. Além disso, o país deve **avaliar os condicionantes sistêmicos e conjunturais para seu posicionamento**, tendo em vista o histórico diplomático brasileiro de independência e autonomia. O Brasil deve **trilhar na sua posição histórica** de promoção do diálogo, do consenso e do respeito ao multilateralismo e ao direito internacional, e **evitar alinhamentos** nessa disputa.

A QUARTA REVOLUÇÃO INDUSTRIAL E A CORRIDA TECNOLÓGICA

No contexto da Quarta Revolução Industrial e da competição sistêmica entre Estados Unidos e China, se faz necessário **assegurar crescente independência sobre sistemas oriundos do exterior**. Assim o Brasil deve **ter o domínio técnico para manter esses sistemas**, mesmo em situações de crise

e de possíveis embargos. Mais além, a fim de garantir a autonomia do Brasil no cenário de competição sistêmica e da quarta revolução industrial, o Brasil deve **buscar soluções tecnológicas próprias**. Deve-se **analisar quais sistemas e tecnologias podem ser desenvolvidos no Brasil, e o que deve ser buscado no exterior** – e para isso deve haver uma institucionalidade adequada no Estado brasileiro para a tomada destas decisões, como demonstram boas práticas internacionais. Em ambos os casos, sublinha-se a importância de haver independência logística no caso de crises e conflitos – ou seja, deve-se **adquirir equipamentos e ter a autonomia de manter seu funcionamento e produção** na eventualidade de embargos externos. Por fim, o Brasil só terá condições de diálogo em fóruns internacionais se tiver condições de produzir tecnologias próprias.

Na agenda de ciência, tecnologia e inovação, há cada vez mais relação direta entre segurança nacional e política industrial por parte das principais potências mundiais. O Brasil precisa **priorizar o fortalecimento da Base Industrial de Defesa (BID)** – conjunto de empresas estatais e privadas que participam de uma ou mais etapas da produção de produtos estratégicos de defesa -, fazendo com que o país, a partir desse setor, possa desenvolver novos modos de incorporar ciência, tecnologia e inovação na indústria nacional e nos bens e serviços por ela produzidos, e buscar a independência tecnológica no preparo das Forças Armada, principalmente em setores em que o Brasil tenha vantagens tecnológicas comparativas.

Problema vital relaciona-se a estabilidade e volume de recursos destinados à consecução desta autonomia em tecnologias

e sistemas críticos. Para reverter essa vulnerablidade, primeiro será necessário **aumentar o nível de percepção do Estado e da sociedade a riscos e ameaças**, inclusive de natureza estatal. Derivado do aumento desta percepção, está a necessidade de um debate, sobretudo com o Congresso Nacional, para o estabelecimento de fontes *estáveis*, com uma programação plurianual, e em *volume* compátivel a um país de nosso porte, tendo como referência os gastos em Defesa Nacional médios dos demais BRICS e dos países da OTAN, na casa de 2% do PIB.

A GUERRA HÍBRIDA E A CIBERSEGURANÇA

Constituir, por ocasião da revisão periódica da Política e da Estratégia Nacional de Defesa, conceitos e iniciativas (contra-medidas) relacionadas aos riscos atinentes à forma híbrida, indireta e dissimulada de ataques à soberania e à integridade nacional no formato que estes tomam contemporeanamente.

Implementar governança da segurança cibernética por intermédio da descrição e separação dos papéis, interfaces e modos de interação entre os setores público e privado, e os institutos de pesquisa nas áreas de ciência e tecnologia.

Promover uma rede colaborativa entre os diversos entes da sociedade brasileira para que a coordenação em múltiplos níveis e setores seja realizada de forma mais intrínseca, diante de princípios de segurança cibernética.

Incrementar o Plano Nacional de Gestão de Incidentes Cibernéticos (PLANGIC) e planos setoriais mais específicos, propiciando maior destaque e detalhamento à defesa cibernética nas Políticas Declaratórias de Defesa Nacional, como a Estratégia Nacional de Defesa, a Política de Defesa Nacional e o Livro Branco de Defesa Nacional.

Criar novas estratégias de regulação e incentivos para uma maior coordenação entre empresas do setor de energia, assim como destas com empresas do setor de telecomunicações.

Manter um ciclo de avaliações para detectar vulnerabilidades cibernéticas em instalações e estruturas nas redes do setor energético.

Criar um perfil de risco nacional de fornecedores de equipamentos ligados à tecnologia 5G e um perfil de risco nacional de operadoras, provedores de Internet e empresas com acesso a redes privadas 5G.

Acoplar a segurança do sistema 5G à proteção dos dados dos usuários, via responsabilização, apesar da Lei Geral de Proteção de Dados Pessoais (LGPD) e a ativação da Autoridade Nacional de Proteção da Dados (ANPD).

Promover estratégias de redução dos riscos e dos danos causados por ataques cibernéticos à segurança da informação de empresas e do governo, assim como estratégias de segurança da informação e proteção de dados nos poderes da República e nas empresas do país.

Incrementar o investimento público direcionado para Ciência e Tecnologia, e promover um maior alinhamento estratégico dos órgãos de fomento para as políticas de defesa e segurança cibernéticas nacionais.

Promover acordos de cooperação internacionais, estabelecendo memorandos de entendimento que possibilitarão o compartilhamento de informações relacionadas com as ameaças cibernéticas, as tendências de crimes e ataques cibernéticos, as vulnerabilidades latentes, os novos malwares e o intercâmbio nas metodologias da prevenção e resposta a incidentes cibernéticos.

A DEFESA E A SEGURANÇA NACIONAL DO BRASIL

A deterioração e perda de legitimidade do ambiente de segurança internacional contemporâneo e do multilateralismo apresentam evidentes riscos à Defesa Nacional e à Segurança do Brasil. **A revisão periódica da Política e da Estratégia Naconal de Defesa precisa espelhar estas novas realidades e buscar um envolvimento amplo**, de múltiplos setores do Estado e da sociedade, buscando elevar a percepção desta sobre estes riscos e ameaças. Nesse sentido, deve-se **aprimorar o trâmite dos documentos de Defesa no Congresso Nacional**, como, por exemplo, instituindo um rito similar ao das medidas provisórias, ou ainda o fortalecimento, nos vários formatos que vêm sendo propostos, das Comissões de Defesa, Relações Exteriores e Inteligência existentes nas duas casas legislativas e bicameralmente.

