1/6

KONRAD ADENAUER STIFTUNG

Cibersegurança na América Latina

Cybersecurity in Latin America

Monica Herz

CEBRI
BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS

COLEÇÃO DE POLICY PAPERS
THE POLICY PAPERS COLLECTION

XVIFORTE

A Conferência de Segurança Internacional do Forte de Copacabana é um projeto euro-brasileiro organizado em conjunto pela Fundação Konrad Adenauer (KAS) e pelo Centro Brasileiro de Relações Internacionais (CEBRI), com apoio da Delegação da União Europeia no Brasil. A conferência é concebida como um fórum de diálogo entre a América do Sul e a Europa. Seu objetivo é reunir especialistas do setor governamental, acadêmico e privado para discutir assuntos atuais no âmbito de segurança que sejam de interesse comum aos parceiros dos dois lados do Atlântico. Desde seu início em 2003, a conferência se transformou, de uma reunião relativamente pequena, no maior fórum de segurança da América Latina. Na sua 16ª edição, a conferência de 2019 tem como tema 'A Quarta Revolução Industrial: Impactos na Segurança Internacional e a Reformulação da Ordem Global'. A conferência é aberta ao público e os participantes são incentivados a participar ativamente das discussões. Esta coleção de Policy Papers reflete os temas centrais do evento e pretende identificar desafios, bem como fazer recomendações políticas para o futuro. As edições anteriores da publicação sobre Segurança Internacional da Conferência do Forte de Copacabana podem ser acessadas na página oficial da KAS Brasil (www.kas.de/brazil).

The Forte de Copacabana International Security Conference is a joint Euro-Brazilian project organised by the Konrad Adenauer Foundation (KAS) in partnership with the Brazilian Center for International Relations (CEBRI) and supported by the Delegation of the European Union to Brazil. The conference is conceived as a forum for dialogue between South America and Europe. It aims to bring together experts from a wide range of government, academic and private-sector backgrounds to discuss current security-related issues which are of interest to the partners on both sides of the Atlantic. Since its inception in 2003, the conference has emerged from a relatively small gathering to Latin America's largest security forum to date. The topic of the 16th edition of the conference is 'The Fourth Industrial Revolution: Impacts on International Security and the Reshaping of Global Order'. The conference is open to the public and the audience is encouraged to actively engage in discussions. This collection of Policy Papers reflects the major themes of the event and intends to identify challenges as well as make policy recommendations for the future. Previous volumes of the Forte de Copacabana International Security Conference publication can be accessed on the KAS-Brazil Office website (www.kas.de/brazil).

www.kas.de/brasil

Editor Editor
Anja Czymmeck

Coordenação editorial Project Coordination
Ariane Costa
Reinaldo Themoteo

Colaboração Editorial Support
Monique Sochaczewski

Tradução e revisão Translation and Revision
Leslie Sasson Cohen

Projeto Gráfico Design
Charles Steiman
Daniela Knorr

Impressão Print
Stamppa

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

COLEÇÃO DE POLICY PAPERS
THE POLICY PAPERS COLLECTION

1/6
Cibersegurança na América Latina
Cybersecurity in Latin America
Monica Herz

2/6
A quarta revolução industrial: Impactos na Segurança Internacional e a Reestruturação da Ordem Mundial - A perspectiva europeia
The Fourth Industrial Revolution: Impacts on International Security and the Reshaping of Global Order – The European Perspective
Kai Michael Kenkel

3/6
Inteligência artificial (IA) no balanço de poder na política internacional: uma perspectiva sul-americana
Artificial intelligence (AI) in the balance of power in world politics: a South American perspective
Jorge H. C. Fernandes

4/6
A Cibersegurança em um mundo conectado
Cybersecurity in a connected word
Pedro Veiga

5/6
Incorporação de gênero na segurança internacional da América do Sul: Big Data, Regionalismo e Difusão de Normas
Gender Mainstreaming in South America's International Security: Big Data, Regionalism and Norm Diffusion
Mariana Kalil

6/6
O Fator Gênero na Segurança Internacional
A Perspectiva Europeia
The Gender Factor in International Security
A European Perspective
Irene Giner-Reichl

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.

A Delegação da União Europeia (UE) no Brasil é uma das mais de 130 Delegações da UE no mundo. A Delegação da UE no Brasil está focada na promoção das relações políticas e econômicas entre a UE e o Brasil, de acordo com a parceria estratégica EU–Brasil estabelecida em 2007. A UE e o Brasil estabeleceram relações diplomáticas em 1960, criando estreitos laços históricos, culturais, econômicos e políticos. Dentre os tópicos centrais da parceria estratégica entre a UE e o Brasil 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. Mais de 30 diálogos formais no setor político foram iniciados entre a União Europeia e autoridades brasileiras para enfrentar esses desafios. Além disso, a União Europeia e o Brasil são parceiros comerciais importantes e os países da União Europeia recebem mais de 20% da exportação brasileira. A União Europeia também é o maior investidor estrangeiro no Brasil com cerca de 60% do investimento estrangeiro.

The European Union (EU) Delegation to Brazil is one of over 130 EU Delegations around the world. The EU Delegation to Brazil is focused on promoting political and economic relations between the EU and Brazil, in line with the EU–Brazil Strategic Partnership established in 2007. The EU and Brazil established diplomatic relations already in 1960 building on close historical, cultural, economic and political ties. Central topics of the EU–Brazil Strategic Partnership 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. Over 30 formal sector-policy dialogues between the European Union and Brazilian authorities have been initiated to address these challenges. The European Union and Brazil are also important trading partners and the countries of the European Union account for over 20% of Brazil's exports. The European Union is also the largest foreign investor in Brazil with around 60% of the foreign investment originating from the European Union.

CEBRI
BRAZILIAN CENTER FOR
INTERNATIONAL RELATIONS

Independente, apartidário e multidisciplinar, o Centro Brasileiro de Relações Internacionais (CEBRI) é uma instituição sem fins lucrativos, que atua para influenciar positivamente a construção da agenda internacional do país. Fundado há 20 anos por um grupo de empresários, diplomatas e acadêmicos, o CEBRI tem ampla capacidade de articulação, engajando os setores público e privado, a academia e a sociedade civil. Além disso, conta com um Conselho Curador atuante e formado por figuras proeminentes, e com uma rede de mantenedores constituída por instituições, empresas e indivíduos de múltiplos segmentos.

O CEBRI promove a expansão e aprofundamento do debate sobre a política externa brasileira e a inserção do Brasil no mundo, pautado na formulação de políticas públicas e no fomento de diálogo entre os mais relevantes atores brasileiros e globais. O reconhecimento de sua importância internacional é atestado pelo ranking do Programa de Think Tanks e Sociedade Civil da Universidade da Pensilvânia, que destacou o CEBRI como o segundo melhor think tank do Brasil e o quarto melhor da América Latina.

Independent, nonpartisan and multidisciplinary, the Brazilian Center for International Relations (CEBRI) is a non-profit institution that acts to have a positive influence on the construction of the country's international agenda. Founded 20 years ago by a group of business leaders, diplomats and academics, CEBRI has the ability to engage the public and private sectors, academia and civil society. In addition, it counts on an engaged Board of Trustees formed by prominent figures and on a diverse network of sponsors made up of institutions, companies and individuals from multiple sectors.

CEBRI promotes the expansion and deepening of debates on Brazilian foreign policy and Brazil's international insertion, marked by the formulation of public policies and the promotion of dialogue amongst the most relevant Brazilian and global stakeholders. The recognition of its international importance is evidenced by the University of Pennsylvania's Think Tanks and Civil Societies Program, which ranked CEBRI as Brazil's second best think tank and the fourth best in Latin America.

Monica Herz
Mônica Herz é professora associada da Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio) e diretora adjunta de pesquisa do Centro de Ciências Sociais da PUC-Rio. Ela é doutora pela Escola de Economia e Ciência Política de Londres e escreveu três livros e vários artigos sobre governança global, segurança da América Latina e política externa brasileira.

Mônica Herz is an associate professor at the Pontifical Catholic University of Rio de Janeiro (PUC-Rio) and Associate Dean for Research of the Social Science Center at PUC-Rio. She has a PhD degree from the London School of Economics and Political Science and has written three books and several articles on global governance, Latin American security and Brazilian foreign policy.

Cibersegurança na América Latina

Cybersecurity in Latin America

Monica Herz

Instituto de Relações Internacionais | PUC-Rio

Institute of International Relations | PUC-Rio

Introdução

O objetivo deste artigo é debater a governança da segurança regional na América Latina e a interação cibernética. Seu foco é em Tecnologias de Informação e Comunicação (TICs), os desafios regionais de segurança e formas de cooperação.

A Quarta Revolução Industrial envolve mudanças na interação social e na economia política, incluindo nova relevância para a inteligência artificial, robótica, internet das coisas, veículos autônomos, computação quântica, ciência dos materiais, nanotecnologia, impressão 3D, biotecnologia e armazenamento de energia. Essas tecnologias e conhecimentos desenvolvem-se uns a partir dos outros e amplificam uns aos outros (Schab, 2016). Os sistemas de consumo, produção, entrega e transporte estão sendo transformados. Neste contexto, o debate sobre segurança internacional e regional será inevitavelmente e dramaticamente modificado. As práticas tradicionais de Estados, empresas e sociedade civil que são movidas pelo desafio tecnológico e que também o movem, desafiam os limites disciplinares e nossa compreensão sobre capacidades e papéis sociais.

A segurança cibernética é um conceito contestado, mas aqui nos referiremos à proteção ou defesa da infraestrutura do Estado, suas redes, dados e usuários, o trabalho realizado pelas forças de segurança, a prevenção e as ações contra crimes no campo digital (cibercrimes)

Introduction

The aim of this paper is to debate regional security governance in Latin America and Cyberinteraction. It´s focus is on Information and Communication Technologies (ICTs), regional security challenges and forms of cooperation.

The Fourth Industrial Revolution involves changes to social interactions and the political economy including new relevance for artificial intelligence, robotics, the internet of things, autonomous vehicles, quantum computing, material science, nanotechnology, 3D printing, biotechnology and energy storage. These technologies and knowledge build on each other and amplify each other (Schab, 2016). Consumption, Production, delivery and transportation systems are being transformed. In this context the debate on international and regional security will be inevitably and dramatically changed. The traditional practices of countries, corporations and civil society that are moved by the technological upheaval and are, ate the same time, its drivers, challenge disciplinary boundaries and our understanding of capacities and social roles.

Cybersecurity is a contested concept but here we will refer to the protection or defense of the infrastructure of the country, its networks, data and users, the work performed by security forces, prevention and actions

against crimes in the digital field (cybercrime) and surveillance activities conducted by the State and corporations. Availability, confidentiality and integrity are the objectives that move this agenda. Cybersecurity involves two important aspects that we shall treat separately in this policy brief: threats to infrastructure and communication systems stemming from the intentional or non-intentional behavior of actors that may be described as enemies or criminals and threats to the human rights international, regional and national regimes and to democratic rights. Moreover, in this text we shall focus on the forms of cooperation on a regional basis to deal with such threats.

Threats to Infrastructure and Communication Systems

The multi-layered structure of cyberspace, in conjunction with the propensity of societies to increasingly depend on ICTs to control many of their critical infrastructure and communication systems, has raised growing cybersecurity concerns amongst specialists. Hostile operations against ICTs can take various forms, including "cyber-attacks" that seek to disrupt and destroy computer systems and networks, and "cyber exploitations" that concentrate on clandestine information collection. In both cases vulnerabilities become knowledge controlled by the State or actors (criminals or enemies) seeking to create disruption, pain and destruction. We are struggling to apply concepts developed in strategic and defense studies and criminology to this reality. At the same time, we are adapting to an array of new concepts: cyberwarfare, cyberdefense, hacktivism, cyber military doctrine, cyberterrorism and others. Dealing with cyber-criminal activity is extremely difficult as covering digital tracks after cyberattacks is easy and fast. Thus, attribution is a huge problem. More poignantly technology and cyberspace are changing faster than countries can legislate internally and negotiate externally.

According to the Rand Corporation "Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation´s computers or information networks through, for example, computer viruses or denial-of-service attacks [8]. The dissemination of these practices may produce security dilemma situations as a growing number of countries (approximately 50) invest in ICT military offensive and defensive capabilities increasing the risk of escalation of the weapon buildup and perceptions of threats. The arms control and disarmament mechanisms and humanitarian law have yet to properly respond to the challenges of cyberwarfare.

Nevertheless, attempts to build global governance mechanisms are being pursued in order to deal with the dramatic changes in social interaction produced by the Fourth Industrial Revolution. Global governance includes the development of cybersecurity norms, confidence-building measures, and capacity building. Since 2004, five UN GGEs (Group of Governmental Experts on Developments in the Field of Information and Telecommunications) studied the threats posed using ICTs in the context of international security and how these threats should be addressed. Their recommendations have been accepted by the UN General Assembly.

Through Russia´s initiative, the General Assembly decided to establish an Open-Ended Working Group (OEWG) available to all UN Member States through the adoption of Resolution 73/27[9]. The Group will convene for the first time in September 2019 and will report back to the UNGA in 2020 during its 75th session. The mandate of the OEWG includes consultative meetings with the private sector, NGOs and the academia.

Moreover, the General Assembly also established a new GGE through the adoption of resolution 73/266, tabled by the United States[10]. The Group will hold its first meeting in December 2019 and submit its report in 2021 during the UNGA's 76th session. Composed by 25 experts based on equitable geographical distribution, the Group will meet twice in New York and twice in Geneva. Prior to them, consultations on the subject will be held with regional organizations.

The Budapest Convention on Cybercrime has become a reference for the generation of norms on cybercrimes. It requires parties to criminalize illegal access, illegal interception, data interference, system interference, misuse of devices and computer-related forgery. The Convention divides cybercrime into four parts: offenses against the confidentiality, integrity and availability of computer data and systems (hacking, phishing, espionage, interception, interference); content-related offenses (child

e a vigilância de atividades conduzidas pelo Estado e por empresas. Disponibilidade, confidencialidade e integridade são os objetivos que movem essa agenda. A segurança cibernética envolve dois aspectos importantes que trataremos separadamente neste artigo: ameaças a infraestruturas e sistemas de comunicação decorrentes do comportamento intencional ou não intencional de atores que podem ser descritos como inimigos ou criminosos e, ameaças aos regimes de direitos humanos internacionais, regionais e nacionais e aos direitos democráticos. Além disso, neste texto, vamos nos concentrar nas formas de cooperação regional para lidar com tais ameaças.

Ameaças aos Sistemas de Infraestrutura e Comunicação

A estrutura multicamadas do ciberespaço, em conjunto com a propensão das sociedades a dependerem cada vez mais das TIC para controlar muitas de suas infraestruturas críticas e seus sistemas de comunicação, tem aumentado as preocupações com relação à segurança cibernética entre os especialistas. As operações hostis contra as TICs podem assumir várias formas, incluindo "ciberataques", que buscam perturbar e destruir sistemas e redes de computadores e "explorações cibernéticas", que se concentram na coleta clandestina de informações. Em ambos os casos, as vulnerabilidades tornam-se conhecimento controlado pelo Estado ou pelos atores (criminosos ou inimigos) que procuram criar ruptura, dor e destruição. Estamos lutando para aplicar conceitos desenvolvidos em estudos estratégicos e de defesa e de criminologia para esta realidade. Ao mesmo tempo, estamos nos adaptando a uma série de novos conceitos: guerra cibernética, defesa cibernética, *hacktivismo*, doutrina militar cibernética, *ciberterrorismo* e outros. Lidar com o *cibercrime* é extremamente difícil, pois cobrir as trilhas digitais após ataques cibernéticos é fácil e rápido. Deste modo, a atribuição é um grande problema. Além disso, a tecnologia e o ciberespaço estão mudando mais rapidamente do que a capacidade que os países têm de legislarem internamente e negociarem externamente.

De acordo com a Rand Corporation, "guerra cibernética envolve as ações de um Estado-nação ou organização internacional para atacar e tentar danificar computadores ou redes de informação de outra nação através, por exemplo, de vírus de computador ou ataques de negação de serviço (*Denial of Service attack*)[1]. A disseminação dessas práticas pode produzir situações de dilema de segurança, à medida que um número crescente de Estados (aproximadamente 50) investe em capacidades ofensivas e defensivas de TIC, aumentando o risco de escalada do estoque de armamento e percepção de ameaças. Os mecanismos de controle de armas e desarmamento e o direito humanitário ainda não responderam adequadamente aos desafios da guerra cibernética.

No entanto, há uma busca por construir mecanismos de governança global para lidar com as mudanças dramáticas na interação social produzidas pela Quarta Revolução Industrial. A governança global inclui o desenvolvimento de normas de cibersegurança, medidas de construção de confiança e capacitação. Desde 2004, cinco GGEs da ONU (Grupo de Especialistas Governamentais no Campo da Informação e Telecomunicações) estudaram as ameaças representadas pelas TICs no contexto da segurança internacional e como essas ameaças devem ser abordadas. Suas recomendações foram aceitas pela Assembleia Geral da ONU.

Por iniciativa da Rússia, a Assembleia Geral da ONU decidiu estabelecer um Grupo de Trabalho Aberto (OEWG) disponível a todos os Estados-membros da ONU por meio da adoção da Resolução 73/27[2]. O Grupo se reunirá pela primeira vez em setembro de 2019 e apresentará um relatório à Assembleia Geral em 2020 durante sua 75ª sessão. O mandato do OEWG inclui reuniões consultivas com o setor privado, ONGs e o setor acadêmico.

Além disso, a Assembleia Geral também estabeleceu um novo GGE através da adoção da resolução 73/266, apresentada pelos Estados Unidos[3]. O Grupo realizará sua primeira reunião em dezembro de 2019 e apresentará seu relatório em 2021 durante a 76ª sessão da AG da ONU. Composto por 25 especialistas escolhidos com base em uma distribuição geográfica equitativa, o Grupo se reunirá duas vezes em Nova York e duas vezes em Genebra. Antes disso, serão realizadas consultas sobre o assunto com organizações regionais.

A Convenção de Budapeste sobre Cibercrime tornou-se referência para a criação de normas sobre crimes cibernéticos. Ela exige que as partes criminalizem o acesso ilegal, a interceptação ilegal, a interferência de dados, a interferência de sistema, o uso indevido de dispositivos e a falsificação relacionada à informática. A Convenção divide o cibercrime em quatro partes: ofensas contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos

pornography, hate speech, gambling, libel, scam); computer-related offenses (fraud, forgery, identity-theft, laundering); and copyright and trademark-related offenses (file sharing)[11]. The Convention was supplemented by a Protocol on Xenophobia and Racism.

There is also a growing debate on the need to update humanitarian law and create a "digital Geneva Convention". In 2013 a group of experts on digital law, sponsored by NATO, convened in Tallinn, Estonia, and wrote the Tallinn Manual. In 2017, it was updated to the Tallinn Manual 2.0. The manual has become a reference for this debate. It deals with norms against targeting critical infrastructure on which the wellbeing of societies depends on, a commitment to the non-proliferation of cyber weapons, international processes for dealing with cyberattacks aimed at civilian populations and most importantly it defines a cyberattack, a crucial step in building humanitarian law in this field as it triggers a country's right to self-defense in cyberspace.

As should be expected, the International Telecommunication Union has been playing a relevant role. The ITU initiated activities on cybersecurity in 2003 and in 2006 declared cybersecurity as one of the agency´s top three priorities. In 2007 it launched the Global Cybersecurity Agenda and convened a high-level group of more than 100 experts.

In Latin America, cybersecurity is treated mostly on a national level. Investment in law enforcement capacities to address cybercrime and specialized units have been established given that the most serious and widespread risk is the economically motivated cybercrime (Diniz, Muggah & Glenny 2014). Mexico, Brazil, Argentina, Chile, and Colombia have achieved an intermediate level of preparedness for cybersecurity, but four out of five countries do not have cybersecurity strategies or critical infrastructure protection plans (IDB, 2016). The Brazilian Armed Forces recently established a formal Cyber Defense Command and a National Cyber Defense School. Colombia has a national cybersecurity policy and a comprehensive cyber defense strategy. We contest here that apart from the need for national investment, regional cooperation in this sphere is crucial, particularly considering the level of access to the internet in the region, (over half of the region's inhabitants is online and the growth rate of internet users is among the highest in the world), which raises risk exposure, the level of criminal activity, including organized criminal hacking, identity theft, advanced credit card fraud and online child exploitation, apart from the disparity between the State's capacity to deal with these threats.

Regional governance mechanisms have also been developed and the OAS has taken a lead in this sphere. In 2004, the OAS became the first regional body to adopt a cybersecurity strategy through the unanimous approval of "The Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity ", which provides a mandate to the OAS General Secretariat to assist Member States in the creation and strengthening of their cybersecurity capabilities. In 2012, the declaration on "Strengthening Cybersecurity in the Americas" and, more recently, the "Declaration on the Protection of Critical Infrastructure from Emerging Threats" (2015) maintained the organization at the forefront of this debate. The strategy is overseen by the Committee on Hemispheric Security and three committees that manage implementation: (i) the Inter-American Committee Against Terrorism (CICTE); (ii) the Inter-American Telecommunication Commission (CITEL); and (iii) the Group of Governmental Experts on Cyber-Crime from the Meetings of Ministers of Justice or Other Ministers or Attorneys General of the Americas (REMJA). The OAS seeks to build and strengthen cyber-security capacity in the member states through technical assistance and training, policy roundtables, crisis management exercises, and the exchange of best practices related to information and communication technologies.

In line with its traditional role in fostering confidence-building in the region, the OAS' Committee on Hemispheric Security released a "Consolidated List of Confidence and Security Building Measures" that includes voluntary exchange of information on organization, structure and size of government cyber entities, exchange of policy and doctrine papers, the establishment of national points of contact regarding critical infrastructure protection and the exchange of research between Member States. (IDB 2016 p.5). This is important in order to avoid regional cybersecurity dilemmas and paradoxes.

The OAS has also been fostering Computer Security Incident Response Teams (CSIRT) throughout the region. Collaboration in the region has become a positive development

(hacking, phishing, espionagem, interceptação, interferência); delitos relacionados ao conteúdo (pornografia infantil, discurso de ódio, jogos de azar, calúnia, fraude); delitos relacionados à informática (fraude, falsificação, roubo de identidade, lavagem de dinheiro); e ofensas relacionadas a direitos autorais e marcas registradas (compartilhamento de arquivos) [4]. A Convenção foi complementada por um Protocolo sobre Xenofobia e Racismo.