É necessário que o Brasil tenha relevância em termos militares, para garantir a sua segurança e a paz na América do Sul coletivamente. Nesse sentido, o **relançamento do Conselho de Defesa Sul-americano (CDS)** é desafio urgente. Não se trata de "questão ideológica", mas problema de Estado, visando, por um lado, aumentar o nível de confiança entre os países sul-americanos, e, por outro lado, inibir a presença de potências extra-regionais em nosso entorno estratégico mais imediato - a América do Sul. Medida com idêntico sentido e motivação se faz necessária para o Atlântico Sul, com a urgente necessidade de **reestruturação da ZOPACAS (Zona de Paz e Cooperação do Atlântico Sul)**.

No contexto de suas políticas declaratórias de defesa, o Brasil deve **identificar necessidades atinentes à modernização e reequipamento da Estrutura de Defesa** tendo por base as ameaças claramente identificadas, com destaque para o fato de termos parte do território nacional (a Amazônia) situada como uma das principais áreas de tensão geoestratégica no nível global. Além disso, nesse processo, o país deve ser capaz de planejar gastos de médio e longo prazo, tendo como referência investimento na casa de 2% do PIB, como o fazem países de nosso porte geopolítico.

Deve-se ainda **valorizar socialmente o tema de defesa e segurança na sociedade e no orçamento da União; e realizar investimentos em ciência e tecnologia na indústria de defesa**, pois estes são chave para o desenvolvimento econômico de países. Por fim, deve-se **refletir sobre as ameaças à segurança nacional advindas do narcotráfico**, e executar ações para enfrentar as consequências dessa atividade.

CONCLUSÃO

As crescentes instabilidades do sistema internacional e suas transformações oferecem riscos à Defesa e à Segurança do Brasil, e demandam que o país tenha condições de enfrentá-los. Em um cenário em que a competição sistêmica entre Estados Unidos e China se torne mais acirrada, o Brasil deve ter condições de assumir uma postura autônoma em relação a ambas as superpotências. Mais além, o país tem condições de se posicionar como um ator que contribui para a construção de entendimentos e que mantém relação com todos os países do globo.

Um dos principais marcos dessa conjuntura internacional que se apresenta atualmente é a competição pelo domínio e liderança de novas tecnologias ligadas à Quarta Revolução Industrial e ao processo de digitalização de interações sociais e processos produtivos. Há, inclusive, a possibilidade de criação de dois "ecossistemas" liderados por EUA e China. Nesse cenário, a dependência brasileira de tecnologias estrangeiras oferece grandes riscos à segurança nacional, e demandam ações no sentido de construir soluções tecnológicas próprias e garantir a autonomia do país no contexto de acirramento da competição sistêmica.

As inovações associadas à Quarta Revolução Industrial criam um novo campo de batalha para conflitos e crimes internacionais: o espaço cibernético. A guerra, nos dias atuais, é híbrida, e exige novas medidas para garantir a defesa nacional e minimizar as vulnerabilidades advindas do ciberespaço. O governo brasileiro deve, portanto, estar atento aos crescentes desafios rela-

cionados à digitalização e atuar para que a Estratégia Nacional de Segurança Cibernética seja efetiva na garantia da segurança cibernética no país. Além disso, internacionalmente, o Brasil deve buscar a cooperação com os demais Estados para o estabelecimento de acordos e redes de confiança para lidar com as ameaças cibernéticas.

Por fim, o Brasil possui características – territoriais, populacionais, econômicas, geopolíticas e diplomáticas – que não permitem que o país seja um ator reativo no sistema internacional. O Brasil tem capacidades para atuar no sentido de promover a paz nesse sistema e garantir a segurança não apenas da região em que está inserido – a América do Sul e o Atlântico Sul -, mas também de outras, dado seu porte geopolítico. Para isso, se faz necessário que além de uma diplomacia ativa, o país tenha capacidades materiais de se projetar internacionalmente. A modernização e o reequipamento de sua estrutura de defesa, portanto, devem ser prioridades, e não apenas para garantir meios de ação no sistema internacional, mas também porque esse tipo de investimento tem desdobramentos nos demais setores da economia e é chave para o desenvolvimento nacional.

REFERÊNCIAS

CARMONA, RONALDO.

Reflexões sobre a Geopolítica no contexto da quarta revolução industrial e dos novos desafios de segurança internacional. CEBRI, janeiro de 2022. Disponível em: https://cebri.org/br/doc/241/reflexoes-sobre-a-geopolitica-no-contexto-da-quarta-revolucao-industrial-e-dos-novos-desafios-de-seguranca-internacional. Acesso em 25 de agosto de 2022.

CARMONA, RONALDO.

Ameaças globais, multilateralismo e soberania. **Ameaças sem fronteiras:** Somos capazes de lidar com os desafios? KAS, 2022, p. 197-211. Disponível em https://www.cebri.org/br/doc/277/ameacas-sem-fronteiras-somos-capazes-de-lidar-com-os-desafios. Acesso em 25 de agosto de 2022.

CARMONA, RONALDO.

A guerra na Ucrânia: uma análise geopolítica. **CEBRI-Revista**, Ano 1, Número 3, 2022. Disponível em https://cebri-revista.emnuvens.com.br/revista/index. No prelo.

CARVALHO, PAULO SÉRGIO MELO DE.

A segurança cibernética e a tecnologia 5G no cenário brasileiro. CEBRI, dezembro de 2020. Disponível em https://www.cebri.org/br/doc/28/a-seguranca-cibernetica-e-a-tecnologia-5g-no-cenario-brasileiro. Acesso em 25 de agosto de 2022.

CARVALHO, PAULO SÉRGIO MELO DE; MARCONDES, CESAR AUGUSTO CAVALHEIRO.

Sociedade digital e impactos da tecnologia na ciberguerra. **Ameaças sem fronteiras:** Somos capazes de lidar com os desafios? KAS, 2022, p. 181-195. Disponível em https://www.cebri.org/br/doc/277/ameacas-sem-fronteiras-somos-capazes-de-lidar-com-os-desafios. Acesso em 25 de agosto de 2022.

Global Geopolitical Tensions and the Challenges of Strengthening Defense and National Security: preliminary comments

INTRODUCTION

The effects of the current disruptive transformations in International Security will not be limited to the short term but rather will be structural and long-term. The dominant feature of the international scenario in the first two decades of the 21st century was the systemic dispute between the United States, the victorious Cold War power, and China, a contesting and reemerging power that has been rising exponentially for over four decades, to some extent in consequence of Cold War geopolitical maneuvers. The key facet of that dispute for hegemony, which in contemporary history takes place over generations, are renewed and multidimensional threats to stability and international security. Therein lies the first disruption in the international scenario: the potential occurrence of a dispute for positions in the international system or of some hybrid solution represented by a protracted and multilevel struggle for a position of leadership.