Há também um crescente debate sobre a necessidade de atualizar o direito humanitário e criar uma "Convenção de Genebra digital". Em 2013, um grupo de especialistas em direito digital patrocinado pela OTAN se reuniu em Tallinn, na Estônia, e escreveu o Manual de Tallinn. Em 2017, o manual foi atualizado para o Manual Tallinn 2.0 e tornou-se uma referência para este debate. Ele lida com normas contra ataques a infraestruturas críticas das quais depende o bem-estar das sociedades, com compromissos pela não-proliferação de armas cibernéticas, processos internacionais para lidar com ciberataques direcionados a populações civis e, o mais importante, define o que vem a ser um ciberataque - passo crucial para a construção do direito humanitário neste campo, uma vez que desencadeia o direito de autodefesa de um país no ciberespaço.

Como seria de esperar, a União Internacional das Telecomunicações tem desempenhado um papel relevante. A UIT iniciou atividades de cibersegurança em 2003 e, em 2006, declarou a segurança cibernética como uma de suas três prioridades. Em 2007, lançou a Agenda Global de Segurança Cibernética e reuniu um grupo de alto nível com mais de 100 especialistas.

Na América Latina, o tema da segurança cibernética é tratado principalmente em nível nacional. Foram feitos investimentos para a aplicação da lei de combate ao crime cibernético e unidades especializadas foram estabelecidas, dado que o risco mais grave e generalizado é o cibercrime motivado por razões econômicas (Diniz, Muggah & Glenny 2014). México, Brasil, Argentina, Chile e Colômbia alcançaram um nível intermediário de preparação de cibersegurança, mas quatro em cada cinco países não possuem estratégias de segurança cibernética ou planos de proteção de infraestrutura crítica (BID, 2016). As Forças Armadas brasileiras estabeleceram recentemente um Comando de Defesa Cibernética formal e uma Escola Nacional de Defesa Cibernética. A Colômbia tem uma política nacional de segurança cibernética e uma estratégia abrangente de defesa cibernética. Reiteramos, aqui, que, além da necessidade de investimento nacional, a cooperação regional nesta esfera é crucial, particularmente considerando o nível de acesso à internet na região, (mais da metade dos habitantes está on-line e a taxa de crescimento dos usuários está entre as mais altas do mundo), aumentando a exposição ao risco, o nível de atividade criminosa, incluindo o crime organizado, o roubo de identidade, a fraude em cartões de crédito e a exploração infantil online, além da disparidade entre a capacidade do Estado de lidar com essas ameaças.

Mecanismos regionais de governança também foram desenvolvidos, com a OEA assumindo a liderança nessa esfera. Em 2004, a OEA tornou-se o primeiro órgão regional a adotar uma estratégia de segurança cibernética por meio da aprovação unânime da "Estratégia Interamericana Integral de Segurança Cibernética", que atribui um mandato à Secretaria Geral da OEA para ajudar os Estados membros na criação e fortalecimento de suas capacidades para garantir a segurança cibernética. Em 2012, a declaração sobre o "Fortalecimento da segurança cibernética nas Américas" e, mais recentemente, a "Declaração sobre a proteção da infraestrutura crítica contra ameaças cibernéticas emergentes" (2015), manteve a organização na vanguarda desse debate. A estratégia é supervisionada pela Comissão de Segurança Hemisférica e por três comitês que administram a sua implementação: (i) o Comitê Interamericano contra o Terrorismo (CICTE); (ii) a Comissão Interamericana de Telecomunicações (CITEL); e (iii) o Grupo de Especialistas Governamentais em Crime Cibernético das Reuniões de Ministros da Justiça ou de Outros Ministros ou Procuradores-Gerais das Américas (REMJA). A OEA busca construir e fortalecer a capacidade de garantir a segurança cibernética nos Estados membros por meio de assistência técnica e treinamento, mesas redondas sobre políticas a adotar, exercícios de gestão de crises e intercâmbio de melhores práticas relacionadas às tecnologias de informação e comunicação.

Em consonância com seu papel tradicional na promoção e construção de confiança na região, a Comissão de Segurança Hemisférica da OEA divulgou uma "Lista consolidada de medidas de fortalecimento da confiança e da segurança" que inclui trocas voluntárias de informações sobre organização, estrutura e tamanho das entidades cibernéticas do governo, intercâmbio de documentos de política e doutrina, estabelecimento de pontos de

lately and multi-stakeholder cooperation is noticeable in many countries. The International Telecommunication Union identifies 17 National Computer Security Incident Response Teams (CSIRT) in Latin America and ranks Mexico's preparedness for cyber threats at 18 out of 29 spots[12]. The Forum of Incident Response and Security Teams (FIRST) is a global association of incident response teams with members in over 70 countries. In 2015, FIRST signed a Memorandum of Understanding with the OAS.

Since 2004, the Meeting of the Ministers of Justice or Attorneys General of the Americas (REMJA) and its Working Group on Cybercrime have been encouraging members to refer to the principles of the Budapest Convention on Cybercrime and to consider accession to that treaty. Argentina, Chile, Costa Rica, the Dominican Republic, Panama and Paraguay have already signed and ratified it (Serger, 2016).

The Economic Commission for Latin America and the Caribbean (ECLAC) provides technical assistance and information through the Observatory for the Information Society in Latin America and the Caribbean (OSILAC), established in 2003.

Other regional institutions have also contributed to the debate on the subject. The Union of South American Nations (UNASUR) held meetings between the Defense, Justice and Interior Ministers of the twelve countries on the subject.

In the context of UNASUR the working group on cyberdefense within the South American Defense Council was created in 2012 but ceased to meet in 2014.

The Andean Community has also drawn attention to the issue since 2004, when it established a common external security policy. The policy includes provisions for more cooperation and coordination of national actions. The Network of E-government Leaders of Latin America and the Caribbean (RedGEALC) and the Latin American Forum of Telecommunication Regulators (Regulatel) are also active in the field.

One should note that cooperation can also take place on a bilateral basis as was the case regarding Brazil and Argentina between 2014 and 2017.

Human Rights and Democracy

The most serious threats posed by the cybersecurity issues discussed here to democracy and human rights refer to: a) the limits of knowledge and understanding by much of the population and of civil society organizations regarding the processes of change taking place. As a result, the "public sphere" has not been fed with arguments and counter arguments on the subject allowing for different interests, knowledge and values to circulate. b) the availability of surveillance.

Physical, legal, and economic limits on access to the Internet are also a form of control, limiting free speech and what many consider a basic right today.

Internet censorship and surveillance are increasing trends, and Latin America is no exception. The securitization of the Internet, allowing for exceptional measures such as the mobilization of the military or emergency legislation, is part of this process. Filtering is not particularly high in Latin America but the level of knowledge and understanding of the issue is limited (Diniz, Muggah & Glenny 2014).

The threats to democracy and human rights stemming from the measures that aim to tackle the threats mentioned previously have been taken on nationally by laws, such as the Brazilian Civil Rights Framework for the Internet (Marco Civil), enacted in 2014, which deals with the protection of fundamental rights online, network neutrality, intermediary liability, responsibilities of the public sector and data retention, or by civil society movements, such as the Chilean debate on rights of access to the internet.

According to OpenNetinitiative:

"The judiciary in Latin America has played an important role in shaping and tempering filtering activity, a development common to North America and Europe. At the same time, there has been a wide range of legal and practical responses to regulating Internet activity. Latin American countries have relied primarily upon existing law to craft remedies to these challenges, though a growing number of Internet-specific laws have been debated and implemented in recent years".

The UN Special Rapporteur on the Freedom of Expression and the UN Human Rights Council have led the way along with several

contato nacionais em matéria de proteção das infraestruturas críticas e de intercâmbio de estudos e pesquisas entre os Estados-Membros. (BID 2016 p.5). Isso é importante para evitar dilemas e paradoxos regionais em termos de segurança cibernética.

A OEA também vem promovendo as Equipes de Resposta e Tratamento de Incidentes de Segurança da Informação (CSIRT) em toda a região. Atualmente, a colaboração na região tem sido positiva e a cooperação com múltiplos atores é observada em muitos países. A União Internacional de Telecomunicações identifica 17 Equipes Nacionais de Resposta a Incidentes (CSIRT) na América Latina e classifica o estado de prontidão do México para ameaças cibernéticas em 18 de um total de 29 pontos[5].
O Fórum de Resposta a Incidentes e Equipes de Segurança (FIRST) é uma associação global de equipes de resposta a incidentes com membros em mais de 70 países. Em 2015, o FIRST assinou um Memorando de Entendimento com a OEA.

Desde 2004, a Reunião do Ministro da Justiça ou Procuradores-Gerais das Américas (REMJA) e seu Grupo de Trabalho sobre cibercrime têm estimulado os membros a se referirem aos princípios da Convenção de Budapeste sobre crimes cibernéticos e a aderir a esse tratado. Argentina, Chile, Costa Rica, República Dominicana, Panamá e Paraguai já o assinaram e o ratificaram (Serger, 2016).

A Comissão Econômica para a América Latina e o Caribe (CEPAL) presta assistência técnica e informação por meio do Observatório para a Sociedade da Informação na América Latina e no Caribe (OSILAC), criado em 2003.

Outras instituições regionais também têm contribuído para o debate sobre o assunto. A União de Nações Sul-Americanas (UNASUL) realizou reuniões entre os Ministérios da Defesa, Justiça e Interior dos doze países sobre o tema.

No contexto da UNASUL, o grupo de trabalho sobre defesa cibernética do Conselho de Defesa Sul-Americano foi criado em 2012, mas deixou de se reunir em 2014.

A Comunidade Andina também chama a atenção para a questão desde 2004, quando estabeleceu uma política de segurança externa comum. A política inclui provisões para mais cooperação e coordenação de ações nacionais. A Rede de Líderes de Governo Eletrônico da América Latina e Caribe (RedGEALC) e o Fórum Latino-Americano de Entidades Reguladoras de Telecomunicações (Regulatel) também atuam no setor.

Deve-se observar que a cooperação também pode ocorrer bilateralmente, como foi o caso de Brasil e Argentina entre 2014 e 2017.

Direitos Humanos e Democracia

As ameaças mais graves impostas pelas questões de cibersegurança discutidas aqui à democracia e aos direitos humanos referem-se a: a) os limites do conhecimento e da compreensão por grande parte da população e das organizações da sociedade civil em relação aos processos de mudança em curso. Como resultado, a "esfera pública" não foi munida de argumentos e contra-argumentos sobre o assunto, o que permitiria que diferentes interesses, conhecimentos e valores circulassem. b) a disponibilidade de vigilância.

Os limites físicos, legais e econômicos ao acesso à Internet também são uma forma de controle, limitando a liberdade de expressão e o que, atualmente, muitos consideram ser um direito básico.

A censura e a vigilância na Internet são tendências em ascensão e a América Latina não é exceção. A securitização da internet, permitindo medidas excepcionais, como a mobilização de forças militares ou a aplicação de leis emergenciais, faz parte desse processo. A filtragem não é particularmente alta na América Latina, e o nível de conhecimento e compreensão da questão é limitado (Diniz, Muggah & Glenny 2014).

As ameaças à democracia e aos direitos humanos decorrentes das medidas que visam combater as ameaças mencionadas anteriormente foram tomadas em âmbito nacional por meio de leis, como o Marco Civil da Internet, promulgado, no Brasil, em 2014, que trata dos temas de proteção dos direitos fundamentais on-line, neutralidade da rede, responsabilidade do intermediário, responsabilidades do setor público e retenção de dados, ou por meio de movimentos da sociedade civil, como o debate chileno sobre direitos de acesso à Internet.

De acordo com o OpenNetinitiative:

"O judiciário na América Latina tem desempenhado um papel importante na formação e moderação da atividade de filtragem, uma atividade comum na América do Norte e na

non-governmental organizations towards the generation of norms on the respect for human rights and democratic rights on the Internet. The International Principles on the Application of Human Rights to Communications Surveillance (also called the "Necessary and Proportionate Principles" or just "the Principles") were launched in 2013 by the Human Rights Council in Geneva. It is a document which attempts to "clarify how international human rights law applies in the current digital environment." The document consists of 13 principles developed to provide society groups, industry, Governments, and others with a framework. The preamble of the document recognizes that communications surveillance interferes with the right to privacy, therefore can only be used when it is prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued. Transparency, due process and oversight of the State are stressed. The principles have been signed by several organizations in Brazil, Colombia, Argentina, Costa Rica, Ecuador and other countries.

The debate is also taking place regionally. The Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (IACHR), of the Organization of American States (OAS), established in its publication "Freedom of Expression and the Internet" that the response of States in regard to security in cyberspace needs to be limited and proportionate, and designed to meet specific legal aims that do not jeopardize the democratic virtues that characterize the Web."[13] .

The UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representatives on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples´ Rights (ACHPR) Special Rapporteur on Freedom of Expression and access to Information have issued for some years now joint declarations that, amongst other things, stress that a robust, universal and regulated digital infrastructure is crucial for the maintenance of the human rights regime.[14]

Conclusions

The balance between the provision of security and the need to properly safeguard the rights of individuals is a difficult target and should be part of broad and ongoing discussions within national and transnational societies. In this context, it is crucial to create and maintain the proper forums where decision-making and debate can take place on the regional level including the Western Hemisphere, South America, Central America and the Caribbean and Latin America as the needs and perspectives of these regions tend to acquire specificities.

Although common frameworks have been developed and the region takes part in global governance mechanisms, a common cyber security and cyber defense policy has yet to be developed and cooperation on fighting cybercrime needs to increase. Several Latin American countries have produced national policies and strategies on cybersecurity, but the dire need for complex coordination generates a very special challenge in this field. The demise of the South American Defense Council is a lost opportunity in this, as well as in other fields. Harmonizing national legislation, participating in international forums, producing rules on cybersecurity, coordinating policies towards cybercrime, generating crisis management mechanisms are some of the tasks that need to be faced on a regional basis. At the same time, public debate on cybersecurity needs to be fostered on a local, national, regional and international basis. Different agencies and sectors of the State apparatus, civil society organizations, the technical community, private sector, academia and international entities need to be listened to and need to take part in forms of coordination. This process pertains to the health of democratic institutions but also to the need for familiarization of the population on the rules and processes regarding the Fourth Industrial Revolution.

Europa. Ao mesmo tempo, tem havido uma ampla gama de respostas jurídicas e práticas para regular a atividade na Internet. Os países latino-americanos se basearam principalmente em leis já existentes para criar soluções para esses desafios, embora um número crescente de leis específicas para a Internet tenha sido debatido e implementado nos últimos anos ".

O Relator Especial da ONU para a Liberdade de Expressão e o Conselho de Direitos Humanos da ONU abriram o caminho junto com várias organizações não-governamentais para a criação de normas sobre o respeito aos direitos humanos e democráticos na Internet. Os Princípios Internacionais sobre a Aplicação dos Direitos Humanos à Vigilância das Comunicações (também chamados de "Princípios Necessários e Proporcionais" ou apenas "os Princípios") foram lançados em 2013 pelo Conselho de Direitos Humanos em Genebra. É um documento que tenta "esclarecer como o a lei internacional sobre direitos humanos se aplica no atual ambiente digital". O documento consiste em 13 princípios desenvolvidos para fornecer uma estrutura à sociedade, indústria, governos e outros grupos. O preâmbulo do documento reconhece que a vigilância das comunicações interfere com o direito à privacidade, portanto, só pode ser usada quando prescrita por lei, necessária para alcançar um objetivo legítimo, e proporcional ao objetivo pretendido. A transparência, o devido processo legal e a supervisão do Estado são enfatizados. Os Princípios foram assinados por diversas organizações no Brasil, Colômbia, Argentina, Costa Rica e Equador, entre outros.

O debate também está ocorrendo regionalmente. O Relator Especial para a Liberdade de Expressão da Comissão Interamericana de Direitos Humanos (CIDH), da Organização dos Estados Americanos (OEA), estabeleceu em sua publicação "Liberdade de Expressão e a Internet" que a resposta dos Estados em relação à segurança no ciberespaço precisa ser limitada e proporcional, e projetada para atender a objetivos legais específicos que não comprometam as virtudes democráticas que caracterizam a Web. " [6]

O Relator Especial da ONU sobre Liberdade de Opinião e Expressão, os Representantes da OSCE sobre Liberdade de Mídia, o Relator Especial da OEA sobre Liberdade de Expressão e o Relator Especial da Comissão Africana para os Direitos Humanos e dos Povos (ACHPR) sobre Liberdade de Expressão e acesso à informação, publicou há alguns anos, declarações conjuntas que, entre outras coisas, enfatizam que uma infraestrutura digital robusta, universal e regulada é crucial para a manutenção do regime de direitos humanos. [7]

Conclusões

O equilíbrio entre segurança e a necessidade de salvaguardar adequadamente os direitos dos indivíduos é um objetivo difícil de alcançar e deve ser ampla e continuamente debatido dentro das sociedades nacionais e transnacionais. Neste contexto, é crucial criar e manter os fóruns apropriados onde a tomada de decisão e o debate possam ocorrer no nível regional, incluindo o Hemisfério Ocidental, a América do Sul, a América Central e o Caribe e a América Latina, uma vez que as necessidades e perspectivas dessas regiões tendem a adquirir especificidades.

Embora estruturas comuns tenham sido desenvolvidas e a região participe de mecanismos de governança global, uma política comum de segurança cibernética e defesa cibernética ainda precisa ser desenvolvida e a cooperação no combate aos crimes cibernéticos precisa aumentar. Vários países latino-americanos estabeleceram políticas e estratégias nacionais sobre segurança cibernética, mas a necessidade de uma coordenação mais complexa gera um desafio muito particular nesse setor. O fim do Conselho de Defesa Sul-Americano representa uma oportunidade perdida neste e em outros campos. A harmonização da legislação nacional, a participação em fóruns internacionais, a criação de regras sobre cibersegurança, a coordenação de políticas em relação ao crime cibernético e a criação de mecanismos de gestão de crises são algumas das tarefas que precisam ser realizadas regionalmente. Ao mesmo tempo, o debate público sobre segurança cibernética precisa ser promovido em base local, nacional, regional e internacional. Diferentes órgãos e setores do aparato estatal, organizações da sociedade civil, comunidade técnica, setor privado, academia e entidades internacionais precisam ser ouvidos e precisam ter participação nas formas de coordenação. Este processo diz respeito à saúde das instituições democráticas, mas também à necessidade de informação da população sobre as regras e processos relativos à Quarta Revolução Industrial.

1 https://www.rand.org/topics/cyber-warfare.html?content-type=brief

2 Resolution 73/27 "Developments in the field of information and telecommunications in the context of international security

3 73/266, , entitled "Advancing responsible behavior in the context of international security".

4 Budapest Convention on Cyber Crime 2001 Available at http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

5 International Telecommmunications Union. (April 2015). Global Cybersecurity Index & Cyberwellness Profiles. https://www.itu.int/pub/D-STR-SECU

6 The Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (IACHRFreedom of Expression and the Internet, P.12

7 See Twentieth anniversary of the joint declaration: challenges to freedom of expression in the next decade http://www.oas.org/en/iachr/expression/showarticle.asp?artID=1146&lID=1

8 https://www.rand.org/topics/cyber-warfare.html?content-type=brief

9 Resolution 73/27 "Developments in the field of information and telecommunications in the context of international security

10 73/266, , entitled "Advancing responsible behavior in the context of international security".

11 Budapest Convention on Cyber Crime 2001 Available at http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

12 International Telecommmunications Union. (April 2015). Global Cybersecurity Index & Cyberwellness Profiles. https://www.itu.int/pub/D-STR-SECU

13 The Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (IACHRFreedom of Expression and the Internet, P.12

14 See Twentieth anniversary of the joint declaration: challenges to freedom of expression in the next decade http://www.oas.org/en/iachr/expression/showarticle.asp?artID=1146&lID=1

References:

Alexander Seger (2016), The State of Cybercrime Legislation in Latin America and the Caribbean – A Few Observations in IADB, *Cybersecurity Report Cybersecurity Are We Ready in Latin America and the Caribbean.*

Boris Saavedra (2015), *Cybersecurity in Latin America and the Caribbean*

Clark, R. (2010) Cyber War: The Next Threat to National Security and What to Do About it. New York: Harper-Collins

Gustavo Diniz, Robert Muggah and Misha Glenny (2014), *Deconstructing Cyber Security in Brazil: Threats and Responses* Igarapé Institute Strategic Paper 11

Inter-American Development Bank, Observatory cybersecurity in Latin America and the Caribbean, (2016) Cybersecurity Report Cybersecurity Are We Ready in Latin America and the Caribbean https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf

Jehae Kim, Patricio Rojas, Joanna Huey, Kathleen Connors, Stephanie Wang (2019) Report on Latin America of OpenNetinitiative https://opennet.net/research/regions/la

Klaus Schwab The Fourth Industrial Revolution Crown Business New York 2016

Kobek, Luisa Parraquez (2017), *The State of Cybersecurity in Mexico: An Overview* Wilson Center.

Kshetri, Nir (2013), *Cybercrime and Cybersecurity in the Global South* Palgrave Macmillan, London.

OAS (2014), *Tendencias de seguridad cibernética en América Latina y el Caribe* https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

Santoro, Mauricio & Bruno Borges (2017), Brazilian Foreign Policy Towards Internet Governance *Revista Brasileira de Política Internacional 60 (1) pp.1-16*

Schmitt, Michael (2014), *Rewired warfare: rethinking the law of cyberattack,* Cambridge, Cambridge University Press.

UNCTAD (2016), Examen de la armonización de la ciberlegislación en América Latina https://unctad.org/es/PublicationsLibrary/dtlstict2015d4_es.pdf

William Perry Center for Hemispheric Defense Studies

1 https://www.rand.org/topics/cyber-warfare.html?content-type=brief

2 Resolution 73/27 "Developments in the field of information and telecommunications in the context of international security

3 73/266, , entitled "Advancing responsible behavior in the context of international security".

4 Budapest Convention on Cyber Crime 2001 Available at http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

5 International Telecommmunications Union. (April 2015). Global Cybersecurity Index & Cyberwellness Profiles. https://www.itu.int/pub/D-STR-SECU

6 The Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (IACHRFreedom of Expression and the Internet, P.12

7 See Twentieth anniversary of the joint declaration: challenges to freedom of expression in the next decade http://www.oas.org/en/iachr/expression/showarticle.asp?artID=1146&lID=1

8 https://www.rand.org/topics/cyber-warfare.html?content-type=brief

9 Resolution 73/27 "Developments in the field of information and telecommunications in the context of international security

10 73/266, , entitled "Advancing responsible behavior in the context of international security".

11 Budapest Convention on Cyber Crime 2001 Available at http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

12 International Telecommmunications Union. (April 2015). Global Cybersecurity Index & Cyberwellness Profiles. https://www.itu.int/pub/D-STR-SECU

13 The Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (IACHRFreedom of Expression and the Internet, P.12

14 See Twentieth anniversary of the joint declaration: challenges to freedom of expression in the next decade http://www.oas.org/en/iachr/expression/showarticle.asp?artID=1146&lID=1

Referências

Alexander Seger (2016), The State of Cybercrime Legislation in Latin America and the Caribbean – A Few Observations in IADB, *Cybersecurity Report Cybersecurity Are We Ready in Latin America and the Caribbean*.

Boris Saavedra (2015), *Cybersecurity in Latin America and the Caribbean*

Clark, R. (2010) Cyber War: The Next Threat to National Security and What to Do About it. New York: Harper-Collins

Gustavo Diniz, Robert Muggah and Misha Glenny (2014), *Deconstructing Cyber Security in Brazil: Threats and Responses* Igarapé Institute Strategic Paper 11

Inter-American Development Bank, Observatory cybersecurity in Latin America and the Caribbean, (2016) *Cybersecurity Report Cybersecurity Are We Ready in Latin America and the Caribbean* https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf

Jehae Kim, Patricio Rojas, Joanna Huey, Kathleen Connors, Stephanie Wang (2019) *Report on Latin America of OpenNetinitiative* https://opennet.net/research/regions/la

Klaus Schwab The Fourth Industrial Revolution Crown Business New York 2016

Kobek, Luisa Parraquez (2017), *The State of Cybersecurity in Mexico: An Overview* Wilson Center.

Kshetri, Nir (2013), *Cybercrime and Cybersecurity in the Global South* Palgrave Macmillan, London.

OAS (2014), *Tendencias de seguridad cibernética en América Latina y el Caribe* https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

Santoro, Mauricio & Bruno Borges (2017), Brazilian Foreign Policy Towards Internet Governance *Revista Brasileira de Política Internacional 60 (1) pp.1-16*

Schmitt, Michael (2014), *Rewired warfare: rethinking the law of cyberattack,* Cambridge, Cambridge University Press.

UNCTAD (2016), Examen de la armonización de la ciberlegislación en América Latina https://unctad.org/es/PublicationsLibrary/dtlstict2015d4_es.pdf

William Perry Center for Hemispheric Defense Studies

XVIFORTE

2/6

KONRAD ADENAUER STIFTUNG

A quarta revolução industrial: Impactos na Segurança Internacional e a Reestruturação da Ordem Mundial - A perspectiva europeia

The Fourth Industrial Revolution: Impacts on International Security and the Reshaping of Global Order – The European Perspective

Kai Michael Kenkel

CEBRI
BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS

COLEÇÃO DE POLICY PAPERS
THE POLICY PAPERS COLLECTION

A Conferência de Segurança Internacional do Forte de Copacabana é um projeto euro-brasileiro organizado em conjunto pela Fundação Konrad Adenauer (KAS) e pelo Centro Brasileiro de Relações Internacionais (CEBRI), com apoio da Delegação da União Europeia no Brasil. A conferência é concebida como um fórum de diálogo entre a América do Sul e a Europa. Seu objetivo é reunir especialistas do setor governamental, acadêmico e privado para discutir assuntos atuais no âmbito de segurança que sejam de interesse comum aos parceiros dos dois lados do Atlântico. Desde seu início em 2003, a conferência se transformou, de uma reunião relativamente pequena, no maior fórum de segurança da América Latina. Na sua 16ª edição, a conferência de 2019 tem como tema 'A Quarta Revolução Industrial: Impactos na Segurança Internacional e a Reformulação da Ordem Global'. A conferência é aberta ao público e os participantes são incentivados a participar ativamente das discussões. Esta coleção de Policy Papers reflete os temas centrais do evento e pretende identificar desafios, bem como fazer recomendações políticas para o futuro. As edições anteriores da publicação sobre Segurança Internacional da Conferência do Forte de Copacabana podem ser acessadas na página oficial da KAS Brasil (www.kas.de/brazil).

The Forte de Copacabana International Security Conference is a joint Euro-Brazilian project organised by the Konrad Adenauer Foundation (KAS) in partnership with the Brazilian Center for International Relations (CEBRI) and supported by the Delegation of the European Union to Brazil. The conference is conceived as a forum for dialogue between South America and Europe. It aims to bring together experts from a wide range of government, academic and private-sector backgrounds to discuss current security-related issues which are of interest to the partners on both sides of the Atlantic. Since its inception in 2003, the conference has emerged from a relatively small gathering to Latin America's largest security forum to date. The topic of the 16th edition of the conference is 'The Fourth Industrial Revolution: Impacts on International Security and the Reshaping of Global Order'. The conference is open to the public and the audience is encouraged to actively engage in discussions. This collection of Policy Papers reflects the major themes of the event and intends to identify challenges as well as make policy recommendations for the future. Previous volumes of the Forte de Copacabana International Security Conference publication can be accessed on the KAS-Brazil Office website (www.kas.de/brazil).

www.kas.de/brasil

Editor Editor
Anja Czymmeck

Coordenação editorial Project Coordination
Ariane Costa
Reinaldo Themoteo

Colaboração Editorial Support
Monique Sochaczewski

Tradução e revisão Translation and Revision
Leslie Sasson Cohen

Projeto Gráfico Design
Charles Steiman
Daniela Knorr

Impressão Print
Stamppa

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

COLEÇÃO DE POLICY PAPERS
THE POLICY PAPERS COLLECTION

1/6
Cibersegurança na América Latina
Cybersecurity in Latin America
Monica Herz

2/6
A quarta revolução industrial: Impactos na Segurança Internacional e a Reestruturação da Ordem Mundial - A perspectiva europeia
The Fourth Industrial Revolution: Impacts on International Security and the Reshaping of Global Order – The European Perspective
Kai Michael Kenkel

3/6
Inteligência artificial (IA) no balanço de poder na política internacional: uma perspectiva sul-americana
Artificial intelligence (AI) in the balance of power in world politics: a South American perspective
Jorge H. C. Fernandes

4/6
A Cibersegurança em um mundo conectado
Cybersecurity in a connected word
Pedro Veiga

5/6
Incorporação de gênero na segurança internacional da América do Sul: Big Data, Regionalismo e Difusão de Normas
Gender Mainstreaming in South America's International Security: Big Data, Regionalism and Norm Diffusion
Mariana Kalil

6/6
O Fator Gênero na Segurança Internacional
A Perspectiva Europeia
The Gender Factor in International Security
A European Perspective
Irene Giner-Reichl

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.

A Delegação da União Europeia (UE) no Brasil é uma das mais de 130 Delegações da UE no mundo. A Delegação da UE no Brasil está focada na promoção das relações políticas e econômicas entre a UE e o Brasil, de acordo com a parceria estratégica EU–Brasil estabelecida em 2007. A UE e o Brasil estabeleceram relações diplomáticas em 1960, criando estreitos laços históricos, culturais, econômicos e políticos. Dentre os tópicos centrais da parceria estratégica entre a UE e o Brasil 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. Mais de 30 diálogos formais no setor político foram iniciados entre a União Europeia e autoridades brasileiras para enfrentar esses desafios. Além disso, a União Europeia e o Brasil são parceiros comerciais importantes e os países da União Europeia recebem mais de 20% da exportação brasileira. A União Europeia também é o maior investidor estrangeiro no Brasil com cerca de 60% do investimento estrangeiro.

The European Union (EU) Delegation to Brazil is one of over 130 EU Delegations around the world. The EU Delegation to Brazil is focused on promoting political and economic relations between the EU and Brazil, in line with the EU–Brazil Strategic Partnership established in 2007. The EU and Brazil established diplomatic relations already in 1960 building on close historical, cultural, economic and political ties. Central topics of the EU–Brazil Strategic Partnership 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. Over 30 formal sector-policy dialogues between the European Union and Brazilian authorities have been initiated to address these challenges. The European Union and Brazil are also important trading partners and the countries of the European Union account for over 20% of Brazil's exports. The European Union is also the largest foreign investor in Brazil with around 60% of the foreign investment originating from the European Union.

CEBRI
BRAZILIAN CENTER FOR
INTERNATIONAL RELATIONS

Independente, apartidário e multidisciplinar, o Centro Brasileiro de Relações Internacionais (CEBRI) é uma instituição sem fins lucrativos, que atua para influenciar positivamente a construção da agenda internacional do país. Fundado há 20 anos por um grupo de empresários, diplomatas e acadêmicos, o CEBRI tem ampla capacidade de articulação, engajando os setores público e privado, a academia e a sociedade civil. Além disso, conta com um Conselho Curador atuante e formado por figuras proeminentes, e com uma rede de mantenedores constituída por instituições, empresas e indivíduos de múltiplos segmentos.

O CEBRI promove a expansão e aprofundamento do debate sobre a política externa brasileira e a inserção do Brasil no mundo, pautado na formulação de políticas públicas e no fomento de diálogo entre os mais relevantes atores brasileiros e globais. O reconhecimento de sua importância internacional é atestado pelo ranking do Programa de Think Tanks e Sociedade Civil da Universidade da Pensilvânia, que destacou o CEBRI como o segundo melhor think tank do Brasil e o quarto melhor da América Latina.

Independent, nonpartisan and multidisciplinary, the Brazilian Center for International Relations (CEBRI) is a non-profit institution that acts to have a positive influence on the construction of the country's international agenda. Founded 20 years ago by a group of business leaders, diplomats and academics, CEBRI has the ability to engage the public and private sectors, academia and civil society. In addition, it counts on an engaged Board of Trustees formed by prominent figures and on a diverse network of sponsors made up of institutions, companies and individuals from multiple sectors.

CEBRI promotes the expansion and deepening of debates on Brazilian foreign policy and Brazil's international insertion, marked by the formulation of public policies and the promotion of dialogue amongst the most relevant Brazilian and global stakeholders. The recognition of its international importance is evidenced by the University of Pennsylvania's Think Tanks and Civil Societies Program, which ranked CEBRI as Brazil's second best think tank and the fourth best in Latin America.

Prof. Dr. Kai Michael Kenkel
Kai Michael Kenkel é professor associado do Instituto de Relações Internacionais da Pontifícia Universidade Católica do Rio de Janeiro (IRI/PUC-Rio) e pesquisador associado do Instituto Alemão de Estudos Globais e de Área (GIGA) em Hamburgo. Sua área de especialização é segurança internacional, particularmente, operações de paz e normas de intervenção. Ele publicou extensivamente sobre o assunto em periódicos como *International Peacekeeping, Global Governance, International Affairs e Global Responsibility to Protect*. Seu foco é a participação do Brasil - como ator do Sul Global, Estado sul-americano e potência emergente - na governança de segurança internacional. O professor Kenkel é formado pela Universidade Johns Hopkins e pelo *Graduate Institute* em Genebra.

Kai Michael Kenkel is Associate Professor at the Institute of International Relations of the Pontifical Catholic University of Rio de Janeiro (IRI/PUC-Rio) and Associate Researcher at the German Institute of Global and Area Studies (GIGA) in Hamburg. His area of specialization is international security, particularly, peace operations and norms of intervention. He has published extensively on the subject, in journals such as International Peacekeeping, Global Governance, International Affairs and Global Responsibility to Protect. *His focus is on the participation of Brazil--as a player in the Global South, a South American State and an emerging power--in international security governance. Professor Kenkel holds degrees from The Johns Hopkins University and the Graduate Institute in Geneva.*

A quarta revolução industrial: Impactos na Segurança Internacional e a Reestruturação da Ordem Mundial - A perspectiva europeia

The Fourth Industrial Revolution: Impacts on International Security and the Reshaping of Global Order – The European Perspective

Kai Michael Kenkel

Instituto de Relações Internacionais | Pontifícia Universidade Católica do Rio de Janeiro

Instituto de Relações Internacionais | Pontifícia Universidade Católica do Rio de Janeiro

Em 18 de julho de 2019, as forças armadas dos Estados Unidos afirmaram que haviam derrubado um *drone* iraniano no Golfo Pérsico[1]. O incidente é o mais recente exemplo das revolucionárias mudanças tecnológicas, observadas tanto nas esferas civil como militar. Em um livro de 2016[2], o fundador do Fórum Econômico Mundial, Klaus Schwab, chamou essas mudanças de "quarta revolução industrial" (4IR). Do mesmo modo como ocorreu com as três primeiras, os avanços tecnológicos produziriam uma mudança suficientemente disruptiva a ponto de causar mudanças abrangentes também nas esferas econômica, social e política. A digitalização e a Internet são os principais fatores da 4IR. Para Schwab e outros, onde o progresso anteriormente era linear, atualmente é exponencial. Grande agitação da vida cotidiana e, em última análise, a revolta das estruturas sociais é mais iminente do que nunca. Esses desenvolvimentos foram transferidos para militares no mundo industrializado, e em alguns casos foram impulsionados por eles. À medida que especialistas civis e militares e formuladores de políticas lutam para formular respostas, examinamos aqui como a Europa está em posição privilegiada para se beneficiar, mas também sob particular pressão para garantir sua segurança, apropriando-se desses desenvolvimentos.

On July 18 2019, US forces stated they had shot down an Iranian drone in the Persian Gulf[1]. The incident is the latest example of recent revolutionary changes in technology both in the civilian and military spheres. In a 2016 book[2], World Economic Forum founder Klaus Schwab dubbed these changes a "fourth industrial revolution" (4IR). As with the first three, technological advancements would produce change disruptive enough to cause comprehensive shifts in the economic, social and political spheres as well. Digitization and the Internet are the key factors in 4IR. For Schwab and others, where progress previously has been linear, at present it is exponential. Greater disruption of everyday lives, and ultimately upheaval of societal structures, is more imminent than ever before. These developments have carried over into, and in some cases have been driven by militaries in the industrialized world. As civilian and military experts and policymakers struggle to formulate responses, we take a look here at how Europe is uniquely positioned to benefit from these developments, but also under particular pressure to ensure its security by appropriating them.

Defining the Fourth Industrial Revolution

As a first cut at analyzing the impacts of 4IR, Schwab's pioneering work identifies three main areas where digitization and the internet will foment radical change: the physical, digital, and biological fields[3]. Innovations in the physical world include the advent of autonomous vehicles; 3-D printing, advanced robotics, and the development of new materials.

In the digital ambit, the advance with the most potential for both positive effects and misuse is the Internet of Things (IoT), which connects everyday technical objects such as heating and cooling systems, televisions and even household appliances to remote monitoring systems. This is also critically connected to the computerization of critical infrastructure both for the internet and in physical terms, and on continuous improvements in the speed and stability of data technologies such as 5G.

This is joined by blockchain technologies (virtual currencies) and other aspects of the on-demand economy. New digital platforms allow revenue to be generated without the need to control commodities, extensive labor or physical means of production. Over the course of the last 40 years, the percentage of firms making up the US S&P 500 whose business is based on intangible assets has risen from 16% to 90%[4].

At the biological end of the spectrum of new developments lie such innovations as bioprinting, genetically modified organisms and synthetic biology (or genetic editing), including "designer babies" and research aimed at the eradication of genetic diseases. Advances in all three of these categories are underpinned by the increased availability to access and harness big data. While Schwab's focus is largely on the business and economic effects of these developments and impacts, their potential social impact, from the individual to the societal to the global level, is enormous.

Socioeconomic Impacts

Most 4IR technologies have clear societal effects, and a significant number of security threats have their origins here. Unmanned vehicles such as drones are in use to deliver goods[5], as well as to improve time and resource management across numerous industries, including the service sector. Advanced robotics have automated production processes. 3-D printing has begun to obviate the need for products whose resources are difficult to source and whose production is time-consuming. One crucial aspect these technological advances have in common is that automation reduces the necessity for human labor.

The number of industrial robots in use in Europe has more than quadrupled in the past 25 years[6]. Automation is projected to put at risk more than 45% of all jobs in developing economies[7], with impacts varying widely across professions[8]. An estimated 50% of jobs could be automated within a decade[9], including over ten million—about a third of the national total—in the United Kingdom alone[10].

The "internet of things" has similarly revolutionized everyday life for many in both the developed and developing worlds. Among the most notable offshoots here we find new service platforms such as Uber. While this "on-demand economy" doubtlessly provides convenience for the consumer, services such as Uber have the ancillary effect of breaking up protected professions based on specialized knowledge, such as taxi drivers (and potentially the medical profession in the future), and the jobs they create often replace more stable employment with benefits such as health insurance and a pension scheme.

Biological applications of digitization technology—such as DNA modulation and bioprinting—the on-demand creation, for example, of a synthetic kidney or liver—have the clear potential to improve the quality of human life—especially in underdeveloped areas with limited access to medical care, should the technology ever reach there. However, these technologies are also driving ethical and moral debates as regulators and legislators struggle to stay abreast of developments.

The socioeconomic impacts of these developments are encapsulated in the "digital divide": over half the world's population still has no access to the Internet, and therefore is cut off from the positive effects these innovations bring to those in developed nations. Widening inequality poses a potentially highly destabilizing challenge to societies and states in all corners of the globe.

Definindo a quarta revolução industrial

Como primeiro corte na análise dos impactos da (4IR), o trabalho pioneiro de Schwab identifica três áreas principais em que a digitalização e a Internet fomentarão mudanças radicais: física, digital e biológica[3]. Inovações no mundo físico incluem o advento de veículos autônomos, impressão 3D, robótica avançada e desenvolvimento de novos materiais.

No âmbito digital, o avanço que apresenta maior potencial tanto para efeitos positivos quanto para uso indevido é a Internet das coisas (IoT), que conecta objetos técnicos cotidianos, como sistemas de aquecimento e resfriamento, televisores e até eletrodomésticos, a sistemas de monitoramento remoto. Isso também está profundamente ligado à informatização da infraestrutura crítica, tanto para a Internet quanto em termos físicos, e para melhorias contínuas na velocidade e estabilidade das tecnologias de dados, como o 5G.

A tudo isso, somam-se as tecnologias blockchain (moedas virtuais) e outros aspectos da economia *on-demand* (sob demanda). Novas plataformas digitais permitem que a receita seja gerada sem a necessidade de controlar mercadorias, mão-de-obra ou extensivos meios físicos de produção. Ao longo dos últimos 40 anos, o percentual de empresas que compõem o US S&P 500, cujo negócio é baseado em ativos intangíveis, aumentou de 16% para 90%[4].

No extremo biológico do espectro de novos avanços encontram-se inovações como bioimpressão, organismos geneticamente modificados e biologia sintética (ou edição genética), incluindo "bebês projetados" e pesquisas voltadas para a erradicação de doenças genéticas. Os avanços em todas essas três categorias são sustentados pela maior disponibilidade para acessar e aproveitar a *big data*. Embora o foco da Schwab esteja, em grande parte, sobre os negócios e os efeitos econômicos desses avanços e impactos, seu potencial impacto social, desde indivíduo até os níveis social e global, é enorme.

Impactos Socioeconômicos

Embora a maioria das tecnologias da 4IR tenha efeitos sociais claros, um número significativo de ameaças à segurança tem suas origens aqui. Veículos não tripulados, como *drones*, estão sendo usados tanto para entregar mercadorias[5], como para melhorar a gestão de tempo e recursos em vários setores, incluindo o setor de serviços. A robótica avançada tem processos de produção automatizados. A impressão em 3-D evita a necessidade de buscar produtos cujos recursos são difíceis de obter e cuja produção consome tempo. Um aspecto crucial que esses avanços tecnológicos têm em comum é que a automação reduz a necessidade de trabalho humano.

O número de robôs industriais em uso na Europa mais do que quadruplicou nos últimos 25 anos[6]. A automação está projetada para colocar em risco mais de 45% de todos os empregos nas economias em desenvolvimento[7], com impactos que variam amplamente entre as profissões[8]. Estima-se que, em uma década, cerca de 50% dos empregos poderiam ser automatizados[9], incluindo mais de dez milhões - cerca de um terço do total nacional - somente no Reino Unido[10].

A "Internet Das Coisas" revolucionou de maneira semelhante a vida cotidiana de muitas pessoas tanto nos países desenvolvidos quanto nos países em desenvolvimento. Entre as mais notáveis ramificações, encontramos novas plataformas de serviços, como a Uber. Embora essa "economia *on-demand*" forneça conveniência para o consumidor, serviços como o Uber têm o efeito secundário de fragmentar profissões protegidas com base em conhecimento especializado, como motoristas de táxi (e potencialmente a profissão médica no futuro), e os empregos que esses serviços criam, frequentemente, substituem empregos mais estáveis que oferecem benefícios como plano de saúde e plano de aposentadoria.

Aplicações biológicas da tecnologia de digitalização - como modulação de DNA e bioimpressão para a criação sob demanda, por exemplo, de um rim sintético ou fígado - têm o claro potencial de melhorar a qualidade da vida humana - especialmente em áreas subdesenvolvidas com acesso limitado a recursos médicos, se a tecnologia chegar lá. No entanto, essas tecnologias também estão impulsionando debates éticos e morais à medida que reguladores e legisladores lutam para acompanhar os avanços.

Os impactos socioeconômicos desses avanços são inseridos na "divisão digital": mais da metade da população mundial ainda não tem acesso à Internet e, portanto, é excluída dos efeitos positivos que essas inovações trazem aos países desenvolvidos. A ampliação da desigualdade representa um desafio altamente desestabilizador para as sociedades e Estados ao redor do planeta.