Beginning in 2020, the world faced the threat of the Sars-Cov-2 virus, which quickly spread all over the planet and, in an extreme case scenario, imperiled the very survival of humankind. Some earlier trends gathered speed after the outbreak of the Covid-19 pandemic, including the digitization of the economy and of social interaction and the crisis in the international global order and in multilateralism by virtue of the increasing importance of national options within the system. In addition, some movements associated with so-called "deglobalization" and decoupling lead to the reversal, so far partial, of global chains, especially

for critical inputs. Although worldwide mass vaccination has minimized the global health risks posed by Covid-19, the effects of this pandemic on international geopolitics remain significant.

Finally, the armed conflict raging in the Ukraine since February 2022 is another recent international event that will have long-term influence on world geopolitics and on the security architecture consolidated after the end of World War II. The Russia-Ukraine war and the support North Atlantic Treaty Organization (NATO) countries have been giving the latter pose risks to international stability and deepen earlier trends such as the degradation of the multilateral system and the fragmentation of global chains. That war, the effects of the Covid-19 pandemic, and the United States-China dispute have significant consequences for international security, as well as for Brazil's defense and security. Against a backdrop of systemic confrontation where contemporary warfare offers new and unprecedented facets, this Policy Paper from the CEBRI Defense and International Security Program seeks to review the major challenges Brazil today faces and to propose some actions.

The CEBRI Defense and International Security Program was established in the current format in 2021 to help plug a gap. Under the aegis of CEBRI, a premier Brazilian and Southern Hemisphere think-thank, the group aims at building knowledge on Defense and International Security outside all Government structures, in similarity to major organizations in other countries, such as the US RAND Corporation and European institutes and foundations.

CHALLENGES

SYSTEMIC COMPETITION BETWEEN SUPERPOWERS

The world currently lives in an era of systemic competition between superpowers, in which one contender – China – seeks to consolidate its rise, and the other – the United States – seeks to curb the rise of the contestant and, at the same time, to reverse the relative loss of its power. Military confrontation between nation States, in particular between major powers, is the main classic threat to the security of the international system. The competition between China and the United States involves the risk of confrontation, especially of the non-kinetic and indirect kind now in course, both because they are nuclear powers and because of the complementarity between their economies, which, however, is diminishing with the decoupling movement. The threat of military confrontation between States is real, as the ongoing conflict between Russia and Ukraine shows. Going beyond the impending challenges to international security caused by the war, that dispute will also have long-term effects on international geopolitics and on the relationship between superpowers.

The crisis in the international order, and in globalization itself, creates challenges for Brazil, which maintains important relationships both with the United States and with China

spanning cultural, political, economic, technological and military aspects. Brazil will be required to take position in the competition between the two superpowers. But the national interest calls for shunning antagonistic or acute, exclusive positions. Brazil has the potential to become a world power. The country has a vast territory and large population, is a major supplier of food to the world, boasts a clean energy mix and faces no military threat to its security - although some significant antagonisms may flare up in the near future, as described in our Defense papers.

Merely identifying the risks and threats to Brazil's territorial integrity and sovereignty will be a major challenge for Brazil's Government and society. Actions to mitigate both, including in the fields of Defense and National Security, take a long time to bear fruit. Brazilians must urgently face the challenge of raising awareness in regard to the serious threats that now loom over the international scenario.

THE FOURTH INDUSTRIAL REVOLUTION AND THE TECHNOLOGICAL RACE

The competition between the United States and China unfolds in the midst of another structural phenomenon, the accelerated development of new technologies. The world is now seeing the first inklings of a new technical and scientific revolution – the Fourth Industrial Revolution -, with the coming of age of technologies that have great impact on productivity and work. Those emerging technologies – among which artificial

intelligence, big data algorithms and the multiplication of sensors in all things (Internet of Things - IoT) – are, by definition, *dual in nature*. As in prior Industrial Revolutions, the countries that dominate the technical and technological framework of this Fourth Revolution will lead the world in the 21st century.

The appearance of two information and communication technology "ecosystems" and of sensitive production chains will magnify the competition between States. Said ecosystems will be led by the US and China, in fierce technical and scientific competition. The international system will then be marked by a technological race between superpowers for leadership in the standards around which global productive forces will be organized in response to economic digitization and to technologies such as 5G.

The great powers have actively engaged in new industrial policies grounded on Science, Technology and Innovation (ST&I) and aiming at greater relative self-sufficiency in vital or critical inputs. The Covid-19 crisis has put wind in the sails of that process and caused increased protectionism, disruption of Global Value Chains and the "re-shoring" movement. In a nutshell, there is an increasingly direct relationship between the national security and industrial policy of major world powers.

The challenges and risks Brazil will have to meet in this scenario are associated with its dependence on global chains, especially for defense technologies and products. Recent events such as the Covid-19 pandemic and the Ukraine war

show that Brazil's dependence on foreign technologies to build its defense structure is one of the main risks for the country's security. And that risk becomes especially acute in a context including large-scale conflicts. The dearth of home-grown technological solutions reduces Brazil's room for maneuver in the current scenario and raises the risk of automatic alignment within the context of competition between the United States and China.

HYBRID WARFARE AND CYBERSECURITY

The new technologies and the disruptions they cause directly affect the stability of countries and of the international system. New technologies that allow for breaking up an opponent's national unity give warfare a hybrid character. Control of the metadata harvested from the 2/3 of humankind daily connected to the internet allows for novel and ever more stealthy strategic movements to destabilize an opponent. Contemporary warfare takes place permanently, under the guise of peace, with disinformation campaigns and psychological operations aimed at the masses.

The new social standards due to mass access to the internet and to the advent of social networks create highly critical vulnerabilities to national unity and to democracy itself. Actions on social networks, such as the dissemination of false information and rumors, the exposure of political leaders, the incitement of mistrust towards institutions, and interference in electoral processes can affect social cohesion within States.

Cyberwarfare is within reach for a greater number of countries, as well as for transnational criminal organizations.

Societies today are highly dependent on services and are therefore highly vulnerable to attacks against critical infrastructure. Hybrid warfare involves attacks against non-government businesses and infrastructure and thereby ultimately blurs the lines between government and non-government entities. The great powers are now designing a number of programs to mitigate those vulnerabilities, ranging from legal action to intelligence countermeasures. Within that context, one must consider what structures are necessary to confront such a threat. Those structures will require international cooperation because attacks come from transnational players.

Information and communications technologies have become indispensable for a State, its economy and social life to fully function. The gathering pace at which digitization penetrates the workplace, the political arena and social life has created opportunities but also challenges. In that regard, there is great effort to keep the cyberspace open, free and secure. *Open*, to promote universal, accessible and equal access to the internet and in particular to enable economic growth and innovation and to spark political, social and economic development worldwide. *Free*, to promote and protect human rights and fundamental freedoms, including freedom of expression, access to information, freedom of assembly and of association, the right to privacy and to a fair trial. *Secure*, to promote better cooperation and action against cybercrime, especially through the use of diplomatic and legal tools and by building resilience against cyberattacks.

Cyberattacks can cause serious damage to business facilities, services and assets in strategic industries such as the power industry, which, if disrupted or destroyed, will have major social, economic, political and security impacts. The increasingly digitized and automated management of the power industry requires advanced control resources at system endpoints and across system layers, which entails using well-designed measures and strictly managing information asset governance to facilitate the operation of the various systems within a business. Said digital transformation makes it likewise essential for government agencies to establish cybersecurity policies in protection of critical power assets and other infrastructure facilities.

Following the approval of the Federal Government Information and Communications Security and Cybersecurity Strategy in 2015 and of the National Information Security Policy in 2018, in early 2020 the Brazilian government launched the National Cybersecurity Strategy - E-Ciber. That document is part of the Brazilian Government's broader general strategic planning framework and is the first of the several thematic modules the National Strategy for Information Security will comprise as set out in the 2018 declaratory policy. The purpose of the Strategy is to seek best cybersecurity practices and to define the main strategic goals and objectives to spur and guide future action over the next four years. It is now time to review the Brazilian Government's strategic vision on how to keep the domestic cyberspace safe and to reflect on the initiatives required for E-Ciber to evolve from a declaratory policy into an effective cybersecurity strategy. It is likewise relevant to reflect if the original versions and

periodic reviews of the White Paper on National Defense; of the National Defense Strategy and of the National Defense Policy can raise awareness across Brazilian society of the cyber risks to national security and defense.

In addition to the National Cybersecurity Strategy, another important milestone for Brazilian cybersecurity was the enactment, in 2018, of the General Personal Data Protection Act (LGPD). That statute establishes rules on the collection, storage, processing and sharing of personal data so as to protect data processing operations involving information on identified or identifiable individuals in observance of the constitutional right to privacy. Created under the LGPD, the National Data Protection Authority (ANPD) was activated in October 2020 by the Brazilian Senate. The ANPD is responsible for overseeing the protection of personal data and of business and industrial secrets and for punishing any violations of pertinent law. Although those initiatives do contribute to foster cybersecurity centered on individual privacy, neither the LGPD nor the ANPD will suffice to objectively and specifically promote information security, meaning the protection of information, systems, resources and other assets against disasters, errors and unauthorized tampering, so as to reduce the likelihood and impact of any cybersecurity incident. It is necessary to reflect on strategies to reduce the risk of cyberattacks and the damage they cause to business and government information security and on the limits and potential of encryption to ensure information security and data protection in every branch of Brazil's Government and in Brazilian businesses.

BRAZIL'S DEFENSE AND NATIONAL SECURITY

The risks and threats stemming from the deterioration of the current international security environment have clear consequences for National Defense and, in a broader perspective, for National Security. Brazil's characteristics make the country a significant player in the international system and a regional power: its territory and population rank among the biggest in the world and its almost 17,000 kilometers of land borders touch almost all South American countries. Brazil must possess the military capacity to guarantee its security. The disputes in progress within the international system have repercussions in South America also, making it necessary for Brazil to have the military capacity to guarantee peace in the region and its security. Brazil must urgently relaunch a policy and strategy for South America and for its broader strategic surroundings, which include the South Atlantic and Africa.

Brazil's security faces no short- or long-term direct threat from other States, mainly because Brazil is located in a region with no major interstate conflicts. But that reality may change, as shown, say, by the securitization of the environmental issue in NATO's recent strategic update. Our South American environment is marked by the actions of non-state players, especially those associated with drug trafficking activities. Both violence within its borders and the guarantee of security along its borders already are challenges for Brazil. Efforts to address those problems require deep reflection and ample debate within Brazilian society.

Finally, within the context of Brazil's National Defense Policy and Strategy and of a potential new National Security Strategy, Brazil must rise to the challenge of modernizing and re-equipping its defense structure. Institutional adjustments and the reversal of budget instability - which makes it impossible to plan medium and long-term expenditures - are some of the challenges that must be resolved so that Brazil's Armed Forces and defense industry are able to meet the country's needs and to enhance the country's importance within the international system.

PROPOSALS

SYSTEMIC COMPETITION BETWEEN SUPERPOWERS

It is not in Brazil's national interest to associate either with the American or with the Chinese project within the context of the geopolitical rivalry between the two major powers. Brazil must assess **the systemic and circumstantial conditions that surround its choice of position** in view of the country's tradition of diplomatic independence and autonomy. Brazil ought to **remain in its traditional path** of promoting dialogue, consensus and respect for multilateralism and international law, and **avoid any alignment** in that dispute.

THE FOURTH INDUSTRIAL REVOLUTION AND THE TECHNOLOGICAL RACE

Within the context of the Fourth Industrial Revolution and of the systemic competition between the United States and China, Brazil must **build its independence from foreign-made systems and garner the technical skills necessary to maintain those systems** even in situations of crisis and potential embargoes. Brazil must **seek its own technological solutions** that can guarantee its self-sufficiency in a scenario of

systemic competition as the fourth industrial revolution unfurls. Brazil has to **think hard on which systems and technologies can be developed domestically and which should be found abroad**. Good international practice shows that it requires an institutional framework within the Brazilian Government that can adequately make those decisions. Both require logistical independence in the event of crisis or conflict. In other words, Brazil must **acquire equipment and be able to keep it in operation and in production** in the case of foreign embargo. Finally, Brazil will have a voice in international forums only if it is able to produce its own technologies.

The science, technology and innovation agendas of major world powers reflect an increasingly direct relationship between national security and industrial policy. Brazil should **give priority to the invigoration of its Defense Industrial Base (DIB)** - set of state and private companies that participate in one or more stages of the production of strategic defense products -, so that it can operate as a driver to incorporate science, technology and innovation into Brazil's industrial companies, goods and services and as a springboard for the Armed Forces to become technologically independent, mainly in sectors where Brazil has comparative technological advantages.