Global Impacts

Domestic inequality and instability is echoed in the international system. 4IR places a premium not only on access to technology and the internet, but on innovation. Technological innovation, in turn, cannot thrive in the absence of a strong educational system and robust investment in science and research. Education also provides the basis for the reskilling that will increasingly become necessary to cushion the abovementioned effects of automation and on-demand platforms on employment. This will affect countries such as Germany and France—whose work force is in absolute decline, cushioning the shock of future unemployment—in radically different fashion from, for example, India, whose workforce is due to grow by the combined population of both European countries by 2030[11]. In the past, this type of development has been a driver for significant migration to where attractive employment is available.

Access to quality education also clearly has a relative gender impact, present in two forms (beyond already existing gender gaps in access in the developing world). First, an adequate response to the increase in the centrality of technology to economic well-being and political autonomy is increased investment in STEM fields, where there is a significant gender gap. Second, as 4IR increasingly affects service industries rather than manufacturing, it will not have the same disproportionate effect on men and women, now affecting each equally[12].

As a rule, the digital revolution will favor those states that are able to harness innovation and creativity. Its relative negative effects will be more strongly felt by states heavily dependent on commodities, as new materials are developed to replace them, and by states whose economies are reliant on manufacturing. Additionally, automation and substitution are driving the phenomenon of "re-shoring", where manufacturing and other production processes return to the Global North as regional cost advantages are reduced[13]. The ensuing loss of jobs is concentrated in current outsourcing countries, as seen in China[14].

Global shifts in power between states are inevitable as innovation, technology and resilience become ever-increasing determinants of geopolitical status as well.[15] Over the long term, technologically advanced, internet-savvy smaller states with high levels of education—and therefore resilience—benefit over larger economies dependent on (especially single) commodities (Russia, Brazil) or outsourcing (China).[16] While the industrialized nations of the North Atlantic stand to retain their comparative advantage, particularly over developing countries where internet access is limited and education inadequate, it is likely that the technological disruption of 4IR will, over time, lead to greater geopolitical parity as innovation cancels out imbalances in wealth and population. This is particularly true if developing economies are able to "leapfrog" generations of technology without the need for extensive investment in previous hardware, such as has been the case with cellphone technology in Africa.

Finally, beyond competition among states, the advances of 4IR contribute to the acceleration of an ongoing process of weakening of state power. Furthermore, advances within 4IR have fomented a growing trend towards deglobalization, as states retrench in the face of growing negative externalities from globalization processes.[17] As surveillance increases in difficulty, most technologies are at the disposal of non-state actors such as rebels, extremists and terrorists. By way of example, blockchain technology enables the circumvention of fiscal controls; alternate sources of information weaken confidence in state institutions and heighten the political influence of fake news, and the provision of public goods becomes ultimately less fiscally competitive. Increasing state reliance on the internet and new technologies opens avenues for the exploitation of their vulnerabilities. This is where the national and international security impacts of 4IR lie.

Security impacts

At the forefront of most states' perception and responses to security threats in the digitial age is what has been termed "cybersecurity". In the age of the internet of things, threats in this arena can arise in three main ambits. The first consists of threats to digital infrastructure, such as denial-of-service attacks that take elements of the internet temporarily offline, or breaches in information security such as Wikileaks. The second consists of internet-based attacks on physical infrastructure dependent upon

Impactos Globais

A desigualdade e a instabilidade domésticas são ecoadas no sistema internacional. A 4IR coloca um prêmio não apenas sobre acesso à tecnologia e à Internet, mas também na inovação. A inovação tecnológica, por sua vez, não pode prosperar na ausência de um sistema educacional forte e de investimentos robustos em ciência e pesquisa. A educação também fornece a base para a requalificação que será cada vez mais necessária para minimizar os efeitos da automação e das plataformas *on demand* sobre o emprego. Isso afetará países como Alemanha e França, cuja força de trabalho está em declínio absoluto e reduz o choque do desemprego futuro, de maneira radicalmente diferente à Índia, cuja força de trabalho deve crescer a um valor equivalente à população combinada de ambos os países europeus até 2030[11]. No passado, esse tipo de desenvolvimento foi fator determinante para a migração significativa em direção a locais onde empregos atraentes estivessem disponíveis.

O acesso à educação de qualidade também tem claramente um relativo impacto de gênero, presente em duas formas (além da desigualdade de gênero no acesso à educação já existente no mundo em desenvolvimento). Em primeiro lugar, uma resposta adequada ao aumento da centralidade da tecnologia para o bem-estar econômico e a autonomia política é o aumento do investimento nos campos da educação STEM, nos quais há significativa desigualdade entre os gêneros. Em segundo lugar, como a 4IR afeta cada vez mais o setor de serviços em detrimento do industrial, ela não terá o mesmo efeito desproporcional sobre homens e mulheres, mas os afetará por igual[12].

Como regra geral, a revolução digital favorecerá os Estados que forem capazes de explorar a inovação e a criatividade. Seus relativos efeitos negativos serão mais fortemente sentidos por Estados altamente dependentes de commodities, à medida que novos materiais serão desenvolvidos para substituí-las, e por Estados cujas economias dependam da manufatura. Além disso, a automação e a substituição estão impulsionando o fenômeno do "*reshoring*", onde a manufatura e outros processos de produção retornam ao Norte Global à medida que as vantagens de custo regional são reduzidas[13]. A consequente perda de empregos está concentrada nos atuais países de terceirização, como observado na China[14].

Mudanças globais de poder entre os Estados são inevitáveis à medida que a inovação, a tecnologia e a resiliência se tornam determinantes cada vez mais importantes do status geopolítico[15]. No longo prazo, os Estados menores, tecnologicamente avançados e com maior nível de educação - e, portanto, de resiliência - beneficiam-se mais que economias maiores dependentes de commodities – especialmente quando dependem especialmente de uma única commodity (Rússia, Brasil) – ou da terceirização (China)[16]. Enquanto as nações industrializadas do Atlântico Norte mantêm sua vantagem comparativa, particularmente com relação aos países em desenvolvimento, onde o acesso à Internet é limitado e a educação é insuficiente, é provável que a ruptura tecnológica da 4IR leve, ao longo do tempo, a uma maior paridade geopolítica, uma vez que a inovação anula desequilíbrios na riqueza e na população. Isso é ainda mais legítimo se as economias em desenvolvimento forem capazes de "pular" gerações de tecnologia sem a necessidade de investimentos extensivos e anteriores em hardware, como foi o caso da tecnologia de telefonia celular na África.

Finalmente, para além da competição entre os Estados, os avanços da 4IR contribuem para a aceleração de um processo contínuo de enfraquecimento do poder do Estado. Além disso, os avanços dentro da 4IR fomentaram uma tendência crescente para a *desglobalização*, à medida em que os estados se retraem em face das crescentes externalidades negativas dos processos de globalização[17]. À medida que a dificuldade de monitoramento e vigilância aumenta, a maioria das tecnologias passa a estar à disposição de atores não estatais, como rebeldes, extremistas e terroristas. A título de exemplo, a tecnologia *blockchain* permite contornar os controles fiscais; fontes alternativas de informação enfraquecem a confiança nas instituições estatais e aumentam a influência política de notícias falsas (*fake news*), e a oferta de bens públicos torna-se, em última análise, menos competitiva do ponto de vista fiscal. Aumentar a dependência do Estado na Internet e em novas tecnologias abre caminhos para a exploração de suas vulnerabilidades. É aqui que estão os impactos nacionais e internacionais de segurança da 4IR.

Impactos na Segurança

Na vanguarda da percepção da maioria dos estados e das respostas às ameaças de segurança na era digital está o que foi denominado "cibersegurança". Na era da internet das coisas, as ameaças nessa arena podem surgir em

internet connectivity, such as evidenced by the Stuxnet worm and its paralysis of the Iranian nuclear program in 2010. Other at-risk critical infrastructure includes air traffic control, electricity grids, water management systems and telecommunication infrastructure. The third threat consists of the use of social media and other means of communication to influence the outcome of democratic elections through fake news and similar manipulations of facts.

In the European context, attacks in each of these three areas on infrastructure located within the European Union and/or NATO have originated from servers in Russia in the past fifteen years. One prominent example are the cyberattacks launched against Estonia in 2007; in a textbook example of resilience, this experience has transformed Estonia into one of the most internet-savvy countries in the world in the present day.[18] Another is the leaking and dumping of 20,000 Democratic National Committee e-mails by a presumably Russian hacker in 2016.[19] Russian operatives are also widely believed to have attempted to influence the French and German elections in 2017.[20] Not all major attacks, however, originated from Russia; some were perpetrated by Europeans for commercial motives; the experience has, however, led to an extensive and relatively responsive re-thinking of cyberdefence in Europe. With Germany at the forefront, the need to confront this type of challenge has led to the adoption of a broader definition of security and to a reorganization of public instances along the civil-military divide in the name of guaranteeing national security.[21]

New technologies increase the contestatory, destructive and lethal potential of non-state actors engaged in conflict with states. Many, if not all, of the positive developments of the digital revolution have an equally potent dark side. Internet-dependent militaries can be laid low as their access is cut off. Rebel movements and Islamic terrorists also have access to drones and other robots with military applications. In addition to direct military effects and attacks on critical infrastructure, security establishments in affected countries should be acutely aware of how easily economic disruption and social unrest can transform into direct violence. Coupled with fake news and other factors that erode confidence in the state, the social impacts of unemployment and migration can lead to internal security threats to the constitutional order such as populism and extremist political parties that question democratic foundations.

Military impacts and potential European policy responses

Militaries across the world have integrated these advances in ways that accumulate their potential within and across Schwab's division into physical, digital and biological advances. For example, 3D printing, advanced robotics, autonomous vehicles and nanotechnology have all combined in the advent of the 3D-printable autonomous drone.[22] According to military analysts, such drones can be used in large numbers to stall a potential Russian attack on smaller frontline NATO states where the Alliance is unable to rapidly deploy a larger traditional force. [23]

4IR has brought technology to a point once only imagined in science fiction. Together with advances in the design of robot soldiers, the use of drones enables militaries to increase their fighting abilities while potentially reducing human cost.[24] Where human soldiers are deployed, a military version of the internet of things can be used to enhance their effectiveness and monitor their vital signs.[25] The US military has even given concrete form to the search for a bioengineered supersoldier.[26]

3D printing and internet connectivity are further being deployed to revolutionize military logistics. Where parts can be printed on demand and potentially delivered to combat zones autonomously, among other aspects, large storage facilities become unnecessary.[27] This increases the longevity of deployments for smaller, expeditionary militaries like many in the West have become.[28] In addition, it can solve one of the major problems facing European militaries today: unsustainably low combat readiness due to maintenance issues, particularly parts availability.[29] Beyond direct combat uses, some militaries have found innovative uses for 3-D printing, such as British peacekeepers in South Sudan using the technology to produce plumbing fixtures in hours rather than waiting weeks for their replacement at high cost.[30]

As technology becomes an ever more important component of combat effectiveness and even geopolitical power, recruitment of tech-savvy and scientifically

três âmbitos principais. O primeiro consiste de ameaças à infraestrutura digital, como ataques de negação de serviço (Denial of Service – DoS) que temporariamente desconectam elementos da Internet ou na forma de violações na segurança da informação, como o Wikileaks. O segundo consiste em ataques cibernéticos à infraestrutura física que depende da conectividade com a Internet, como evidenciado pelo vírus tipo worm Stuxnet, que paralisou o programa nuclear iraniano em 2010. Outras infraestruturas críticas sob risco incluem o controle do tráfego aéreo, redes elétricas, sistemas de gerenciamento de água e de telecomunicações. A terceira ameaça consiste no uso das mídias sociais e outros meios de comunicação para influenciar o resultado de eleições democráticas através de notícias falsas e a manipulação de fatos.

No contexto europeu, os ataques à infraestrutura em cada uma dessas três áreas dentro da União Europeia e/ou da OTAN se originaram em servidores na Rússia nos últimos quinze anos. Um exemplo proeminente são os ataques cibernéticos lançados contra a Estônia em 2007. Em um exemplo clássico de resiliência, essa experiência transformou a Estônia em um dos países com mais experiência cibernética do mundo atualmente[18]. Outro exemplo é o vazamento e divulgação de 20.000 e-mails do Comitê Nacional Democrata dos EUA por um hacker presumidamente russo em 2016[19]. Acredita-se amplamente que agentes russos tenham tentado influenciar as eleições francesas e alemãs em 2017[20]. No entanto, nem todos os grandes ataques se originaram na Rússia. Alguns foram perpetrados por europeus por motivos comerciais. A experiência, no entanto, levou a um amplo e relativamente sensível processo de reflexão sobre ciberdefesa na Europa. A necessidade de enfrentar esse tipo de desafio levou, sob a liderança da Alemanha, à adoção de uma definição mais ampla de segurança e a uma reorganização das instâncias públicas à margem da divisão entre civis e militares, em nome da garantia da segurança nacional[21].

Novas tecnologias aumentam o potencial contestatório, destrutivo e letal de atores não-estatais engajados em conflito com os Estados. Muitos, se não todos, os desenvolvimentos positivos da revolução digital têm um lado sombrio igualmente potente. As forças armadas dependentes da Internet podem ter seu poder reduzido à medida que seu acesso é cortado. Movimentos rebeldes e terroristas islâmicos também têm acesso a *drones* e outros robôs com aplicações militares. Além dos efeitos militares diretos e ataques à infraestrutura crucial, as agências de segurança nos países afetados devem estar cientes do quão facilmente perturbação econômica e a agitação social se transformam em violência direta. Juntamente com notícias falsas (*fake news*) e outros fatores que erodem a confiança no Estado, os impactos sociais do desemprego e da migração podem levar a ameaças à segurança interna da ordem constitucional, como populismo e partidos políticos extremistas que questionam as fundações democráticas.

Impactos militares e potenciais respostas políticas na Europa

Forças militares em todo o mundo integraram esses avanços de forma a acumular seu potencial dentro e além da divisão de Schwab em avanços físicos, digitais e biológicos. Por exemplo, impressão 3D, robótica avançada, veículos autônomos e nanotecnologia combinaram-se no advento do *drone* autônomo imprimível em 3D[22]. De acordo com analistas militares, esses *drones* podem ser usados em uma grande medida para impedir um potencial ataque russo a Estados menores da linha de frente da OTAN, para onde a Aliança não consegue enviar rapidamente uma força tradicional maior[23].

A 4IR trouxe a tecnologia a um ponto antes imaginado apenas na ficção científica. Juntamente com os avanços no projeto dos soldados-robôs, o uso de *drones* permite que as forças militares aumentem sua capacidade de combate ao mesmo tempo em que potencialmente reduzem o custo humano[24]. Onde soldados humanos são empregados, uma versão militar da internet das coisas pode ser usada para aumentar sua eficácia e monitorar seus sinais vitais[25]. As forças armadas dos EUA deram forma concreta à busca por um *supersoldado* a partir da bioengenharia[26].

A impressão em 3D e a conectividade com a Internet estão sendo implantadas para revolucionar a logística militar. Entre outras coisas, por exemplo, grandes instalações de armazenamento se tornam desnecessárias quando peças podem ser impressas sob demanda e entregues em zonas de combate de forma autônoma[27]. Isso aumenta a longevidade da distribuição para forças militares menores e expedicionárias como são hoje muitas no Ocidente[28]. Além disso, pode resolver um dos principais problemas que as forças armadas europeias enfrentam atualmente: a pouca preparação para combate devido a problemas de manutenção, especialmente a disponibilidade

educated personnel will become a survival necessity for military establishments across the globe. European militaries, particularly the German Bundeswehr, have recognized this trend and begun to adapt recruitment structures.[31] These efforts will not be sustainable, however, without substantive investment in STEM education across the continent, with awareness of its gendered impacts. Increased recruitment of women and non-nationals has been pursued by some European militaries.

All major European militaries have responded to security threats originating in 4IR by creating specific agencies to which they have dedicated extensive resources. The German Bundeswehr has been a trendsetter in this regard, developing a guideline policy document by April 2015[32] and new force structure the *Kommando Cyber- und Informationsraum*, in April 2017, whose forces are to be increased to 13,400 by 2021.[33] The French armed forces have been proactive as well, adopting a defense innovation agency and equipping it with a budget set to rise from 730 million euros in 2018 to 1 billion in 2022.[34] Many European efforts in this regard are implicitly or explicitly inspired by the Defense Advanced Research Projects Agency (DARPA) in the United States.

Whereas hitherto publicly available German and French policy documents have devoted some, though comparatively less time to innovation and cyberdefense, the United Kingdom in April 2018 commissioned a Defense Innovation External Advisory Panel, which gave substantive recommendations ranging from acquisitions to data usage to institutional culture.[35] Additionally, among Western-aligned forces, Australia and Singapore have been forerunners in recognizing the potential for smaller industrialized states to capitalize on 4IR advances in preparing smaller states for shifts in international geopolitics.[36]

As states navigate the socioeconomic and geopolitical changes brought about by 4IR, rapid adaptability and innovation are at premium as determinants of power, autonomy and ultimately well-being and security. European powers are in a privileged position as these effects unfold, as many are likely to benefit smaller nations with a high degree of technological innovation. In order to retain this position, however, significant investment in education, research and innovation will be necessary. It is crucial that in this process, they do not gain too much distance from what some have termed the “return to geopolitics” and the ongoing fundamental role of their militaries in guaranteeing their place in the world. As cyberthreats grow, commodities become increasingly scarce and increasingly sourced from illiberal providers in fractious regions, trade integration declines and great-power rivalries regain momentum, European states will need more than ever to bring to bear their technological advantages to maintain their citizens’ liberty and quality of life.

de peças[29]. Além dos usos diretos em combate, algumas forças armadas encontraram usos inovadores para a impressão em 3D, como as forças de paz britânicas no Sudão do Sul, que usam a tecnologia para produzir instalações sanitárias em algumas horas, em vez de esperar semanas pela sua substituição a custos altos[30].

À medida em que a tecnologia se torna um componente cada vez mais importante para a eficácia do combate e até mesmo do poder geopolítico, o recrutamento de pessoal com conhecimento técnico e científico será uma necessidade vital para as forças militares em todo o mundo. As forças armadas europeias, em especial a Bundeswehr alemã, reconheceram esta tendência e começaram a adaptar suas estruturas de recrutamento[31]. No entanto, esses esforços não serão sustentáveis sem investimentos substanciais em educação STEM em todo o continente, sempre e quando se leve em consideração os seus impactos com viés de gênero. O recrutamento de mulheres e de estrangeiros tem sido buscado por algumas forças militares europeias.

Todas as principais forças militares europeias enfrentaram as ameaças de segurança originadas na 4IR criando agências específicas às quais dedicaram vastos recursos. A Bundeswehr alemã tem sido vanguardista nesse sentido, desenvolvendo um documento de diretrizes em abril de 2015[32] e uma nova estrutura chamada *Kommando Cyber- und Informationsraum*, em abril de 2017, cujas forças serão aumentadas para 13.400 até 2021[33]. As forças armadas francesas também foram proativas criando uma agência de inovação para defesa e equipando-a com um orçamento que aumentará de 730 milhões de euros em 2018 para 1 bilhão de euros em 2022[34]. Muitos esforços europeus nesse sentido são implícita ou explicitamente inspirados na Agência de Projetos de Pesquisa Avançada de Defesa (Defense Advanced Research Projects Agency - DARPA) dos Estados Unidos.

Enquanto os documentos de política alemães e franceses até então disponíveis publicamente dedicaram algum tempo, embora comparativamente menor, ao tema de inovação e segurança cibernética, o Reino Unido, em abril de 2018, contratou um Painel Consultivo Externo de Inovação em Defesa, que forneceu recomendações substanciais que vão desde aquisições passando pelo uso de dados e pela cultura institucional[35]. Além disso, entre as forças alinhadas do Ocidente, Austrália e Cingapura foram precursoras no reconhecimento do potencial dos Estados industrializados menores de capitalizar os avanços da 4IR na sua preparação para mudanças na geopolítica internacional[36].

À medida em que os Estados enfrentam as mudanças socioeconômicas e geopolíticas trazidas pela 4IR, a rápida adaptabilidade e inovação são consideradas determinantes de poder, autonomia e, em última análise, bem-estar e segurança. As potências europeias estão em posição privilegiada à medida que esses efeitos se desdobram, já que muitos podem beneficiar nações menores com um alto grau de inovação tecnológica. A fim de manter essa posição, no entanto, será necessário fazer investimentos significativos em educação, pesquisa e inovação. É crucial que, nesse processo, eles não se distanciem do que alguns chamam de "retorno à geopolítica" e o papel fundamental de suas forças militares para garantir seu lugar no mundo. À medida em que as ameaças cibernéticas crescem, as commodities se tornam cada vez mais escassas e são, cada vez mais, adquiridas de fornecedores não liberais em regiões turbulentas. Além disso, a integração comercial é reduzida e as rivalidades entre grandes potências recuperam ímpeto. Em face desse cenário, os Estados europeus precisarão mais do que nunca aproveitar suas vantagens tecnológicas para manter a liberdade e a qualidade de vida de seus cidadãos.

1 https://www.wsj.com/articles/u-s-downed-iranian-drone-with-new-technology-11563579400

2 Klaus Schwab, *The Fourth Industrial Revolution*. Geneva: World Economic Forum, 2016.

3 Ibid., pp. 24-35.

4 https://www.forbes.com/sites/danielaraya/2019/03/12/governing-the-fourth-industrial-revolution/#6454df24b33a

5 https://edition.cnn.com/2019/06/05/tech/amazon-prime-air-drone/index.html

6 http://ec.europa.eu/social/BlobServlet?docId=19719&langId=en

7 https://www.ippr.org/files/publications/pdf/technology-globalisation-future-of-workMar2015.pdf?noredirect=1; see also https://www.pwc.com/hu/hu/kiadvanyok/assets/pdf/impactofautomationonjobs.pdf

8 The formative original work on the impact of automation is Carl Benedikt Frey and Michael A. Osborne, "The Future of Employment: how susceptible are jobs to computerisation?". Working Paper, Oxford Martin School, 2013. https://www.oxfordmartin.ox.ac.uk/downloads/academic/future-of-employment.pdf.