The stability and volume of funding available in the search for that self-sufficiency on critical technologies and systems will be vital. To reverse that vulnerability, Brazil's Government and society must first **raise their awareness of the risks and threats they face**, including those that involve other States. As an upshot of that increased awareness, all relevant parties in general and the National Congress in particular must debate how to create

stable sources of funding spanning several years ahead and at volumes commensurate with a country of our size, using as benchmark the National Defense average expenditure in other BRICS countries and in NATO countries, i.e., 2% of GDP.

HYBRID WARFARE AND CYBERSECURITY

Shape, when the National Defense Policy and Strategy next comes up for review, concepts and initiatives (countermeasures) that can focus on the risks associated with the hybrid, indirect and disguised format any attack on national sovereignty and territorial integrity will take.

Implement cybersecurity governance through the description and separation of roles, interfaces and modes of interaction between government and non-government entities and science and technology research institutes.

Promote closer cooperation within Brazilian society, at multiple levels and across several sectors, to foster the principles of cybersecurity.

Bolster the National Cyberincident Management Plan (PLANGIC) and more specific sectoral plans so as to give greater prominence and details to cyberdefense within National Defense Declaratory Policies such as the National Defense Strategy, the National Defense Policy and the White Paper on National Defense.

Create new regulatory strategies and incentives for better coordination between businesses in the power and telecommunications industries.

Maintain an assessment cycle to detect cybervulnerabilities in power facilities and structures associated with the electricity networks.

Create national risk profiles for suppliers of 5G technology equipment and for operators, internet providers and businesses with access to private 5G networks.

Use further accountability to **couple the security of the 5G system with the protection of user data**, in addition to the enactment of the General Personal Data Protection Act (LGPD) and to the activation of the National Data Protection Authority (ANPD).

Promote strategies to reduce the risk of cyberattacks and the damage they cause to business and government information security and to buttress information security in every branch of Brazil's Government and in Brazilian businesses.

Boost government investment in Science and Technology and encourage closer strategic alignment between development agencies in relation to national cyberdefense and security policies.

Promote international cooperation agreements and memoranda of understanding to enable the sharing of

information on cyberthreats, trends in cybercrime and in cyberattacks, latent vulnerabilities, new malware, and the exchange of cyberincident prevention and response methods.

BRAZIL'S DEFENSE AND NATIONAL SECURITY

The degradation and diminishing legitimacy of the contemporary international security environment and of multilateralism pose obvious risks to Brazil's National Defense and Security. **The periodic review of the National Defense Policy and Strategy needs to reflect that new reality and to spark the involvement** of multiple Government and societal players, seeking to raise their awareness of these risks and threats. A fast-track system akin to that used for congressional review of presidential provisional measures to **expedite Defense-related bills through Congress**. Several formats are now in debate at the Defense, Foreign Relations and Intelligence committees at Brazil's House of Representatives and Senate.

Brazil must acquire military significance to ensure its security and collective peace in South America. The **relaunch of the South American Defense Council (SDC)** is an urgent challenge. This is not an "ideological issue" but a matter of State, aiming, on the one hand, to increase the level of trust between South American countries, and, on the other hand, to curb the presence of extra-regional powers in our strategic immediate surroundings - South America. A similar effort is for the same reason necessary in relation to the South Atlantic,

focusing on the **urgent restructuring of ZOPACAS (South Atlantic Peace and Cooperation Zone)**.

Within the context of its declaratory defense policies, Brazil must **modernize and re-equip its Defense Structure** with an eye on the threats clearly identified and with emphasis on that portion of Brazilian territory (the Amazon) that now is a major locus of geostrategic tension at the global level. Brazil ought to therefore budget medium- and long-term expenditures to the tune of 2% of GDP, consistent with the investment levels seen in countries of similar geopolitical stature.

Society and the federal budget must give defense and security issues the importance they deserve so as to boost defense-related investment in science and technology, for those are key for national economic development. Finally, Brazil must **reflect on the threats to national security stemming from drug trafficking** and take action to address the consequences of that activity.

CONCLUSION

The growing instability of the international system and the transformations it is going through pose Defense and Security risks Brazil must be able to face. In a scenario of heightened systemic competition between the United States and China, Brazil should assume an independent position in relation to both superpowers. Brazil can potentially position itself as a player that helps build understanding and that maintains relationships with all countries around the globe.

The competition for mastery of and leadership in new technologies associated with the Fourth Industrial Revolution and with the digitization of social interactions and production processes is a key feature of the current international panorama and that competition may lead to the creation of two "echosystems" spearheaded by the US and by China. Brazil's dependence on foreign technologies poses great risks to national security. Brazil must act to create home-grown technological solutions and to guarantee the country's self-sufficiency against the backdrop of heightened systemic competition.

The innovation associated with the Fourth Industrial Revolution opens up a new battleground for international conflict and crime: cyberspace. Modern warfare is hybrid. New actions are required to guarantee national defense and to minimize vulnerabilities associated with the cyberspace. The Brazilian government must therefore be mindful of the growing challenges related to digitization and act so that

the National Cybersecurity Strategy can effectively ensure Brazil's cybersecurity. In the international arena, Brazil should cooperate with other States to establish agreements and to build trust networks that can address cyberthreats.

Finally, a country with Brazil's territorial, population, economic, geopolitical and diplomatic characteristics cannot be a passive bystander in the international system. Brazil's geopolitical statute gives it the capacity to act to promote peace within that system and to guarantee security not only in its immediate region - South America and the South Atlantic -, but elsewhere. To be able to do that, Brazil needs not only an active diplomacy but also the material capacity to project itself internationally. The modernization and re-equipment of its defense structure must then be a priority not only to provide means of action in the international arena but also because of the aftereffect of defense investment in other industries and because of its key role in national development.

REFERENCES

CARMONA, RONALDO.

Reflexões sobre a Geopolítica no contexto da quarta revolução industrial e dos novos desafios de segurança internacional. CEBRI, January 2022. Available at: https://cebri.org/br/doc/241/reflexoes-sobre-a-geopolitica-no-contexto-da-quarta-revolucao-industrial-e-dos-novos-desafios-de-seguranca-internacional. Retrieved on August 25, 2022.

CARMONA, RONALDO.

Ameaças globais, multilateralismo e soberania. **Ameaças sem fronteiras:** Somos capazes de lidar com os desafios? KAS, 2022, p. 197-211. Available at https://www.cebri.org/br/doc/277/ameacas-sem-fronteiras-somos-capazes-de-lidar-com-os-desafios. Retrieved on August 25, 2022.

CARMONA, RONALDO.