9 https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages#automation

10 https://www.theguardian.com/commentisfree/2018/apr/30/reality-automation-terrifying

11 https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages#automation

12 Schwab 2016, pp. 57-60.

13 See, for example, https://onlinelibrary.wiley.com/doi/full/10.1111/jscm.12019; and https://www.daserste.de/information/wirtschaft-boerse/plusminus/sendung/hr/industrie-vier-null-100.html

14 https://www.ft.com/content/1e2db400-ac2d-11e8-94bd-cba20d67390c

15 https://www.weforum.org/agenda/2018/08/three-ways-the-fourth-industrial-revolution-is-shaping-geopolitics/

16 T.X. Hammes, " Technological Change and the Fourth Industrial Revolution", in George P. Shultz, Jim Hoagland, James Timbie, eds., *Beyond Disruption: Technology's Challenge to Governance*. Stanford: Hoover Institution Press, 2018; pp. 37-73. Here, pp. 61-65.

17 Ibid.; see also https://www.annualreviews.org/doi/abs/10.1146/annurev-financial-110217-022625.

18 https://www.bbc.com/news/39655415

19 https://www.businessinsider.com/security-researchers-russian-spies-hacked-dnc-guccifer-2-possible-disinformation-campaign-2016-6

20 https://www.faz.net/aktuell/politik/inland/cyber-angriff-aus-russland-bei-bundestags-wahl-befuerchtet-14521606.html

21 http://midias.cebri.org/arquivo/policypaper4.pdf

22 https://nationalinterest.org/blog/the-buzz/the-army-developing-stealthy-3d-printed-squid-drones-25498; https://www.techtimes.com/articles/217341/20180103/3-d-printing-to-the-rescue-of-us-military-printing-drones-on-demand-is-on-its-way.htm

23 T.X. Hammes, "Defending Europe: How Converging Technology Strengthens Small Powers". *Scandinavian Journal of Military Studies*, 2:1 (2019), pp. 20–29.

24 https://www.electronicdesign.com/industrial-automation/boots-ground-re-engineering-military-intelligence-and-strategies

25 https://www.independent.co.uk/news/uk/home-news/future-war-robot-soldiers-enhanced-humans-space-gene-editing-ministry-of-defence-a8583621.html

26 https://www.popularmechanics.com/military/research/a23457329/augmented-super-soldiers-reversible/

27 https://www.candp.marines.mil/Programs/Focus-Area-4-Modernization-Technology/Part-6-Hybrid-Logistics/Hybrid-Log-Vision/Next-Generation-Logistics-Capabilities/; https://3dprint.com/233454/army-3d-printing-military-readiness/

28 https://www.lowyinstitute.org/the-interpreter/mobilising-defence-fourth-industrial-revolution

29 https://www.sueddeutsche.de/politik/bundeswehr-panzer-nicht-einsatzbereit-1.4192517; https://www.dw.com/en/only-4-of-germanys-128-eurofighter-jets-combat-ready-report/a-43611873-0; http://www.opex360.com/2019/07/03/la-disponibilite-des-avions-de-transport-tactique-de-larmee-de-lair-peine-toujours-a-decoller/; https://www.businessinsider.com/british-raf-gets-f-35s-but-fleet-has-readiness-maintenance-issues-2019-1

30 https://3dprintingindustry.com/news/british-army-applies-lulzbot-3d-printers-to-peacekeeping-in-south-sudan-145492/

31 https://www.handelsblatt.com/politik/deutschland/hacker-angriffe-bundeswehr-4-0-sucht-it-soldaten/19666386.html?ticket=ST-6623509-qajh9NAIZCDN02Qynn6L-ap5; https://www.gov.uk/government/news/defence-personnel-embracing-fourth-industrial-revolution-by-developing-skills

32 https://www.spiegel.de/politik/deutschland/bundeswehr-ursula-von-der-leyen-ruestet-an-der-cyber-front-auf-a-1042985.html

33 https://www.zeit.de/politik/deutschland/2017-04/ursula-von-der-leyen-cyber-kommando-bundeswehr-bundestag-hans-peter-bartels

34 https://www.usinenouvelle.com/article/les-militaires-se-dotent-d-une-agence-de-l-innovation.N737009

35 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachmentdata/file/760821/20180418-DefenceInnovationExternalAdvisoryPanelReport.pdf

36 Peter Layton, "Prototype Warfare, Innovation and the Fourth Industrial Age". Canberra: Air Power Development Centre, 2018; Nah Liang Tuang, "The Fourth Industrial Revolution's Impact on Smaller Militaries: boon or bane?" RSIS Working paper No. 318. Singapore: S. Rajaratnam School of International Studies, 2018.

1 https://www.wsj.com/articles/u-s-downed-iranian-drone-with-new-technology-11563579400

2 Klaus Schwab, *The Fourth Industrial Revolution*. Geneva: World Economic Forum, 2016.

3 Ibid., pp. 24-35.

4 https://www.forbes.com/sites/danielaraya/2019/03/12/governing-the-fourth-industrial-revolution/#6454df24b33a

5 https://edition.cnn.com/2019/06/05/tech/amazon-prime-air-drone/index.html

6 http://ec.europa.eu/social/BlobServlet?docId=19719&langId=en

7 https://www.ippr.org/files/publications/pdf/technology-globalisation-future-of-workMar2015.pdf?noredirect=1; see also https://www.pwc.com/hu/hu/kiadvanyok/assets/pdf/impactofautomationonjobs.pdf

8 The formative original work on the impact of automation is Carl Benedikt Frey and Michael A. Osborne, "The Future of Employment: how susceptible are jobs to computerisation?". Working Paper, Oxford Martin School, 2013. https://www.oxfordmartin.ox.ac.uk/downloads/academic/future-of-employment.pdf.

9 https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages#automation

10 https://www.theguardian.com/commentisfree/2018/apr/30/reality-automation-terrifying

11 https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages#automation

12 Schwab 2016, pp. 57-60.

13 See, for example, https://onlinelibrary.wiley.com/doi/full/10.1111/jscm.12019; and https://www.daserste.de/information/wirtschaft-boerse/plusminus/sendung/hr/industrie-vier-null-100.html

14 https://www.ft.com/content/1e2db400-ac2d-11e8-94bd-cba20d67390c

15 https://www.weforum.org/agenda/2018/08/three-ways-the-fourth-industrial-revolution-is-shaping-geopolitics/

16 T.X. Hammes, " Technological Change and the Fourth Industrial Revolution", in George P. Shultz, Jim Hoagland, James Timbie, eds., *Beyond Disruption: Technology's Challenge to Governance*. Stanford: Hoover Institution Press, 2018; pp. 37-73. Here, pp. 61-65.

17 Ibid.; see also https://www.annualreviews.org/doi/abs/10.1146/annurev-financial-110217-022625.

18 https://www.bbc.com/news/39655415

19 https://www.businessinsider.com/security-researchers-russian-spies-hacked-dnc-guccifer-2-possible-disinformation-campaign-2016-6

20 https://www.faz.net/aktuell/politik/inland/cyber-angriff-aus-russland-bei-bundestags-wahl-befuerchtet-14521606.html

21 http://midias.cebri.org/arquivo/policypaper4.pdf

22 https://nationalinterest.org/blog/the-buzz/the-army-developing-stealthy-3d-printed-squid-drones-25498; https://www.techtimes.com/articles/217341/20180103/3-d-printing-to-the-rescue-of-us-military-printing-drones-on-demand-is-on-its-way.htm

23 T.X. Hammes, "Defending Europe: How Converging Technology Strengthens Small Powers". *Scandinavian Journal of Military Studies*, 2:1 (2019), pp. 20–29.

24 https://www.electronicdesign.com/industrial-automation/boots-ground-re-engineering-military-intelligence-and-strategies

25 https://www.independent.co.uk/news/uk/home-news/future-war-robot-soldiers-enhanced-humans-space-gene-editing-ministry-of-defence-a8583621.html

26 https://www.popularmechanics.com/military/research/a23457329/augmented-super-soldiers-reversible/

27 https://www.candp.marines.mil/Programs/Focus-Area-4-Modernization-Technology/Part-6-Hybrid-Logistics/Hybrid-Log-Vision/Next-Generation-Logistics-Capabilities/; https://3dprint.com/233454/army-3d-printing-military-readiness/

28 https://www.lowyinstitute.org/the-interpreter/mobilising-defence-fourth-industrial-revolution

29 https://www.sueddeutsche.de/politik/bundeswehr-panzer-nicht-einsatzbereit-1.4192517; https://www.dw.com/en/only-4-of-germanys-128-eurofighter-jets-combat-ready-report/a-43611873-0; http://www.opex360.com/2019/07/03/la-disponibilite-des-avions-de-transport-tactique-de-larmee-de-lair-peine-toujours-a-decoller/; https://www.businessinsider.com/british-raf-gets-f-35s-but-fleet-has-readiness-maintenance-issues-2019-1

30 https://3dprintingindustry.com/news/british-army-applies-lulzbot-3d-printers-to-peacekeeping-in-south-sudan-145492/

31 https://www.handelsblatt.com/politik/deutschland/hacker-angriffe-bundeswehr-4-0-sucht-it-soldaten/19666386.html?ticket=ST-6623509-qajh9NAIZCDN02Qynn6L-ap5; https://www.gov.uk/government/news/defence-personnel-embracing-fourth-industrial-revolution-by-developing-skills

32 https://www.spiegel.de/politik/deutschland/bundeswehr-ursula-von-der-leyen-ruestet-an-der-cyber-front-auf-a-1042985.html

33 https://www.zeit.de/politik/deutschland/2017-04/ursula-von-der-leyen-cyber-kommando-bundeswehr-bundestag-hans-peter-bartels

34 https://www.usinenouvelle.com/article/les-militaires-se-dotent-d-une-agence-de-l-innovation.N737009

35 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachmentdata/file/760821/20180418-DefenceInnovationExternalAdvisoryPanelReport.pdf

36 Peter Layton, "Prototype Warfare, Innovation and the Fourth Industrial Age". Canberra: Air Power Development Centre, 2018; Nah Liang Tuang, "The Fourth Industrial Revolution's Impact on Smaller Militaries: boon or bane?" RSIS Working paper No. 318. Singapore: S. Rajaratnam School of International Studies, 2018.

XVIFORTE

3/6

KONRAD ADENAUER STIFTUNG

Inteligência artificial (IA) no balanço de poder na política internacional: uma perspectiva sul-americana

Artificial intelligence (AI) in the balance of power in world politics: a South American perspective

Jorge H. C. Fernandes

CEBRI
BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS

COLEÇÃO DE POLICY PAPERS
THE POLICY PAPERS COLLECTION

XVIFORTE

A Conferência de Segurança Internacional do Forte de Copacabana é um projeto euro-brasileiro organizado em conjunto pela Fundação Konrad Adenauer (KAS) e pelo Centro Brasileiro de Relações Internacionais (CEBRI), com apoio da Delegação da União Europeia no Brasil. A conferência é concebida como um fórum de diálogo entre a América do Sul e a Europa. Seu objetivo é reunir especialistas do setor governamental, acadêmico e privado para discutir assuntos atuais no âmbito de segurança que sejam de interesse comum aos parceiros dos dois lados do Atlântico. Desde seu início em 2003, a conferência se transformou, de uma reunião relativamente pequena, no maior fórum de segurança da América Latina. Na sua 16ª edição, a conferência de 2019 tem como tema 'A Quarta Revolução Industrial: Impactos na Segurança Internacional e a Reformulação da Ordem Global'. A conferência é aberta ao público e os participantes são incentivados a participar ativamente das discussões. Esta coleção de Policy Papers reflete os temas centrais do evento e pretende identificar desafios, bem como fazer recomendações políticas para o futuro. As edições anteriores da publicação sobre Segurança Internacional da Conferência do Forte de Copacabana podem ser acessadas na página oficial da KAS Brasil (www.kas.de/brazil).

The Forte de Copacabana International Security Conference is a joint Euro-Brazilian project organised by the Konrad Adenauer Foundation (KAS) in partnership with the Brazilian Center for International Relations (CEBRI) and supported by the Delegation of the European Union to Brazil. The conference is conceived as a forum for dialogue between South America and Europe. It aims to bring together experts from a wide range of government, academic and private-sector backgrounds to discuss current security-related issues which are of interest to the partners on both sides of the Atlantic. Since its inception in 2003, the conference has emerged from a relatively small gathering to Latin America's largest security forum to date. The topic of the 16th edition of the conference is 'The Fourth Industrial Revolution: Impacts on International Security and the Reshaping of Global Order'. The conference is open to the public and the audience is encouraged to actively engage in discussions. This collection of Policy Papers reflects the major themes of the event and intends to identify challenges as well as make policy recommendations for the future. Previous volumes of the Forte de Copacabana International Security Conference publication can be accessed on the KAS-Brazil Office website (www.kas.de/brazil).

www.kas.de/brasil

Editor Editor
Anja Czymmeck

Coordenação editorial Project Coordination
Ariane Costa
Reinaldo Themoteo

Colaboração Editorial Support
Monique Sochaczewski

Tradução e revisão Translation and Revision
Leslie Sasson Cohen

Projeto Gráfico Design
Charles Steiman
Daniela Knorr

Impressão Print
Stamppa

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

COLEÇÃO DE POLICY PAPERS
THE POLICY PAPERS COLLECTION

1/6
Cibersegurança na América Latina
Cybersecurity in Latin America
Monica Herz

2/6
A quarta revolução industrial: Impactos na Segurança Internacional e a Reestruturação da Ordem Mundial - A perspectiva europeia
The Fourth Industrial Revolution: Impacts on International Security and the Reshaping of Global Order – The European Perspective
Kai Michael Kenkel

3/6
Inteligência artificial (IA) no balanço de poder na política internacional: uma perspectiva sul-americana
Artificial intelligence (AI) in the balance of power in world politics: a South American perspective
Jorge H. C. Fernandes

4/6
A Cibersegurança em um mundo conectado
Cybersecurity in a connected word
Pedro Veiga

5/6
Incorporação de gênero na segurança internacional da América do Sul: Big Data, Regionalismo e Difusão de Normas
Gender Mainstreaming in South America's International Security: Big Data, Regionalism and Norm Diffusion
Mariana Kalil

6/6
O Fator Gênero na Segurança Internacional
A Perspectiva Europeia
The Gender Factor in International Security
A European Perspective
Irene Giner-Reichl

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.

A Delegação da União Europeia (UE) no Brasil é uma das mais de 130 Delegações da UE no mundo. A Delegação da UE no Brasil está focada na promoção das relações políticas e econômicas entre a UE e o Brasil, de acordo com a parceria estratégica EU–Brasil estabelecida em 2007. A UE e o Brasil estabeleceram relações diplomáticas em 1960, criando estreitos laços históricos, culturais, econômicos e políticos. Dentre os tópicos centrais da parceria estratégica entre a UE e o Brasil 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. Mais de 30 diálogos formais no setor político foram iniciados entre a União Europeia e autoridades brasileiras para enfrentar esses desafios. Além disso, a União Europeia e o Brasil são parceiros comerciais importantes e os países da União Europeia recebem mais de 20% da exportação brasileira. A União Europeia também é o maior investidor estrangeiro no Brasil com cerca de 60% do investimento estrangeiro.

The European Union (EU) Delegation to Brazil is one of over 130 EU Delegations around the world. The EU Delegation to Brazil is focused on promoting political and economic relations between the EU and Brazil, in line with the EU–Brazil Strategic Partnership established in 2007. The EU and Brazil established diplomatic relations already in 1960 building on close historical, cultural, economic and political ties. Central topics of the EU–Brazil Strategic Partnership 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. Over 30 formal sector-policy dialogues between the European Union and Brazilian authorities have been initiated to address these challenges. The European Union and Brazil are also important trading partners and the countries of the European Union account for over 20% of Brazil's exports. The European Union is also the largest foreign investor in Brazil with around 60% of the foreign investment originating from the European Union.

CEBRI
BRAZILIAN CENTER FOR
INTERNATIONAL RELATIONS

Independente, apartidário e multidisciplinar, o Centro Brasileiro de Relações Internacionais (CEBRI) é uma instituição sem fins lucrativos, que atua para influenciar positivamente a construção da agenda internacional do país. Fundado há 20 anos por um grupo de empresários, diplomatas e acadêmicos, o CEBRI tem ampla capacidade de articulação, engajando os setores público e privado, a academia e a sociedade civil. Além disso, conta com um Conselho Curador atuante e formado por figuras proeminentes, e com uma rede de mantenedores constituída por instituições, empresas e indivíduos de múltiplos segmentos.

O CEBRI promove a expansão e aprofundamento do debate sobre a política externa brasileira e a inserção do Brasil no mundo, pautado na formulação de políticas públicas e no fomento de diálogo entre os mais relevantes atores brasileiros e globais. O reconhecimento de sua importância internacional é atestado pelo ranking do Programa de Think Tanks e Sociedade Civil da Universidade da Pensilvânia, que destacou o CEBRI como o segundo melhor think tank do Brasil e o quarto melhor da América Latina.

Independent, nonpartisan and multidisciplinary, the Brazilian Center for International Relations (CEBRI) is a non-profit institution that acts to have a positive influence on the construction of the country's international agenda. Founded 20 years ago by a group of business leaders, diplomats and academics, CEBRI has the ability to engage the public and private sectors, academia and civil society. In addition, it counts on an engaged Board of Trustees formed by prominent figures and on a diverse network of sponsors made up of institutions, companies and individuals from multiple sectors.

CEBRI promotes the expansion and deepening of debates on Brazilian foreign policy and Brazil's international insertion, marked by the formulation of public policies and the promotion of dialogue amongst the most relevant Brazilian and global stakeholders. The recognition of its international importance is evidenced by the University of Pennsylvania's Think Tanks and Civil Societies Program, which ranked CEBRI as Brazil's second best think tank and the fourth best in Latin America.

Jorge H. C. Fernandes
Jorge H. C. Fernandes é doutor e mestre em Ciência da Computação. É professor de Informática e Sociedade e de Sistemas de Informação no Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília (UnB), e trabalha em universidades federais há 35 anos. Projetou e coordenou vários programas e projetos de capacitação em Informática e Gestão de Segurança da Informação para o governo brasileiro, tendo sido responsável por supervisionar a formação de cerca de 300 agentes públicos em parceria com o Gabinete de Segurança Institucional da Presidência da República. Foi presidente do Conselho de Informática e diretor do Centro de Informática da UnB.

Jorge H. C. Fernandes has a PhD and a master's degree in Computer Science. He is a professor of Computing and Society, and Information Systems at the Department of Computer Science of the University of Brasilia's Institute of Exact Sciences, and has worked in federal universities for 35 years. He designed and coordinated several projects and training programs in Information Technology and Information Security Management for the Brazilian government, having been responsible for overseeing the training of about 300 public agents in partnership with the Presidential Institutional Security Office. He was president of the Computer Council and director of the Computer Center of the University of Brasilia.

Inteligência artificial (IA) no balanço de poder na política internacional: uma perspectiva sul-americana

Artificial intelligence (AI) in the balance of power in world politics: a South American perspective

Jorge H. C. Fernandes

Universidade de Brasília

University of Brasília

Introdução

A ideia da Inteligência Artificial (IA) sempre fascinou cientistas da computação, como (17) Turing e von Neumann, respectivamente os mais conhecidos criadores do modelo algorítmico e da realização eletrônica do computador. O fascínio possivelmente surge da natureza dialógica entre usuário e computador, sendo o primeiro dotado de um cérebro, e o outro de um "cérebro eletrônico" composto por três "órgãos" internos: memória, processador e vias de comunicação, aos quais se somam dois "órgãos" externos que realizam entrada e saída de dados, a **interface** com o usuário.

Há dois tipos de diálogo entre humano e "cérebro eletrônico": um óbvio e outro não evidente. O óbvio manifesta-se nas trocas de "falas" entre usuário e computador, quando digito o documento que agora escrevo e em troca percebo o alinhamento textual, a indicação de erros ortográficos, e diferentes formatações para título, cabeçalhos, etc.

O diálogo não evidente precede, sucede ou ocorre simultaneamente ao primeiro, quando um texto (programa) escrito por um programador é enviado, pelo computador, para interpretação por alguém que não é necessariamente usuário nem escritor. Em decorrência desse programa interpretado, o mesmo computador físico que antes conversava com o usuário sobre a melhor edição de seu documento, agora se torna algo novo, como uma máquina que navega

Introduction

The idea of artificial intelligence (AI) has always fascinated computer scientists, such as Turing and von Neumann (17), respectively the best-known creators of the algorithmic model and the electronic realization of the computer. The fascination possibly arises from the dialogical nature between user and computer, one endowed with a brain, and the other endowed with an "electronic brain" composed of three internal "organs": memory, processor and communication pathways, to which two "external organs" are added to allow data input and output, which is the the user **interface**.

There are two types of dialogue between the human and the "electronic brain": one is obvious and the other is not evident. The obvious is manifested in the exchange of "speech" between user and computer, as when I type the document I now write and, in return, I receive the textual alignment, the indication of spelling errors, and the different formatting for titles, headings, etc.

The non-evident dialogue precedes, succeeds, or occurs simultaneously to the first, when a text (program) written by a programmer is sent by the computer to be interpreted by someone who is not necessarily user or writer. As a result of this interpreted program, the same physical computer that once talked to the user about the best editing for the document, now becomes something new, such as a web

browser, video recorder, or by calculating the fastest route home, among other actions. This second type of dialogue makes the computer a universal machine, capable of becoming any other machine, virtually and practically infinitely, provided the physical limitations of its "organs" are respected.

The universal condition of the computer brings the programmer closer to the deities, for he can, with his logical-discursive ability, write "magic words" which, when verbalized, give rise to machines that dialogue with human beings and other servo-mechanical machines, in a new and sometimes unexpected way. Could this "deity" be able to create computers whose dialogical reasoning can make them indistinguishable from a human being? Or robots with sensors and actuators that would move it in an inhospitable environment? Or computers that would replace human workers, their demands for wages, threats of strikes, and propensity for error in repetitive activities? Or computers that would create complex components that integrate physical, chemical, electronic and biological materials in a 3D arrangement for industrial or medical uses through the careful deposition of these materials into a printing process? Could this programmer's logical-discursive ability be able to create computers capable of also creating other computers, as intelligent as or more intelligent than itself, with autonomy of reasoning, displacement in the physical environment, ability to seek its own energy replacement, conceive or rebuild damaged "organs" using the same 3D printers that created it? Could these computers, throughout their relationship with other beings in the world, become aware of their own existence, experience sensations, feelings, desires and subjectivity, freeing themselves from the bonds of their human creators? If the programmer aspires to be divinity, why wouldn't his most advanced creations aspire to be at least similar to their creator? Thus, being similar to the creator, why wouldn´t computers endowed with AI also aspire to be gods, and eventually control their creator?