A guerra na Ucrânia: uma análise geopolítica. **CEBRI-Revista**, Year 1, Number 3, 2022. Available at https://cebri-revista.emnuvens.com.br/revista/index. In press.

CARVALHO, PAULO SÉRGIO MELO DE.

A segurança cibernética e a tecnologia 5G no cenário brasileiro. CEBRI, December 2020. Available at https://www.cebri.org/br/doc/28/a-seguranca-cibernetica-e-a-tecnologia-5g-no-cenario-brasileiro. Retrieved on August 25, 2022.

CARVALHO, PAULO SÉRGIO MELO DE; MARCONDES, CESAR AUGUSTO CAVALHEIRO.

Sociedade digital e impactos da tecnologia na ciberguerra. **Ameaças sem fronteiras:** Somos capazes de lidar com os desafios? KAS, 2022, p. 181-195. Available at https://www.cebri.org/br/doc/277/ameacas-sem-fronteiras-somos-capazes-de-lidar-com-os-desafios. Retrieved on August 25, 2022.

AUTORES | AUTHORS



ANDRÉ CLARK

Vice-Presidente Sênior para o hub América Latina da Siemens Energy e General Manager da Siemens Energy Brasil, tendo sido anteriormente presidente e CEO da Siemens Brasil e também CEO da ACCIONA para o Brasil, Bolívia, Uruguai e Paraguai. André nasceu em São Paulo e iniciou sua carreira no setor de Papel e Celulose em 1995. Com 17 anos de experiência nos segmentos de Energia, Óleo e Gás, Manufatura, Logística e Infraestrutura, André é graduado em Engenharia Química pela Universidade de São Paulo (USP) e possui MBA em Finance and Operations Management pela Stern School of Business, New York University. Com atuação ativa na liderança de associações e entidades de diversos segmentos de negócios, está presente nas mais importantes discussões sobre o Brasil. André é Presidente do Conselho de Administração da Associação Brasileira da Infraestrutura e Indústrias de Base (ABDIB); Vice-Presidente da Mesa Plenária da Associação Brasileira de Máquinas e Equipamentos (ABIMAQ); Membro do Conselho Empresarial do Grupo Econômico formado por Brasil, Rússia, Índia e China (BRICS); Membro do Comitê de Líderes da Confederação Nacional da Indústria e do Comitê de Líderes de Mobilização Empresarial para a Inovação (CNI / MEI); Membro do Conselho Curador do CEBRI e conselheiro dos núcleos Infraestrutura e Defesa e Segurança Internacional; Membro do Conselho Consultivo do GRI Club Brasil; Membro do Conselho Superior da Câmara de Comércio Internacional (ICC); Membro do Conselho de Administração e Presidente do Conselho de Transformação Digital do Instituto Brasileiro de Petróleo, Gás e Biocombustíveis (IBP).

André Clark is Senior Vice President for the Siemens Energy hub in Latin America and General Manager of Siemens Energy Brazil, having previously been President and CEO of Siemens Brazil and also CEO of ACCIONA for Brazil, Bolivia, Uruguay and Paraguay. André was born in São Paulo and began his career in the Pulp & Paper industry in 1995. With 17 years of experience in Energy, Oil & Gas, Manufacturing, Logistics and Infrastructure segments, André holds a degree in Chemical Engineering from the University of São Paulo (USP) and an MBA in Finance and Operations Management from Stern School of Business, New York University. With an active role in leading associations and entities from different business segments, he is present in the most important discussions about Brazil. André is President of the Administrative Council of the Brazilian Association of Infrastructure and Basic Industries (ABDIB); Vice-president of the Plenary Board of the Brazilian Association of Machinery and Equipment (ABIMAQ); Member of the Business Council of the Economic Group formed by Brazil, Russia, India and China (BRICS); Member of the Leaders Committee of the National Confederation of Industries and of the Leaders Committee of Business Mobilization for Innovation (CNI /MEI); Member of the Board of Trustees of the Infrastructure and the Defense and International Security Programs (CEBRI); Member of the Advisory Board of GRI Club Brasil; Member of the Superior Council of the International Chamber of Commerce (ICC); Member of the Board of Directors and President of the Digital Transformation Council of the Brazilian Institute of Oil, Gas and Biofuels (IBP).

PAULO SERGIO MELO DE CARVALHO

General de Divisão da Reserva do Exército Brasileiro, com graduação em Comunicações na Academia Militar das Agulhas Negras. Cursou todos os cursos regulares do Exército Brasileiro, sendo Doutor em Ciências Militares e especialista em Tecnologia da Informação e Comunicações (TIC), com atuação na área de Cibernética nos níveis político-estratégico e operacional-técnico. Realizou, ainda, o Curso de Economia de Defesa, no Centro Hemisférico para Estudos de Defesa, nos Estados Unidos da América, e os cursos de pós-graduação MBA Executivo e MBA em Administração Estratégica de Sistemas de Informação, ambos da Fundação Getúlio Vargas. Chefiou o Centro de Defesa Cibernética, de 2014 a 2016, e foi o primeiro comandante do Comando de Defesa Cibernética, criado em 2016. Atualmente, presta consultoria em TIC e Cibernética, participando na capacitação de recursos humanos, no Brasil e no exterior.

Paulo Sérgio Melo de Carvalho is a reserve Lieutenant General for the Brazilian Army. He is a specialist in Information Technology and Communications and has acted in the cybernetics area at the political/strategic and operational/technical levels, having headed the Cybernetic Defense Center between 2014 and 2016 and becoming the first commander of the Cybernetic Defense Command, created in 2016. Currently, he is a consultant for the cybernetic sector and participates in human resources capacitation, in Brazil and abroad.

RONALDO CARMONA

PhD (Doutor) e MPhil (Mestre) em Geografia pela Universidade de São Paulo (USP), com Tese e Dissertação em teoria geopolítica. É Professor de Geopolítica da Escola Superior de Guerra (ESG), onde ministra aulas aos cursos de Altos Estudos em Política e Estratégia, de Estado Maior Conjunto e de Inteligência Estratégica, dentre outros. Ainda na ESG, coordena o Grupo de Pesquisa sobre Guerra. É professor colaborador do Programa de Mestrado em Engenharia Aeroespacial da Universidade Federal do Maranhão (UFMA). É coordenador adjunto da Rede de Pesquisa sobre a Amazônia Azul. Recém organizou o livro Geopolítica e Energia (Editora Synergia, 2020), fruto de cursos ministrados, desde 2019, à Agência Nacional do Petróleo (ANP). Foi Chefe de Planejamento do Ministério da Defesa, com responsabilidades pela revisão quadrienal da Política e da Estratégia Nacional de Defesa. Foi assessor para projetos estratégicos nacionais da presidência da FINEP, a agência brasileira de Inovação do Ministério da Ciência, Tecnologia e Inovação (MCTI). Foi ainda conselheiro da Associação Brasileira da Indústria de Defesa (ABIMDE) e membro do Departamento da Indústria de Defesa da Federação da Indústria do Estado de São Paulo (FIESP). Assessorou também, como acadêmico, as presidências da Comissão de Relações Exteriores e Defesa Nacional (CREDN) da Câmara dos Deputados e da Comissão de Controle das Atividades de Inteligência (CCAI) do Congresso Nacional.

Ronaldo Carmona holds a Ph.D. (Doctor) and MPhil (Master) in Geography from the University of São Paulo (USP), with a Thesis and Dissertation in Geopolitical Theory. He is a Professor of Geopolitics at the Escola Superior de Guerra (ESG), where he teaches courses in Advanced Studies in Politics and Strategy, Joint General Staff, and Strategic Intelligence. He coordinates the War Research Group at ESG. He is a collaborating professor of the Master's Program in Aerospace Engineering at the Federal University of Maranhão (UFMA). He is deputy coordinator of the Research Network on the Blue Amazon. He recently organized the book Geopolítica e Energia (Editora Synergia, 2020), the result of courses given since 2019 to the National Petroleum Agency (ANP). He was Head of Planning at the Ministry of Defense, with responsibility for the quadrennial review of the National Defense Policy and Strategy. He was an advisor for national strategic projects to the presidency of FINEP, the Brazilian Innovation Agency of the Ministry of Science, Technology, and Innovation (MCTI). He was also a member of the Brazilian Defense Industry Association (ABIMDE) and member of the Defense Industry Department of the Federation of Industry of the State of São Paulo (FIESP). He also advised, as an academic, the presidencies of the Committee on Foreign Affairs and National Defense (CREDN) of the Chamber of Deputies and the Committee for the Control of Intelligence Activities (CCAI) of the National Congress.

CONSELHO CURADOR | BOARD OF TRUSTEES

Presidente do Conselho Curador
| Chairman

José Pio Borges

Presidente De Honra
| Honorary Chairman

Fernando Henrique Cardoso

Vice-Presidentes
| Vice-Chairmen

José Alfredo Graça Lima
Jorge Marques de Toledo Camargo

Fundadores
| Founders

Carlos Mariani Bittencourt
Celso Lafer
Daniel Klabin
Gelson Fonseca Jr.
João Clemente Baena Soares
Marcus Vinicius Pratini de Moraes
Maria do Carmo (Kati) Nabuco de Almeida Braga
Roberto Teixeira da Costa
Eliezer Batista da Silva *(in memoriam)*
Luciano Martins de Almeida *(in memoriam)*
Luiz Felipe Palmeira Lampreia *(in memoriam)*
Luiz Olavo Baptista *(in memoriam)*
Sebastião do Rego Barros *(in memoriam)*
Walther Moreira Salles *(in memoriam)*

Vice-Presidentes Eméritos
| Vice-Chairmen Emeriti

Daniel Klabin
José Botafogo Gonçalves
Luiz Augusto de Castro Neves
Rafael Benke

Conselheiros Eméritos
| Trustees Emeriti

Izabella Teixeira
Luiz Felipe de Seixas Corrêa
Luiz Fernando Furlan
Marcos Azambuja
Pedro Malan
Rubens Ricupero
Winston Fritsch

Conselheiros
| Trustees

Ana Toni
André Lara Resende
André Clark
Armando Mariante
Armínio Fraga
Cláudio Frischtak
Clarissa Lins
Demétrio Magnoli
Edmar Bacha
Francisco Müssnich
Henrique Rzezinski
Ilona Szabó
Joaquim Falcão
José Aldo Rebelo
José Luiz Alquéres
Luiz Ildefonso Simões Lopes
Marcos Galvão
Paulo Hartung
Pedro Henrique Mariani
Renato Galvão Flôres Júnior
Roberto Abdenur
Roberto Jaguaribe
Ronaldo Veirano
Sergio Amaral
Tomas Zinner
Vitor Hallack

ASSOCIADOS | MEMBERS

Aegea
Air Products
Altera
Australian Embassy in Brazil
BAMIN
Banco Bocom BBM
BASF
BAT Brasil
Bayer
BMA Advogados
BRF
Bristow
Brookfield Brasil
CCCC/Concremat
Chinese Embassy in Brazil
Consulate General of Ireland, São Paulo
Consulate General of Mexico in Rio de Janeiro
CTG Brasil
Dynamo
EDF Norte Fluminense
EDP
Eletrobras
Embassy of Switzerland in Brazil
Embraer
ENEVA
ENGIE Brasil
Equinor
ExxonMobil
FCC S.A.
Furnas
Galp
Grupo Lorentzen
Grupo Ultra
Haitong
Huawei
IBÁ
IBRAM
Icatu Seguros
Instituto Clima e Sociedade
Itaú Unibanco
Klabin
Light
Machado Meyer
Mattos Filho Advogados
Microsoft
Museu do Amanhã
Neoenergia
Netherlands consulate-general in Rio de Janeiro
PATRI
Petrobras
Pinheiro Neto Advogados
Promon Engenharia
Prumo Logística
Repsol Sinopec
Royal Norwegian Consulate in Rio de Janeiro
Sanofi
Santander
Shell
Siemens
Siemens Energy
SPIC Brasil
State Grid
Suzano
Total E&P do Brasil
Unilever
Vale
Veirano Advogados
Vinci Partners

EQUIPE | TEAM

DIRETORIA
| EXECUTIVE BOARD

Diretora-Presidente
| CEO
Julia Dias Leite

Diretora de Relações Externas
| Director of External Affairs
Carla Duarte

Diretora de Projetos
| Director of Projects
Luciana Gama Muniz

Diretor Acadêmico
| Academic Director
Feliciano Sá Guimarães

Diretora Administrativa Financeira
| Administrative Financial Director
Ana Paula Marotte

PROJETOS
| PROJECTS

Diretora Adjunta de Projetos
| Deputy Director of Projects
Marianna Albuquerque

Coordenadores de Projetos
| Project Coordinator
Léa Reichert
Paulo Robilloti
Barbara Brant
Thais Jesinski Batista