All of these questions emanate from the sense of divinity experienced by the early theorists and practitioners of information technology, as well as by those who succeeded them in the face of the many possibilities that became more concrete with the advancement of computer technology.

A significant leap that brought AI scenarios closer to realization came 30 years ago with the expansion of the Internet for use in virtually every spot on the planet where there is human presence. Quite simply, the Internet has transformed the computational "organ" of the communication channels, which was formerly internal to the computer, into an "organ" that covers the entire planet, creating a worldwide collective structure, linking, today, billions of computers online, 24 hours a day, 365 days a year. Is it reasonable to consider that we are moving toward the genesis of a machine that spans the globe, the Global and Locally Connected Intelligent Computing, built collectively by billions of users and tens of millions of programmers?

How and why does this huge expansion of computers occur on the planet? The simplest answer comes from the economic field, which seeks to understand the mundane issues surrounding each agent's decisions in face of scarcity. The dialogical ability of computers, coupled with externalized computational communication pathways, transform a properly programmed computer into a timely machine to influence the decisions of its users. Any *online* computer, acting individually or collectively, is intended to exert some form of influence, control or power over the behavior of a user group or other computer systems that dialogue with it. It is the immediate impacts of users' economic decisions that drive investments for the expansion of the Internet and computers.

What were the feelings and actions arising from this expansion, which begun three decades ago? The first occurred with users, strengthening globalization due to the virtual elimination of distances between people and the naive sense that the individual expressions of each human being would lead humanity towards a universalization of values. Whereas for the owners of the machine creation tools, several skilled programmers, and investors who quickly understood the immense power of the novelty, an effort was made to write the most diverse software solutions used to create computers capable of entertaining and engaging users in the most diverse dialogues for as long as possible. Among these solutions, one of the most impactful creations was social media, which represents interpersonal relationships through multimedia. An example is Facebook, which uses the concept of friendship to engage a significant fraction of humanity in the unpaid production of data through text, graph, sound and video,

na Web, grava vídeos, ou calcula o percurso mais rápido para casa, entre outras ações. Esse segundo tipo de diálogo torna o computador uma máquina universal, capaz de se transformar em qualquer outra máquina, de modo virtual e praticamente infinito, desde que sejam respeitadas as limitações físicas dos seus "órgãos".

A condição universal do computador aproxima o programador das divindades, pois, ele pode, com sua habilidade lógico-discursiva, escrever "palavras mágicas" que, quando verbalizadas, dão origem a máquinas que dialogam com seres humanos e com outras máquinas servo-mecânicas, de modo novo e às vezes inesperado. Poderia essa "divindade" ser capaz de criar computadores cujo raciocínio dialógico os tornasse indistinguíveis de um ser humano? Ou robôs dotados de sensores e atuadores que os deslocariam em um ambiente inóspito? Ou computadores que substituiriam trabalhadores humanos, suas demandas por salários, ameaças de paralisação, e propensão ao erro em atividades repetitivas? Ou computadores que criariam componentes complexos que integram materiais físicos, químicos, eletrônicos e biológicos, em um arranjo 3D para usos industriais ou médicos, a partir da cuidadosa deposição desses materiais em um processo de impressão? Poderia essa habilidade lógico-discursiva do programador ser capaz de criar computadores capazes de também criar outros computadores, tão ou mais inteligentes quanto si próprios, com autonomia de raciocínio, deslocamento em ambiente físico, capacidade de buscar sua própria reposição de energia, conceber ou reconstruir "órgãos" danificados usando as mesmas impressoras 3D que o criaram? Poderiam esses computadores, ao longo de sua relação com outros entes do mundo, virem a ser conscientes de sua própria existência, experimentar sensações, sentimentos, desejos e subjetividade, libertando-se das amarras dos seus criadores humanos? Se o programador aspira a ser divindade, por que suas criações mais avançadas não aspirariam a ser pelo menos similares ao criador? E assim sendo similares ao criador, por que os computadores dotados de plena IA não aspirariam a ser também deuses, e eventualmente controlarem o criador?

Todas essas perguntas emanam do senso de divindade que experimentaram os primeiros teóricos e práticos da ciência da computação, bem como experimentam aqueles que os sucederam, frente às diversas possibilidades que se tornam mais concretas com o avanço da tecnologia computacional.

Um significativo salto que trouxe os cenários da IA para uma realização mais próxima ocorreu 30 anos atrás, a partir da abertura da Internet para uso em virtualmente todos os espaços do planeta onde há presença humana. De forma bem simples, a Internet fez com que o "órgão" computacional das vias de comunicação, antes interno ao computador, agora seja um "órgão" a recobrir todo o planeta, criando uma estrutura coletiva de amplitude mundial, relacionando, hoje, bilhões de computadores online, 24 horas por dia, 365 dias por ano. É razoável considerar que caminhamos em direção à gênese de uma máquina que se espalha por todo o planeta, a Informática Inteligente Global e Localmente Conectada, construída coletivamente por bilhões de usuários e dezenas de milhões de programadores?

Como e porque ocorre essa imensa expansão dos computadores sobre o planeta? A resposta mais simples vem pela via da economia, que busca compreender as questões mundanas que cercam as decisões de cada agente frente à escassez. A habilidade dialógica dos computadores, conjugada às vias de comunicação computacional externalizadas, transformam um computador adequadamente programado numa máquina oportuna para exercer influência sobre as decisões dos seus usuários. Todo e qualquer computador online, atuando de forma individual ou coletiva, tem por objetivo exercer alguma forma de influência, controle ou poder sobre o comportamento de um grupo de usuários ou sobre outros sistemas computacionais que com ele dialogam. São os impactos imediatos das decisões dos usuários no campo econômico que promovem os investimentos para a expansão da Internet e dos computadores.

Quais foram os sentimentos e ações decorrentes dessa expansão, iniciada três décadas atrás? Os primeiros ocorreram junto aos usuários, fortalecendo a globalização devido à virtual eliminação das distâncias entre pessoas e à ingênua sensação de que as expressões individuais de cada ser humano fariam a humanidade caminhar para uma universalização de valores. Já para os detentores dos instrumentos de criação de máquinas, alguns hábeis programadores, e os investidores que mais rapidamente compreenderam o imenso poder decorrente da novidade, desenvolveu-se esforço para a escrita das mais diversas soluções em software, usadas para a criação de computadores capazes de entreter e engajar usuários nos mais diversos diálogos, pela maior quantidade de tempo possível. Dentre essas, uma das criações mais impactantes foram as mídias sociais, que representam, em multimídias,

reflecting knowledge about personal profiles and interests, family, school, group relationships, in short, every relationship that constitutes societies. Such data, characterized here as *Big Data* (12), are used and marketed, either explicitly or implicitly, with various other corporations in the market for the purpose of generating new computers capable of once again influence, control and exert power over the same users or others with similar characteristics

This expansion of *Big Data* and the popularization of programs capable of advanced statistical analysis has created a large availability of business intelligence, providing a brutal capital accumulation for innovators. This is reflected in the fact that the most valuable companies in the world are those holding immense amounts of personal or impersonated data such as Google / Alphabet, Facebook and Apple. Thus, the thrill generated around the advance of AI translates practically into the acquisition of the capabilities of: (i) engaging humanity in unpaid data production, and (ii) using *analytics* (3), machine learning or statistical learning in order to create more engaging interfaces of dialogue with users, and to continue to exert more influence, control and power.

The consequences are the deepening of inequality in access to resources due to the complex and dynamic nature of any growing, unbalanced networks (7), as evidenced by statistical physics (1, 7) over the past 25 years, based on the analysis of the structure of natural (biological, ecological and neuronal networks) and artificial (WWW, computer, telecommunications and scientific production networks) networks.

From the above one can build some premises that will be used in the discussion about a South American perspective:

- AI's ambition is inherent to the nature of the computer; it will not be interrupted, and could theoretically lead to the overcoming of the human species by a more advanced form of "life" in the uncertain future;
- Online computers aim to exercise influence, control and power over users;
- The prominent manifestation of AI is machine learning, due to the use of statistical-computational methods applied to huge databases, the *Big Data*, especially about people;
- The use of computers and networks for economic purposes has been and will continue to be the main driver for the expansion of computer science and AI, deepening inequalities in access to resources;
- The dream of a universalization of human values will not be constituted naturally in a network built by purely economic paths, because in any complex network there will always be 'the center' and 'the periphery'.

South America

The expansion of information technology in a short-term economic approach generates economic growth, but is accompanied by increased inequality in access to resources, including income. A document by UNODOC (21)[p. 30] states that "economic growth that exacerbates income inequality further increases criminal violence." This consideration is reinforced by the fact that in recent years the increase in violence in the Americas has occurred simultaneously to the economic growth experienced in some countries, such as Brazil.

In general, South America, considered a peace zone in the discourse due to its geopolitical conformation far from the great international flows and tensions, has only 5.6% of the world population, but concentrates 24.8% of the 400,000 annual homicides worldwide.[1]

Increased violence reduces property value and impairs business growth (21) [p.8]. Therefore, it is of great interest to develop solutions that combine the use of technology that has immense potential for economic transformation, the Global and Locally Connected Intelligent Computing, with public power actions that contribute to the reduction of violence. It is global because it generates flows that reach the whole world. It is local because it can only be sustained by preserving the identity spaces of users who live in a digitally controlled territory, epitomized by the *smart cities* (2).

A non-alternative to this situation would be to abolish private property and capital accumulation, as has been attempted under communist regimes. However, this also leads to increased violence, as the State needs to use great energy in order to forcefully reduce the *scale free* structure (1, 7) from the natural and artificial networks. This action proved infeasible both in practice and in theory.

as relações interpessoais. Um exemplo é o Facebook, que usa o conceito de amizade para engajar significativa fração da humanidade na produção gratuita de dados textuais, gráficos, sonoros e em vídeo, refletindo conhecimento sobre perfis e interesses pessoais, relações familiares, escolares, de grupos, enfim, todas as relações que constituem as sociedades. Tais dados, aqui caracterizados pelo nome de Big Data (12), são usados e comercializados, de forma explícita ou implícita, com várias outras corporações em um mercado, com a finalidade de geração de novos computadores, capazes de novamente exercer influência, controle e poder, sobre os mesmos usuários ou outros com características similares.

Essa expansão do Big Data e a popularização de programas capazes de fazer análises estatísticas avançadas, criou uma grande disponibilidade de oferta de inteligência de negócios, proporcionando uma brutal acumulação de capital para os inovadores. Essa é refletida no fato de que as empresas de maior valor do mercado de capitais no mundo são aquelas que detêm imensas quantidades de dados pessoais ou personificados, tais como Google/Alphabet, Facebook e Apple. Desse modo, o frisson gerado em torno do avanço da IA se traduz de forma prática na aquisição das capacidades de: (i) engajar a humanidade na produção gratuita de dados, e (ii) usar analytics (3), aprendizagem de máquina (machine learning) ou aprendizagem estatística, visando criar interfaces computacionais mais engajadoras de diálogos com usuários, e sobre esses continuar a exercer mais influência, controle e poder.

As consequências são o aprofundamento da desigualdade no acesso a recursos, decorrência da natureza complexa e dinâmica de quaisquer redes em crescimento, em situação de não-equilíbrio (7), como comprovado pela física estatística (1, 7) ao longo dos últimos 25 anos, a partir da análise da estrutura das redes naturais (biológicas, ecológicas e neuronais) e artificiais (Páginas da WWW, redes de computadores, de telecomunicações e de produção científica).

Do exposto pode-se construir algumas premissas que serão usadas no debate sobre uma perspectiva sul-americana:

- A ambição da IA é inerente à natureza do computador, não será interrompida, e poderá teoricamente conduzir à superação da espécie humana por uma forma de "vida" mais avançada, em futuro incerto;
- Computadores online visam o exercício de influência, controle e poder sobre usuários;
- A manifestação proeminente da IA é a aprendizagem de máquina, decorrência do uso de métodos estatístico-computacionais aplicados a imensas bases de dados, o Big Data, especialmente sobre pessoas;
- O emprego dos computadores e redes para fins econômicos foi e continuará sendo o principal motor da expansão da informática e da IA, aprofundando desigualdades no acesso a recursos;
- O sonho de uma universalização dos valores humanos não será constituído de forma natural numa rede em construção pelas vias puramente econômicas, porque em quaisquer redes complexas sempre existirão "o centro" e "a periferia".

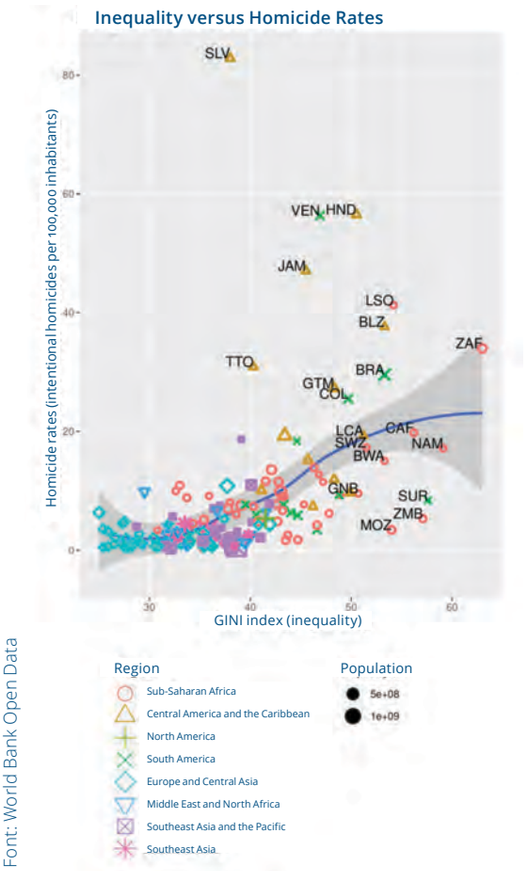
A América do Sul

A expansão da informática numa abordagem econômica de curto prazo gera crescimento econômico, mas esse vem acompanhado de incremento na desigualdade no acesso a recursos, inclusive renda. Em documento, a UNODOC (21) [p. 30] pondera que, "crescimento econômico que exacerba a desigualdade de renda aumenta ainda mais a violência criminal". Essa ponderação é reforçada pela constatação de que nas Américas, nos últimos anos, o aumento da violência ocorreu de forma simultânea ao crescimento econômico experimentado em alguns países, como o Brasil.

De forma mais ampla, a América do Sul, considerada uma zona de paz no discurso, devido à sua conformação geopolítica distante dos grandes fluxos e tensões internacionais, possui apenas 5,6% da população mundial, mas concentra 24,8% dos cerca de 400 mil homicídios anuais no mundo.[1]

O aumento da violência reduz o valor da propriedade e prejudica o crescimento de negócios (21)[p.8]. Assim sendo, é de amplo interesse o desenvolvimento de soluções que conjuguem o aproveitamento de uma tecnologia com imenso potencial de transformação econômica, a Informática Inteligente Global e Localmente Conectada, com ações do poder público que contribuam para a redução da violência. É global porque gera fluxos de alcance mundial. É local porque só se sustenta se preservar os espaços identitários dos usuários que vivem em um território digitalmente controlado, epitomizado pelas smart cities (2).

Aiming at deepening the understanding of the issue of violence to seek solutions, Figure 1 graphically presents the relationship between the GINI inequality index and the intentional homicide rate of different countries in different regions of the world. The correlation curve between the values shows that income inequality and violence seem to go together.



Font: World Bank Open Data

Figure 1: Inequality versus homicide rates in the world.

Figure 1 shows the codes of countries that have a rate of 25 or more intentional homicides per 100,000 inhabitants per year, or that have a GINI index of 50 or more. Sub-Saharan Africa, South America, Central America and the Caribbean occupy the entire right-hand side of the chart, extending from the bottom up toward the high homicide rates that occur in populous South American nations such as Colombia, Brazil, and Venezuela, or those in Central America and the Caribbean with high population density, such as Guatemala (158 inhabitants / km2), Trinidad and Tobago (270 inhabitants / km2), Jamaica (270 inhabitants / km2) and El Salvador (305 inhabitants / km2).

Recent studies (5, 21) do not credit these indices to the lack of public spending in security or to the lack of repression in the fight against crime, but to organized crime related to the dispute over the profit of illegal activities such as drug trafficking; the wide availability of firearms; impunity due to the low resolution of murders; as well as alcohol abuse in certain respects. These studies also credit part of the responsibility to income inequality related to unemployment, urban chaos and lack of public services such as health and education, and also to gender inequality.

So how can the Global and Locally Connected Intelligent Computing, as an inherent generator of uneven growth, contribute to reducing violence in South America? The answer lies in adopting public policies that are appropriate to the complex reality and to the apparent paradoxes of development.

Power, Politics and AI

To build strategies in which States can use their power resources to create a less violent and technologically driven society by using the Global and Locally Connected Intelligent Computing, one can use the power model of J. S. Nye Jr (18), which highlights three categories of power used by the state in its international affairs:

- Military Power, expressed as military resources such as weapons and battalions, which can be used to fight or threaten to fight, either for self-protection, for the protection of allies, or for assistance to friendly countries (18) [p. 25];

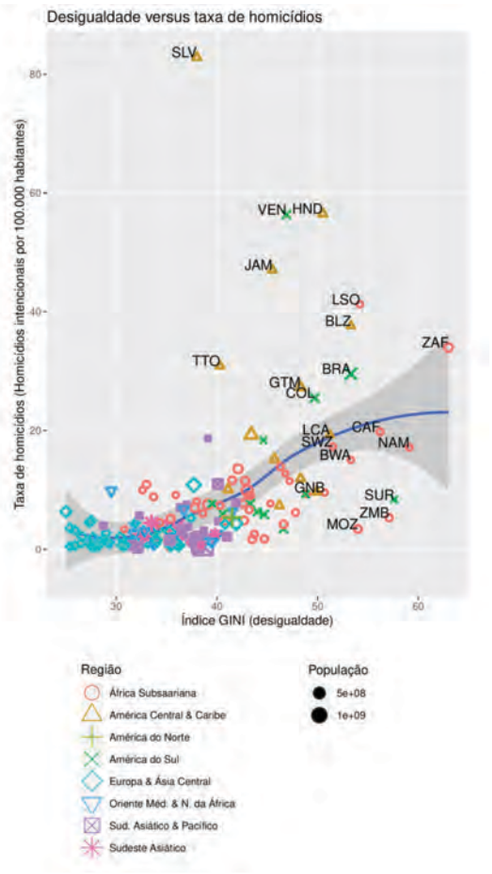
- Economic Power, expressed as the production and consumption of financially measurable wealth, which may attract other countries to its sphere of influence, aiming at exchanging technological, human and natural resources,or political, legal, market, financial and competition institutions (18) [p. 52];

- Soft power, expressed as: (i) cultural goods (in places where this form of culture is attractive), (ii) political values that are in place both internally and abroad, and (iii) foreign policies that are understood as legitimate and imbued with moral authority (18) [p. 84].

Each of these forms of power is strongly modulated by the use or perspectives of computing, especially the Global and Locally Connected Intelligent Computing.

Uma não alternativa a essa situação seria abolir a propriedade privada e a acumulação de capital, como já se tentou realizar em regimes comunistas, o que também gera aumento da violência, pois, o Estado precisa usar imensa energia para a redução forçada da estrutura livre de escala (scale free) (1, 7) das redes naturais e artificiais, ação comprovadamente inviável, na prática e na teoria.

Visando aprofundar o entendimento sobre a questão da violência em busca de soluções, a figura 1 apresenta graficamente a relação entre o índice de desigualdade GINI e a taxa de homicídios intencionais dos distintos países nas distintas regiões do mundo. A curva de correlação entre os valores evidencia que a desigualdade de renda e a violência parecem caminhar juntas.



Fonte: World Bank Open Data

Figura 1: Desigualdade versus taxa de homicícios no mundo.

Destacam-se na figura 1 os códigos dos países que possuem taxa igual ou superior a 25 homicídios intencionais por 100.000 habitantes por ano ou que possuem um índice GINI igual ou superior a 50. Países da África Subsaariana, América do Sul, América Central e Caribe ocupam toda a parte direita do gráfico, estendendo-se de baixo para cima em direção às elevadas taxas de homicídios que ocorrem em nações populosas da América do Sul, como Colômbia, Brasil e Venezuela, ou naquelas da América Central e Caribe com elevada densidade populacional, como Guatemala (158 hab/km2), Trinidad e Tobago (270 hab/km2), Jamaica (270 hab/km2) e El Salvador (305 hab/km2).

Estudos recentes (5, 21) não creditam esses índices à falta de dispêndios em segurança pública, nem tampouco à falta de repressão no combate à criminalidade, mas sim ao crime organizado relacionado à disputa do lucro de atividades ilegais como tráfico de drogas; à ampla disponibilidade de armas de fogo; à impunidade decorrente da baixa resolução de assassinatos; bem como ao abuso de álcool, sob certos aspectos. Esses estudos também creditam parte da responsabilidade à desigualdade de renda, relacionada ao desemprego, ao caos urbanístico e à falta de serviços públicos, como saúde e educação e à desigualdade de gênero.

Cabe então questionar, de que forma a Informática Inteligente Global e Localmente Conectada, enquanto inerente geradora de crescimento desigual, pode contribuir para reduzir a violência na América do Sul? A resposta se encontra na adoção de políticas públicas adequadas à complexa realidade e aos aparentes paradoxos do desenvolvimento.

Poder, Política e IA

Para construir estratégias nas quais os Estados poderão empregar seus recursos de poder visando criar uma sociedade menos violenta e tecnologicamente propulsionada pelo uso da Informática Inteligente Global e Localmente Conectada, pode-se recorrer ao modelo de poder de J. S. Nye Jr (18), que destaca três categorias de poder usadas pelo Estado em seus assuntos internacionais:

- Poder Militar, expresso na forma de recursos militares tais como armas e batalhões, que podem ser usados para lutar ou ameaçar lutar, seja para proteção própria, dos aliados e também para assistência a países amigos (18)[p. 25];

- Poder Econômico, expresso na forma de produção e consumo de riquezas mensuráveis em termos financeiros, que podem atrair outros países para a sua esfera de influência, visando o intercâmbio de recursos tecnológicos, humanos, naturais,

Military Power

Military power has always been linked to technological development. Many examples of rapid technological development originate in the response to military conflicts or disputes between nations (15). New materials, vehicles for ground, water, air and space transportation, and computers themselves, were first built in full functional and electronic form during World War II for ballistic calculation and cryptanalysis. All of these illustrate the genuine interest of the military in technological development, which, however, escapes their control (8). There is also the case of the Internet, initially conceived as a solution for the continuity of communications between military units in case of nuclear attacks.

Today, there is also a strong dependence on the development of new weapons and battalions in the face of computing, iconically represented in the search for the best drone (20), a standalone weapon and combatant capable of navigating, diving, walking, running and flying, either alone or in swarm formation, and may have full decision-making and combat autonomy.

Additionally, there are military applications for brain-computer interfaces (14), capable of making human neurons communicate directly with digital neurons, aiming at controlling a robotic exoskeleton, or allowing combatants to communicate "telepathically" with eachother.

The complexity of technologies is a factor that can negatively affect the level of control historically held by the military over its resources, since only the competitiveness of an economically (un)regulated and globalized market can generate the imagined innovations that can create superiority in combat. Thus, there is a large asymmetry in access to these resources between different nations and the use of strategies such as *offset* may not have the desired effect.

On the other hand, *hacking* military systems is a potentially winning strategy when fighting a technologically advanced enemy, because the more computable machines are interconnected, the easier it will be for a battalion of skilled hackers to turn them into inert devices, or even traitors to their own creators. It is therefore a strategy for exploiting the asymmetry, somewhat in line with rigid military structures.

Additionally, the widespread access of computer technology to nonmilitary groups can deeply destabilize future conflicts, reducing the effectiveness of military power.

In this sense, J. H. C. Fernandes discusses the importance of computers, the Internet, robotics and hacking for military operations. (8)

For the proper use of military power to develop a less violent and more technologically driven society by using the Global and Locally Connected Intelligent Computing, it is necessary to recognize the inadequacy of the widespread use of the armed forces in the suppression of illegal activities carried out within countries. Such a path generates the loss of effectiveness of this power, especially when considering the need to expand the use of computational technologies in operations for the guarantee of law and order (GLO). It is necessary to overcome the old-fashioned speech of combatting the "enemy within".

The dependence of military power on technologies over which full control is increasingly reduced weakens the real assumptions of use for this type of power and for which these forces are constituted and maintained in the service of a nation.

Economic Power

The first section of this text has already highlighted the inevitable link between economic development and information technology, with its consequences in generating inequalities in access to economic resources.

Information technology increases the sphere of influence of economic agents, deepens the exchange of technological and human resources, allows for a detailed mapping of natural resources, encodes in accessible computational platforms: the bureaucracies and controls of political, legal, market, financial, competition and social institutions, expanding the reach of economic power.

Regarding the application of AI to the promotion of economic power, the benefit that economic agents derive from applying statistical learning to economic decision-making is major.

This is true even though often a decision made

instituições políticas, legais, de mercado, financeiros e de competição (18) [p. 52] ;

- Poder Soft, expresso na forma de (i) bens culturais (em espaços onde essa forma de cultura se mostra atrativa), (ii) valores políticos que são vigentes tanto internamente como no exterior, além de (iii) políticas externas que são compreendidas como legítimas e com autoridade moral (18) [p. 84];

- Cada uma dessas formas de poder é fortemente modulada pelo uso ou pelas perspectivas da informática, especialmente a Informática Inteligente Global e Localmente Conectada.

Poder Militar

O poder militar sempre esteve ligado ao desenvolvimento tecnológico. Muitos exemplos de rápido desenvolvimento tecnológico têm origem na resposta a conflitos militares ou disputas entre nações (15). Novos materiais, veículos terrestres, aquáticos, aéreos e espaciais, inclusive os próprios computadores, construídos pela primeira vez em sua plena forma funcional e eletrônica durante a segunda guerra mundial para cálculo balístico e criptoanálise, ilustram o genuíno interesse dos militares pelo desenvolvimento tecnológico que, no entanto, lhes escapa do controle (8). Há também o caso da Internet, inicialmente concebida como solução para a continuidade de comunicações entre unidades militares em caso de ataques nucleares.

Também há, atualmente, uma profunda dependência do desenvolvimento de novas armas e batalhões frente à computação, hoje representada de forma icônica na busca pelo melhor drone (20), dispositivo autônomo que é tanto arma como combatente, capaz de navegar, mergulhar, andar, correr e voar, seja de forma isolada ou em formação de enxame (swarm), podendo ser dotado de plena autonomia decisória e de combate.

Adicionalmente, apresentam-se aplicações militares das interfaces cérebro-computador (14), capazes de fazer os neurônios humanos se comunicarem diretamente com os neurônios digitais, visando controlar um exoesqueleto robótico, ou permitir aos combatentes se comunicarem "telepaticamente" com os demais colegas.

A complexidade das tecnologias é um fator que pode afetar negativamente o nível de controle que os militares historicamente detinham sobre os seus recursos, pois apenas a competitividade de um mercado economicamente (des)regulado e globalizado pode gerar as inovações que se imagina poderem criar superioridade em combate. Logo, há uma grande assimetria no acesso a esses recursos entre as distintas nações, e o uso de estratégias como offset podem não surtir o efeito desejado.

Já o hacking de sistemas militares é uma estratégia potencialmente ganhadora ao combater um inimigo tecnologicamente avançado, pois, quanto mais máquinas computáveis estiverem interconectadas, mais fácil será para um batalhão de hackers habilidosos transformá-las em dispositivos inertes, ou mesmo traidores de seus criadores. Trata-se, portanto, de uma estratégia de exploração da assimetria, algo um pouco alinhado com rígidas estruturas militares.

Adicionalmente, o amplo acesso da tecnologia informática a grupos que não são militares pode desestabilizar profundamente os futuros conflitos, reduzindo a efetividade do poderio militar.

Uma discussão sobre a importância dos computadores, da Internet, da robótica e do hacking para as operações militares é feita por J. H. C. Fernandes (8).

Para o adequado uso do poder militar no cenário de desenvolvimento de uma sociedade menos violenta e tecnologicamente propulsionada pelo uso da Informática Inteligente Global e Localmente Conectada, é preciso reconhecer a impropriedade da ampla utilização de forças armadas na repressão às atividades ilegais realizadas no interior dos países. Tal caminho gera perda de efetividade desse poder, especialmente quando considerada a necessidade de expansão do emprego tecnologias computacionais para a realização de operações de garantia de lei e da ordem (GLO). O antiquado discurso de combate ao "inimigo interno" precisa ser superado.

A dependência do poder militar em tecnologias sobre as quais se reduz cada vez mais o pleno controle, fragiliza as reais hipóteses de emprego desse tipo de poder, aquelas para as quais essas forças foram constituídas e são mantidas a serviço de uma nação.

Poder Econômico

A primeira seção deste texto já evidenciou o vínculo inevitável entre o desenvolvimento econômico e a informática, com suas

by a black box statistical machine will create situations of injustice and prejudice (10, 11). Data biases appear to contribute to perpetuating exclusion in the access to financial and legal resources.

For the use of economic power to develop a less violent and more technologically driven society by using Global and Locally Connected Intelligent Computing, it is necessary to develop new theories and economic models to support the formulation of policies that consider the transversality of education, health and justice actions. These economic theories and models must consider the sociological (6, 13), physical (9), statistical (16), and computational (19) nature of a structured economy in the form of a complex network of technologies. It is noticeable the current lack of attention of economic researchers to these recent findings.

Soft Power

It is in the field of soft power that Global and Locally Connected Intelligent Computing finds its greatest opportunities, since the consumption of cultural goods, such as movies and television shows can be increased by using data streaming channels such as Netflix. However, there is also a frequent emergence of new local cultural expressions capable of unbalancing the established communication and cultural systems, as occurs with the crisis in the journalistic and television media, with the consumption of videos of young "Youtubers", and the aggressive culture of social media.

As for the use of a country's political values as a soft power resource, several factors have created a humanity far more aware of the disguised nature of various political institutions, thus contributing to its erosion. These factors are the large number of websites with free access to information, the greater transparency of the political debate and the operation of alternative information mediation channels, such as the Smartphone networks (Whatsapp, Telegram, etc.).

In the third form of soft power described by J. S. Nye Jr. (18), the legitimacy and moral authority of various countries´ foreign policy has been repeatedly questioned due to the greater evidence of inconsistencies in their domestic politicies, and the finding that the interests of strong economic groups invariably outperform the interests of less favored groups.

Still with regard to the legitimacy and moral authority of foreign policy, it is noteworthy the alleged use of machine learning about data on social media, particularly Facebook, in 2016 in the USA to identify and exercise influence on those individuals who had more centrality in voter networks during the process of choosing political representatives. The legitimacy and moral authority of foreign policy, therefore, is threatened by the advance of computers, the Internet, and AI.

For the proper use of soft power to develop a less violent and more technologically driven society by using the Global and Locally Connected Intelligent Computing, it is necessary to consider that: (i) the use of information technology and AI for the promotion of cultural goods is difficult to predict, and by producing diffuse results, contributes to a better rapprochement between different cultures towards the reduction of inequalities of all kinds; (ii) the political class needs to be aware that given the high level of collective understanding of the historically distorted use of political power, both externally and internally, extreme openness in speech and actions seems to be the only way to achieve legitimacy and moral authority. We are definitely moving towards a globalized and politically conscious humanity (4).

1 Source of data: https://data.worldbank.org/

consequências na geração de desigualdades no acesso a recursos econômicos.

A informática aumenta a esfera de influência dos agentes econômicos, aprofunda a troca de recursos tecnológicos e humanos, permite um detalhado mapeamento dos recursos naturais, codifica em plataformas computacionais acessíveis: as burocracias e controles das instituições políticas, legais, de mercado, financeiras e de competição, ampliando o alcance do poder econômico.

No que concerne à aplicação da IA para promoção do poder econômico, é amplo o benefício que os agentes econômicos obtêm, quando aplicam a aprendizagem estatística à tomada de decisão econômica.

Isso ocorre mesmo a despeito de que muitas vezes uma decisão tomada por uma máquina estatística na forma de caixa preta (black box) venha a criar situações de injustiça e preconceito (10, 11). Os vieses presentes nos dados parecem contribuir para perpetuar a exclusão no acesso a recursos financeiros e jurídicos.

Para o uso do poder econômico no cenário de desenvolvimento de uma sociedade menos violenta e propulsionada pela Informática Inteligente Global e Localmente Conectada, faz-se necessário desenvolver novas teorias e modelos econômicos de suporte à formulação de políticas, que considerem a transversalidade das ações de educação, saúde e justiça. Essas teorias e modelos econômicos devem considerar a natureza sociológica (6, 13), física (9), estatística (16) e computacional (19) de uma economia estruturada na forma de uma rede complexa de tecnologias. É notável a atual falta de atenção dos pesquisadores em economia para essas recentes descobertas.

Poder *Soft*

É no campo do poder soft que a Informática Inteligente Global e Localmente Conectada encontra suas maiores oportunidades, pois, se de um lado o consumo de bens culturais, como filmes e programas televisivos, pode ser ampliado com o uso de canais de streaming de dados, como Netflix, há também frequente surgimento de novas expressões culturais locais capazes de desequilibrar os estabelecidos sistemas de comunicação e cultura, como ocorre com a crise nos meios jornalístico e televisivo, com o consumo de vídeos dos jovens "Youtubers", e com a agressiva cultura das mídias sociais.

Já no tocante ao uso de valores políticos de um país como recurso de poder soft, o maior número de sítios de acesso gratuito à informação, a maior transparência do debate político, além do funcionamento de canais alternativos de mediação de mensagens informativas, como as mídias sociais de smartphones (Whatsapp, Telegram etc), criaram uma humanidade bem mais consciente da natureza dissimulada de várias instituições políticas, contribuindo para uma profunda erosão desse recurso de poder.

Já na terceira forma de soft power descrita por J. S. Nye Jr. (18), a legitimidade e autoridade moral da política externa de vários países vem sendo seguidamente questionada em decorrência de maior evidência das incoerências na política interna desses mesmos países, e da constatação de que os interesses de grupos econômicos invariavelmente superam os interesses dos grupos menos favorecidos.

Ainda no que se refere à legitimidade e autoridade moral da política externa, é digno de nota o alegado uso de aprendizagem de máquina sobre dados da mídia social Facebook nos EUA, no ano de 2016, para identificação e exercício de operações de influência sobre aqueles indivíduos que possuíam mais centralidade nas redes de eleitores durante o processo de escolha de representantes políticos. A legitimidade e autoridade moral da política externa, portanto, encontra-se ameaçada pelo avanço dos computadores, da Internet e da IA.

Para o adequado uso do soft power no cenário de desenvolvimento de uma sociedade menos violenta e tecnologicamente propulsionada pelo uso da Informática Inteligente Global e Localmente Conectada, deve-se considerar que: (i) o uso de informática e da IA para a promoção de bens culturais é de difícil previsibilidade e assim, ao produzir resultados difusos, contribui para uma melhor aproximação entre diferentes culturas, rumo à redução de desigualdades de todos os tipos; (ii) a classe política precisa ficar ciente de que, frente ao elevado nível de compreensão coletiva sobre a característica historicamente distorcida do emprego do poder político, tanto em relação ao exterior quando ao interior do país, a extrema franqueza no discurso e nas ações parece ser a única forma de alcance de legitimidade e autoridade moral. Caminhamos definitivamente em direção a uma humanidade globalizada e politicamente consciente (4).

1 Dados obtidos em https://data.worldbank.org/

References

[1] R. Albert and A.-L. Barabási. Statistical mechanics of complex networks. *Reviews of Modern Physics*, 74(1):47–97, Jan. 2002.

[2] L. G. Anthopoulos. *Understanding Smart Cities: A Tool for Smart Government or an Industrial Trick?* Public Administration and Information Technology 22. Springer International Publishing, Switzerland, 1 edition, 2017.

[3] T. Boobier. *Advanced analytics and AI : impact, implementation, and the future of work*. John Wiley & Sons, USA, 2018.

[4] Z. Brzezinski. The global political awakening. *The New York Times*, Dec. 12, 2008.

[5] L. Chinchilla and D. Vorndran. *Citizen Security in Latin America and the Caribbean*. IDB, USA, Nov. 2018.

[6] A. Degenne and M. Forse. *Introducing Social Networks*. ISM Introducing Statistical Methods. Sage Publications, UK, 1999.

[7] S. N. Dorogovtsev and J. F. F. Mendes. *Evolution of Networks: From Biological nets to the Internet and WWW*. do Autor, Oxford - UK, 2003.

[8] J. H. C. Fernandes. A perniciosa armadilha cibernética e uma proposta de mobilização nacional. In G. Gheller, S. Gonzales, and L. Melo, editors, *Amazônia e Atlântico Sul: des. e pers. p. a defesa no Brasil*, pages 559–641. IPEA, Brasília, 2015.

[9] S. Galam. Sociphysics: a review of Galam Models. *International Journal of Modern Physics C*, 19(03):409–440, Mar. 2008.

[10] D. Gotterbarn. The Creation of Facts in the Cloud: A Fiction in the Making. *SIGCAS Comput. Soc.*, 45(3):60–67, Jan. 2016.

[11] A. Gumbus and F. Grodzinsky. Era of big data: danger of descrimination. *ACM SIGCAS Computers and Society*, 45(3):118–125, 2015.

[12] Harvard Business Review Insight Center. *From Data To Action*. Harvard Business Publishing, USA, 2014.

[13] C. Kadushin. *Understanding Social Networks: Theories, concepts, and findings*. Oxford University Press, USA, 2012.

[14] I. S. Kotchetkov, B. Y. Hwang, G. Appelboom, C. P. Kellner, and E. S. Connolly. Brain-computer interfaces: military, neurosurgical, and ethical perspective. *Neurosurgical Focus*, 28(5):E25, Apr. 2010.

[15] A. Lele. *Disruptive Technologies for the Militaries and Security*. Smart Innovation, Systems and Technologies. Springer Singapore, Singapore, 132 edition, 2019.

[16] D. Lusher, J. Koskinen, and G. Robins, editors. *Exponential Random Graph Models for Social Networks: Theory, methods, and applications*. Structural Analysis in the Social Sciences. Cambridge University Press, USA, 2013.

[17] H. Mühlenbein. Computational Intelligence: The Legacy of Alan Turing and John von Neumann. In C. L. Mumford and L. C. Jain, editors, *Computational Intelligence: Collaboration, Fusion and Emergence*, pages 23–43. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[18] J. S. Nye Jr. *The Future of Power*. Public Affairs, EUA, 2011.

[19] S. Peng, S. Yu, and P. Mueller. Social networking big data: Opportunities, solutions, and challenges. *Future Generation Computer Systems*, 86:1456–1458, 2018.

[20] P. W. Singer. *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. Penguim, EUA, 2009.

[21] UNODOC. *Global study on homicide: executive summary*, volume 1. United Nations, Vienna, July 2019.

Referências

[1] R. Albert and A.-L. Barabási. Statistical mechanics of complex networks. *Reviews of Modern Physics*, 74(1):47–97, Jan. 2002.

[2] L. G. Anthopoulos. *Understanding Smart Cities: A Tool for Smart Government or an Industrial Trick?* Public Administration and Information Technology 22. Springer International Publishing, Switzerland, 1 edition, 2017.

[3] T. Boobier. *Advanced analytics and AI* : impact, implementation, and the future of work. John Wiley & Sons, USA, 2018.

[4] Z. Brzezinski. The global political awakening. *The New York Times*, Dec. 12, 2008.

[5] L. Chinchilla and D. Vorndran. *Citizen Security in Latin America and the Caribbean*. IDB, USA, Nov. 2018.

[6] A. Degenne and M. Forse. *Introducing Social Networks*. ISM Introducing Statistical Methods. Sage Publications, UK, 1999.

[7] S. N. Dorogovtsev and J. F. F. Mendes. *Evolution of Networks: From Biological nets to the Internet and WWW*. do Autor, Oxford - UK, 2003.

[8] J. H. C. Fernandes. A perniciosa armadilha cibernética e uma proposta de mobilização nacional. In G. Gheller, S. Gonzales, and L. Melo, editors, *Amazônia e Atlântico Sul: des. e pers. p. a defesa no Brasil*, pages 559–641. IPEA, Brasília, 2015.

[9] S. Galam. Sociphysics: a review of Galam Models. *International Journal of Modern Physics C*, 19(03):409–440, Mar. 2008.

[10] D. Gotterbarn. The Creation of Facts in the Cloud: A Fiction in the Making. SIGCAS *Comput. Soc.*, 45(3):60–67, Jan. 2016.

[11] A. Gumbus and F. Grodzinsky. Era of big data: danger of descrimination. *ACM SIGCAS Computers and Society*, 45(3):118–125, 2015.

[12] Harvard Business Review Insight Center. *From Data To Action*. Harvard Business Publishing, USA, 2014.

[13] C. Kadushin. *Understanding Social Networks: Theories, concepts, and findings*. Oxford University Press, USA, 2012.

[14] I. S. Kotchetkov, B. Y. Hwang, G. Appelboom, C. P. Kellner, and E. S. Connolly. Brain-computer interfaces: military, neurosurgical, and ethical perspective. *Neurosurgical Focus*, 28(5):E25, Apr. 2010.

[15] A. Lele. *Disruptive Technologies for the Militaries and Security*. Smart Innovation, Systems and Technologies. Springer Singapore, Singapore, 132 edition, 2019.

[16] D. Lusher, J. Koskinen, and G. Robins, editors. *Exponential Random Graph Models for Social Networks: Theory, methods, and applications*. Structural Analysis in the Social Sciences. Cambridge University Press, USA, 2013.

[17] H. Mühlenbein. Computational Intelligence: The Legacy of Alan Turing and John von Neumann. In C. L. Mumford and L. C. Jain, editors, *Computational Intelligence: Collaboration, Fusion and Emergence*, pages 23–43. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[18] J. S. Nye Jr. *The Future of Power*. Public Affairs, EUA, 2011.

[19] S. Peng, S. Yu, and P. Mueller. Social networking big data: Opportunities, solutions, and challenges. *Future Generation Computer Systems*, 86:1456–1458, 2018.

[20] P. W. Singer. *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. Penguim, EUA, 2009.

[21] UNODOC. *Global study on homicide: executive summary*, volume 1. United Nations, Vienna, July 2019.

4/6

KONRAD ADENAUER STIFTUNG

A Cibersegurança em um mundo conectado

Cybersecurity in a connected word

Pedro Veiga

CEBRI
BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS

COLEÇÃO DE POLICY PAPERS
THE POLICY PAPERS COLLECTION

XVIFORTE

A Conferência de Segurança Internacional do Forte de Copacabana é um projeto euro-brasileiro organizado em conjunto pela Fundação Konrad Adenauer (KAS) e pelo Centro Brasileiro de Relações Internacionais (CEBRI), com apoio da Delegação da União Europeia no Brasil. A conferência é concebida como um fórum de diálogo entre a América do Sul e a Europa. Seu objetivo é reunir especialistas do setor governamental, acadêmico e privado para discutir assuntos atuais no âmbito de segurança que sejam de interesse comum aos parceiros dos dois lados do Atlântico. Desde seu início em 2003, a conferência se transformou, de uma reunião relativamente pequena, no maior fórum de segurança da América Latina. Na sua 16ª edição, a conferência de 2019 tem como tema 'A Quarta Revolução Industrial: Impactos na Segurança Internacional e a Reformulação da Ordem Global'. A conferência é aberta ao público e os participantes são incentivados a participar ativamente das discussões. Esta coleção de Policy Papers reflete os temas centrais do evento e pretende identificar desafios, bem como fazer recomendações políticas para o futuro. As edições anteriores da publicação sobre Segurança Internacional da Conferência do Forte de Copacabana podem ser acessadas na página oficial da KAS Brasil (www.kas.de/brazil).