Analistas de Projetos
| Project Analyst
Eduardo Neiva Souza
Larissa Vejarano

Estagiário
| Intern
Daniel Fontes

RELAÇÕES EXTERNAS
| EXTERNAL AFFAIRS

Diretora Adjunta de Relações Externas
| Deputy Director of External Affairs
Fernanda Araripe

Diretora Adjunta de Captação de Projetos
| Deputy Director of Fundraising
Maria Eduarda Marques

Coordenadora de Parcerias
| Partnership Coordinator
Cintia Reschke Borba Hoskinson

Coordenador de Relações Institucionais
| Institutional Relations Coordinator
Fernando Mattos

EQUIPE | TEAM

Coordenador de Projetos Especiais
| Special Projects Coordinator
Caio Vidal

Analista de Projetos Especiais
| Special Projects Analyst
Lucas Bilheiro

Assistente de Parcerias
| Partnership Assistant
Beatriz Pfeifer

Estagiário
| Intern
Heron Fiório

COMUNICAÇÃO E EVENTOS
| COMMUNICATIONS AND EVENTS

Gerente de Eventos
| Events Manager
Nana Villa Verde

Analista de Eventos
| Events Analyst
Adriano Andrade

Analista de TI
| IT Analyst
Eduardo Pich

Assistente de Eventos
| Events Assistant
Isabella Ávila

Assistente de Comunicação
| Communications Assistant
Daniele Thomaselli

ADMINISTRATIVO E FINANCEIRO
| ADMINISTRATIVE AND FINANCIAL

Gerente Administrativa-Financeira
| Administrative-Financial Manager
Fernanda Sancier

Analista Administrativo
| Administrative Analyst
Bruno Garcia

Analista Financeiro
| Financial Analyst
Eliana Mello

FICHA TÉCNICA | CREDITS

Tradução
| Translation
Andrei Winograd

Revisão de texto
| Editing
Wilma R. d' Oliveira Kroff

Projeto Gráfico
| Graphic Design
[Marijaguar Studio]
Mariana Jaguaribe L. Resende

Assistente Design
| Design Assistant
Heloisa Sato

cebri.org.br | cebri@cebri.org.br

LinkedIn CEBRI | **Facebook** /cebrionline **| Twitter** @cebrionline
Instagram @cebrionline **| Youtube** /CEBRIonline

R. Marquês de São Vicente, 336 | Gávea | Rio de Janeiro | RJ | 22451-044 | +55 (21) 2206-4400

CEBRI POLICY PAPERS

PENSAR
TO THINK
DIALOGAR
TO DIALOGUE
DISSEMINAR
TO DISSEMINATE
INFLUENCIAR
TO INFLUENCE

#2 THINK TANK BRASIL | *BRAZIL*
#2 THINK TANK AMÉRICA LATINA | *LATIN AMERICA*

University of Pennsylvania | Think Tanks and Civil Societies Program Index

SOBRE **O CEBRI**

O CENTRO BRASILEIRO DE RELAÇÕES INTERNACIONAIS É O THINK TANK REFERÊNCIA EM RELAÇÕES INTERNACIONAIS NO BRASIL, O SEGUNDO DA AMÉRICA DO SUL E CENTRAL. É UMA INSTITUIÇÃO SEM FINS LUCRATIVOS, APARTIDÁRIA E INDEPENDENTE QUE HÁ 24 ANOS SE DEDICA À PROMOÇÃO DO DEBATE PLURAL E PROPOSITIVO SOBRE A POLÍTICA EXTERNA BRASILEIRA. ESTÁ ESTRUTURADO A PARTIR DE 14 NÚCLEOS TEMÁTICOS, VOLTADOS A CONTRIBUIR PARA A INSERÇÃO INTERNACIONAL DO PAÍS E À FORMULAÇÃO DE POLÍTICAS PÚBLICAS COM ESTE OBJETIVO. COM MAIS DE 100 ASSOCIADOS DOS MAIS RELEVANTES SEGMENTOS, A REDE DO CEBRI REÚNE E MOBILIZA ESPECIALISTAS DE ÁREAS DE ATUAÇÃO E LINHAS DE PENSAMENTO DIVERSAS, ALÉM DE ORGANIZAÇÕES EM TODO O MUNDO.

ABOUT **CEBRI**

THE BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS (CEBRI) IS THE REFERENCE THINK TANK FOR FOREIGN AFFAIRS IN BRAZIL AND THE SECOND BEST THINK TANK IN SOUTH AND CENTRAL AMERICA. AN INDEPENDENT, NON-PARTISAN AND NON-PROFIT INSTITUTION, FOR 24 YEARS CEBRI HAS BEEN PROMOTING A PLURAL AND PROPOSAL-ORIENTED DEBATE ABOUT BRAZIL'S FOREIGN POLICY. IT IS STRUCTURED AROUND FOURTEEN THEMATIC PROGRAMS THAT CREATE POSITIVE CONTRIBUTIONS AND RECOMMENDATIONS FOR POLICY MAKING AND THE COUNTRY'S INTERNATIONAL AGENDA. CEBRI'S DIVERSE NETWORK COMPRISES MORE THAN 100 MEMBERS FROM A BROAD RANGE OF SECTORS, AND GATHERS SPECIALISTS FROM VARIOUS FIELDS OF EXPERTISE AND THOUGHT, AS WELL AS PARTNER INSTITUTIONS FROM AROUND THE WORLD.

CEBRI

“O Brasil possui características – territoriais, populacionais, econômicas, geopolíticas e diplomáticas – que não permitem que o país seja um ator reativo no sistema internacional. O Brasil tem capacidades para atuar no sentido de promover a paz nesse sistema e garantir a segurança não apenas da região em que está inserido – a América do Sul e o Atlântico Sul -, mas também de outras, dado seu porte geopolítico. Para isso, se faz necessário que além de uma diplomacia ativa, o país tenha capacidades materiais de se projetar internacionalmente. A modernização e o reequipamento de sua estrutura de defesa, portanto, devem ser prioridades, e não apenas para garantir meios de ação no sistema internacional, mas também porque esse tipo de investimento tem desdobramentos nos demais setores da economia e é chave para o desenvolvimento nacional.”

A country with Brazil’s territorial, population, economic, geopolitical and diplomatic characteristics cannot be a passive bystander in the international system. Brazil’s geopolitical statute gives it the capacity to act to promote peace within that system and to guarantee security not only in its immediate region - South America and the South Atlantic -, but elsewhere. To be able to do that, Brazil needs not only an active diplomacy but also the material capacity to project itself internationally. The modernization and re-equipment of its defense structure must then be a priority not only to provide means of action in the international arena but also because of the aftereffect of defense investment in other industries and because of its key role in national development.