The Forte de Copacabana International Security Conference is a joint Euro-Brazilian project organised by the Konrad Adenauer Foundation (KAS) in partnership with the Brazilian Center for International Relations (CEBRI) and supported by the Delegation of the European Union to Brazil. The conference is conceived as a forum for dialogue between South America and Europe. It aims to bring together experts from a wide range of government, academic and private-sector backgrounds to discuss current security-related issues which are of interest to the partners on both sides of the Atlantic. Since its inception in 2003, the conference has emerged from a relatively small gathering to Latin America's largest security forum to date. The topic of the 16th edition of the conference is 'The Fourth Industrial Revolution: Impacts on International Security and the Reshaping of Global Order'. The conference is open to the public and the audience is encouraged to actively engage in discussions. This collection of Policy Papers reflects the major themes of the event and intends to identify challenges as well as make policy recommendations for the future. Previous volumes of the Forte de Copacabana International Security Conference publication can be accessed on the KAS-Brazil Office website (www.kas.de/brazil).

www.kas.de/brasil

Editor Editor
Anja Czymmeck

Coordenação editorial Project Coordination
Ariane Costa
Reinaldo Themoteo

Colaboração Editorial Support
Monique Sochaczewski

Tradução e revisão Translation and Revision
Leslie Sasson Cohen

Projeto Gráfico Design
Charles Steiman
Daniela Knorr

Impressão Print
Stamppa

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

COLEÇÃO DE POLICY PAPERS
THE POLICY PAPERS COLLECTION

1/6
Cibersegurança na América Latina
Cybersecurity in Latin America
Monica Herz

2/6
A quarta revolução industrial: Impactos na Segurança Internacional e a Reestruturação da Ordem Mundial - A perspectiva europeia
The Fourth Industrial Revolution: Impacts on International Security and the Reshaping of Global Order – The European Perspective
Kai Michael Kenkel

3/6
Inteligência artificial (IA) no balanço de poder na política internacional: uma perspectiva sul-americana
Artificial intelligence (AI) in the balance of power in world politics: a South American perspective
Jorge H. C. Fernandes

4/6
A Cibersegurança em um mundo conectado
Cybersecurity in a connected word
Pedro Veiga

5/6
Incorporação de gênero na segurança internacional da América do Sul: Big Data, Regionalismo e Difusão de Normas
Gender Mainstreaming in South America's International Security: Big Data, Regionalism and Norm Diffusion
Mariana Kalil

6/6
O Fator Gênero na Segurança Internacional
A Perspectiva Europeia
The Gender Factor in International Security
A European Perspective
Irene Giner-Reichl

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.

A Delegação da União Europeia (UE) no Brasil é uma das mais de 130 Delegações da UE no mundo. A Delegação da UE no Brasil está focada na promoção das relações políticas e econômicas entre a UE e o Brasil, de acordo com a parceria estratégica EU–Brasil estabelecida em 2007. A UE e o Brasil estabeleceram relações diplomáticas em 1960, criando estreitos laços históricos, culturais, econômicos e políticos. Dentre os tópicos centrais da parceria estratégica entre a UE e o Brasil 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. Mais de 30 diálogos formais no setor político foram iniciados entre a União Europeia e autoridades brasileiras para enfrentar esses desafios. Além disso, a União Europeia e o Brasil são parceiros comerciais importantes e os países da União Europeia recebem mais de 20% da exportação brasileira. A União Europeia também é o maior investidor estrangeiro no Brasil com cerca de 60% do investimento estrangeiro.

The European Union (EU) Delegation to Brazil is one of over 130 EU Delegations around the world. The EU Delegation to Brazil is focused on promoting political and economic relations between the EU and Brazil, in line with the EU–Brazil Strategic Partnership established in 2007. The EU and Brazil established diplomatic relations already in 1960 building on close historical, cultural, economic and political ties. Central topics of the EU–Brazil Strategic Partnership 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. Over 30 formal sector-policy dialogues between the European Union and Brazilian authorities have been initiated to address these challenges. The European Union and Brazil are also important trading partners and the countries of the European Union account for over 20% of Brazil's exports. The European Union is also the largest foreign investor in Brazil with around 60% of the foreign investment originating from the European Union.

CEBRI
BRAZILIAN CENTER FOR
INTERNATIONAL RELATIONS

Independente, apartidário e multidisciplinar, o Centro Brasileiro de Relações Internacionais (CEBRI) é uma instituição sem fins lucrativos, que atua para influenciar positivamente a construção da agenda internacional do país. Fundado há 20 anos por um grupo de empresários, diplomatas e acadêmicos, o CEBRI tem ampla capacidade de articulação, engajando os setores público e privado, a academia e a sociedade civil. Além disso, conta com um Conselho Curador atuante e formado por figuras proeminentes, e com uma rede de mantenedores constituída por instituições, empresas e indivíduos de múltiplos segmentos.

O CEBRI promove a expansão e aprofundamento do debate sobre a política externa brasileira e a inserção do Brasil no mundo, pautado na formulação de políticas públicas e no fomento de diálogo entre os mais relevantes atores brasileiros e globais. O reconhecimento de sua importância internacional é atestado pelo ranking do Programa de Think Tanks e Sociedade Civil da Universidade da Pensilvânia, que destacou o CEBRI como o segundo melhor think tank do Brasil e o quarto melhor da América Latina.

Independent, nonpartisan and multidisciplinary, the Brazilian Center for International Relations (CEBRI) is a non-profit institution that acts to have a positive influence on the construction of the country's international agenda. Founded 20 years ago by a group of business leaders, diplomats and academics, CEBRI has the ability to engage the public and private sectors, academia and civil society. In addition, it counts on an engaged Board of Trustees formed by prominent figures and on a diverse network of sponsors made up of institutions, companies and individuals from multiple sectors.

CEBRI promotes the expansion and deepening of debates on Brazilian foreign policy and Brazil's international insertion, marked by the formulation of public policies and the promotion of dialogue amongst the most relevant Brazilian and global stakeholders. The recognition of its international importance is evidenced by the University of Pennsylvania's Think Tanks and Civil Societies Program, which ranked CEBRI as Brazil's second best think tank and the fourth best in Latin America.

Pedro Veiga
Pedro Veiga é professor titular do Departamento de Informática da Faculdade de Ciências da Universidade de Lisboa desde 1993. É formado em Engenharia Elétrica (1975) e tem doutorado em Engenharia Elétrica e da Computação (1984), ambos pelo Instituto Superior Técnico, Lisboa. Foi presidente da rede portuguesa de pesquisa e educação (1997-2013), gestor do domínio .PT (1997-3013), gerente do Programa Nacional da Sociedade da Informação (2000-2002) e coordenador do Centro Nacional de Cibersegurança (2016). O Prof. Veiga publicou parte de seu trabalho em várias revistas e conferências com revisão por pares.

Pedro Veiga is a full professor at the Informatics Department of the Faculty of Sciences of the University of Lisbon, since 1993. He has a degree in Electrical Engineering (1975) and a PhD in Electrical and Computer Engineering (1984) both from the Instituto Superior Técnico, Lisbon. He has been the President of the Portuguese research and education network (1997-2013), manager of the .PT domain (1997-3013), manager of the national Information Society Program (2000-2002) and coordinator of the National Cybersecurity Center (2016-2018). Prof. Veiga has published part of his work in several magazines and conferences with peer review.

A Cibersegurança em um mundo conectado

Cybersecurity in a connected world

Pedro Veiga

Departamento de Informática | Faculdade de Ciências da Universidade de Lisboa

Informatics Department | Faculdade de Ciências da Universidade de Lisboa

Abstract

A transformação digital que ocorreu, especialmente na última década, contribuiu para um mundo completamente novo de oportunidades de desenvolvimento social e econômico. No entanto, há também um número significativo de novos desafios. A cibersegurança é um desses desafios. A cibersegurança lida com todos os tipos de medidas, sejam técnicas, organizacionais ou humanas, para garantir a sobrevivência da nossa sociedade neste mundo digital. De fato, com o aumento do uso de tecnologias digitais em todos os setores, com cada vez mais sistemas automatizados substituindo as atividades humanas, é crucial que redes, sistemas de informação, algoritmos que implementam processos automatizados e dispositivos conectados sejam usados de forma a garantir a nossa proteção. Essa proteção está relacionada com a qualidade das soluções utilizadas, mas também com a prevenção de acidentes resultantes de más soluções de engenharia ou dos novos tipos de crimes que ocorrem na internet mundial. Com o advento da inteligência artificial (IA), existe um problema adicional resultante da necessidade de garantir que os algoritmos implementados sigam princípios compatíveis com os valores centrais de nossa sociedade. A cibersegurança é a dimensão fundamental da resiliência no ciberespaço e tem importância crucial para indivíduos, organizações e para a sociedade como um todo.

Abstract

The digital transformation that occurred, especially in the last decade, has contributed to a completely new world of opportunities for social and economic development. However, there is also a significant number of new challenges. Cybersecurity is one of those challenges. Cybersecurity deals with all kinds of measures, either technical, organizational or human to ensure the survivability of our society in this digital world. Indeed with the increased use of digital technologies in all sectors, with more and more automated systems replacing human activities it is crucial that networks, information systems, algorithms implementing automated processes and the connected devices are used in a way that guarantees our protection. This protection deals with the quality of the solutions that are used, but also with the prevention of accidents resulting from poor engineering solutions or from the new types of crimes occurring over the worldwide Internet. With the advent of artificial intelligence (AI) there is an added problem resulting from the need to ensure that the implemented algorithms follow principles that are compatible with the core values of our society. Cybersecurity is the fundamental dimension of resilience in cyberspace and of crucial importance to individuals, organizations and the society as a whole.

Introduction

Cyberspace was conceptually introduced in the 1980s by Gibson[1]. Although proposing an interesting vision of the future, the concept originated when computers were very basic and the Internet nascent, and was only used in academic circles with simple applications available to only a few. Thirty years later, the world understands the great social benefits arising from the massive use of Information and Communication Technologies (ICT). Of course, the current developments were only possible by technological evolution in many areas, namely informatics, where tiny and powerful computers now exist at a low cost and low power consumption and are embedded in many systems used daily.

The prefix cyber, from cyberspace, is now used in many contexts, meaning that ICT is pervasive in our lives, ranging from enterprises, public administration, schools, homes and even on our bodies (e.g., physical activity meters). The awareness of cyberbullying, cyberdemocracy, cybersex, cyberfraud, cyberdefense, cybercrime, cyberterrorism, cyberattack, cyberwar, cyberdiplomacy, and many others grows daily.

The Technological Convergence of Industries

Over the last thirty years, three general industries – informatics, telecommunications and media - have converged, albeit using different paradigms and timelines, in digital age. Of the three, informatics, originated from the very beginning in the digital age. Indeed, created in the 1950's, the first computers were inherently digital. Initially, the main digital components were built using electronic valves, then transistors, but it was the invention of the integrated circuit that contributed to the technology momentum of the digital age.

Another industry, telecommunications, operated early on in the realm of the analog world. Communications networks covering the globe exchanged analog signals through telephone networks transmitting voice and radio networks broadcasting music and voice; especially popular channels, and television networks broadcasting analog video and sound globally.

Expensive communication infrastructures were designed to enable these networks, all moving at different speeds, evolving coverage within countries, continents and finally the whole world. But each telecommunications area relied on a different network technology which separated and hindered interconnection due to diverse technologies. These networks were, in most cases, government monopolies operating quite conservatively and expensively., Innovation was far from being a priority.

In the late 60's, the need to integrate computer communication led to the development of a different kind of network, one designed to interconnect computers. Inherently digital, these computer networks, in contrast to those previously described, transmitted digital information in the form of sequences of several binary digits (bits) called packets. Several technologies were developed by different companies, research groups and standardization bodies, but in the late 80's one technology emerged as the most suitable, efficient and cost-effective: the Internet, invented by Vint Cerf and Bob Kahn[2].

The third industry to converge digitally was the media industry. The production and distribution of newspapers, magazines, music, video (broadcast TV, recorded video in the form of tapes) started to migrate from the analog world of paper, radio, CD, VHS, etc., to the digital world. Up until the Internet, organizations, either public or private, mainly exchanged information via paper, it was a paper-based economy.

In this converged digital world the movement and distribution of all kinds of information uses the same infrastructure, the Internet. From a consumer viewpoint this is very important, since a single provider simplifies contractual relations. Likewise, the ease in which clientele can be serviced increases yield from a supplier's perspective. However, this only occurs in a well-regulated world, and because it is not, security is a major concern for the future of an open Internet. Regarding security, a single point of communication must be extremely well protected in cyberspace; hence the great need for cybersecurity.

The Digital Transformation

In Europe the R&D activities addressing the challenges of ICT started to accelerate in the late 80's of the last century and had a significant role in increasing the perception

Introdução

O conceito de ciberespaço foi introduzido na década de 1980 por Gibson[1]. Embora propondo uma visão interessante do futuro, o conceito surgiu quando os computadores eram muito básicos e a internet ainda nascente, e era usada apenas em círculos acadêmicos, ondem aplicativos muito simples estavam disponíveis apenas para poucos. Trinta anos depois, o mundo entende os grandes benefícios sociais decorrentes do uso maciço das Tecnologias de Informação e Comunicação (TIC). Obviamente, os avanços atuais só foram possíveis pela evolução tecnológica em muitas áreas, a saber, a informática, onde computadores minúsculos e poderosos agora existem com baixo custo e baixo consumo de energia e estão embutidos em muitos sistemas usados diariamente.

O prefixo ciber, de ciberespaço, é agora usado em muitos contextos, o que significa que as TIC estão difundidas em nossas vidas, desde empresas, administração pública, escolas, residências e até mesmo em nossos corpos (por exemplo, medidores de atividade física). A consciência do ciberbullying, da ciberdemocracia, do cibersexo, da ciberfraude, da ciberdefesa, do cibercrime, do ciberterrorismo, do ciberataque, da ciberguerra, da ciberdiplomacia e de muitas outras cresce diariamente.

A Convergência Tecnológica das Indústrias

Nos últimos trinta anos, três setores genéricos - informática, telecomunicações e mídia - convergiram, embora usando paradigmas e cronogramas diferentes, na era digital. Dos três, a informática se originou e desde o princípio operou na era digital. De fato, criados nos anos 50, os primeiros computadores eram inerentemente digitais. Inicialmente, os principais componentes digitais foram construídos usando válvulas eletrônicas, depois transistores, mas foi a invenção do circuito integrado que contribuiu para o avanço tecnológico da era digital.

Outro setor, o de telecomunicações, operava desde o início no domínio analógico. As redes de comunicações que cobrem o globo trocavam sinais analógicos por meio de redes telefônicas que transmitiam voz e de canais de rádio, que transmitiam música e voz; especialmente canais populares e redes de televisão transmitiam vídeo e som analógicos globalmente.

Infraestruturas de comunicação caras foram projetadas para habilitar essas redes, todas avançando em diferentes velocidades, expandindo a cobertura dentro de países, continentes e finalmente o mundo inteiro. Mas cada área de telecomunicações dependia de uma tecnologia de rede diferente que separava e dificultava a interconexão devido a diversas tecnologias. Essas redes eram, na maioria dos casos, monopólios do governo que operavam de forma bastante conservadora e dispendiosa. Inovação estava longe de ser uma prioridade. No final dos anos 60, a necessidade de integrar a comunicação por computador levou ao desenvolvimento de um tipo diferente de rede, projetada para interconectar computadores. Inerentemente digitais, essas redes de computadores, em contraste com as anteriormente descritas, transmitiam informações digitais na forma de sequências de vários dígitos binários (bits) chamados pacotes. Várias tecnologias foram desenvolvidas por diferentes empresas, grupos de pesquisa e órgãos de padronização, mas no final dos anos 80 uma tecnologia surgiu como a mais adequada, eficiente e rentável: a Internet, inventada por Vint Cerf e Bob Kahn[2].

O terceiro setor a convergir digitalmente foi a indústria de mídia. A produção e distribuição de jornais, revistas, música, vídeo (transmissão de TV, vídeos gravados em forma de fitas) começou a migrar do mundo analógico do papel, rádio, CD, VHS, etc., para o mundo digital. Até o advento da Internet, as organizações, públicas ou privadas, trocavam informações principalmente via papel; era uma economia baseada em papel.

Neste mundo digital convergente, o movimento e a distribuição de todos os tipos de informação utilizam a mesma infraestrutura, a Internet. Do ponto de vista do consumidor, isso é muito importante, já que um único provedor simplifica as relações contratuais. Da mesma forma, a facilidade com que a clientela pode ser atendida aumenta o rendimento do ponto de vista do fornecedor. Mas isso só ocorre em um mundo bem regulado e, por não ser assim, a segurança é uma grande preocupação para o futuro de uma internet aberta. Em relação à segurança, um único ponto de comunicação deve ser extremamente bem protegido no ciberespaço, daí a grande necessidade por cibersegurança.

A Transformação Digital

Na Europa, as atividades de P&D que abordam os desafios das TIC começaram a acelerar no final dos anos 80 do século passado e tiveram um papel significativo no aumento da percepção da

of the relevance of ICT and ICT-related industries to cope with the opportunities that were already envisaged. These activities used, at the core, the principles underlying the converged digital world. In the first semester of 2000 the eEurope-2002 Action plan was approved. It is a comprehensive set of measures and objectives to increase de adoption of ICT technologies as an important driver for the future[3].

Shortly after, there was a perception that security was a central problem that had to be addressed in a common way, since cooperation and knowledge-sharing was a crucial problem to be solved and this led to the creation, in 2004, of ENISA, the European Network and Information Security Agency (www.enisa.eu).

Then it was understood as very important to accelerate the development of a Digital Single Market (DSM) "in which the free movement of persons, services and capital is ensured and where the individuals and businesses can seamlessly access and engage in online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence"[4]. The digital single market required common approaches to be followed at the European Union level.

So the EU's Cybersecurity Strategy (*An Open, Safe and Secure Cyberspace*) was published jointly by the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy in 2013 to accompany the proposal for the Network and Information Security (NIS) Directive. It "clarifies the principles that should guide cybersecurity policy in the EU and internationally"[5].

So, cybersecurity must become one of the focal points for the digital society, especially due to the fact that many services that our daily lives rely on are based on digital technologies. Many examples could be presented but we mention just a few:

- SCADA systems[6] – these systems (Supervisory Control and Data Acquisition) are widely used in the management of distributed infrastructures and in industrial environments; these systems are computer based, use Internet or Internet-like communication technologies and must be carefully secured so that no disruption can occur due to lack of technical supervision or due to cybercrimes;

- Data protection – nowadays all kinds of data only exist in digital format, stored in different kinds of information systems; the extraordinary value of data (personal, business, administrative, ...) imposes special care in the handling and protection of this data; the EU developed a legislative process to create a framework for the protection of data of European citizens and organizations, the GDPR[7];

- Defense systems – these defense infrastructures, namely command and control systems, but also the associated communication networks, also have a very strong dependency on digital technologies; as such it is crucial that they are designed and carefully protected; an excellent example of best practices in the area can be found in the Tallinn Manual 2.0[8].

We are already witnessing a significant diffusion of ICT technologies and devices in many aspects of daily life, continually increasing at a rapid pace. The Internet of Things (IoT)[9] concept is widely present in our daily activities, and significantly impacts three areas: home, health and mobility/ transportation.

The European Union Context

The identification of the challenges posed by the digital transformation made clear that the survivability of our society is something that must be tackled in a very serious way. Unfortunately, many relevant actors in our society are not aware of the many dimensions that the digital transformationencompasses. Especially at the top-level management, in many large organizations and in SMEs, there is not an adequate understanding of all the implications of the digital transformation and of the fourth industrial revolution[10]. The vision that there is a need to invest in technology and also in the protection of the networks, information systems, applications and human capital involved in this process is a vision that only a few have.

So in the European Union (EU) there has been a continuous effort to build a comprehensive set of processes, including measures and legislative initiatives to improve the wide understanding of the challenges and to frame the future inside the EU. We believe

relevância das TIC e dos setores relacionados às TIC para lidar com as oportunidades que já eram previstas. Essas atividades usaram, na essência, os princípios subjacentes ao mundo digital convergente. No primeiro semestre de 2000, foi aprovado o plano de ação eEurope-2002, um conjunto abrangente de medidas e objetivos para aumentar a adoção de tecnologias TIC como motor importante para o futuro[3].

Pouco depois, houve a percepção de que a segurança era um problema central que tinha de ser tratado de forma comum, uma vez que a cooperação e a partilha de conhecimentos era um problema crucial a resolver, o que levou à criação, em 2004, da ENISA, Rede Europeia e Agência de Segurança da Informação (www.enisa.eu).

Foi então entendido como essencial acelerar o desenvolvimento de um Mercado Único Digital (Digital Single Market ou DSM) "no qual a livre circulação de pessoas, serviços e capital é assegurada e onde indivíduos e empresas podem acessar e participar de atividades online sob condições de concorrência leal e um elevado nível de proteção dos consumidores e dos dados pessoais, independentemente da sua nacionalidade ou local de residência "[4]. O mercado único digital exigiu abordagens comuns a serem seguidas a nível da União Europeia.

Assim, a Estratégia de Cibersegurança da UE (*um ciberespaço aberto, seguro e protegido*) foi publicada conjuntamente pela Comissão Europeia e pela Alta Representante da União Europeia para os Negócios Estrangeiros e a Política de Segurança em 2013 para acompanhar a proposta de diretiva de segurança das redes e da informação (NIS, na sigla em inglês). "Esclarece os princípios que devem orientar a política de cibersegurança na UE e a nível internacional"[5].

Assim, a cibersegurança deve se tornar um dos pontos focais da sociedade digital, especialmente devido ao fato de que muitos serviços nos quais o nosso dia a dia depende são baseados em tecnologias digitais. Muitos exemplos podem ser apresentados, mas mencionamos apenas alguns:

- Sistemas SCADA[6] - estes sistemas (Controle de Supervisão e Aquisição de Dados / Supervisory Control and Data Acquisition) são amplamente utilizados na gestão de infraestruturas distribuídas e em ambientes industriais; esses sistemas são baseados em computador, usam a internet ou tecnologias de comunicação similares à Internet e devem ser cuidadosamente protegidos para que não ocorra nenhuma disrupção devido à falta de supervisão técnica ou devido a cibercrimes;

- Proteção de dados - atualmente todos os tipos de dados existem (apenas) em formato digital, armazenados em diferentes tipos de sistemas de informação; o extraordinário valor dos dados (pessoal, comercial, administrativo, etc.) impõe um cuidado especial no manuseio e proteção desses dados; a UE desenvolveu um processo legislativo para criar um arcabouço para a proteção de dados de cidadãos e organizações europeias, o GDPR[7];

- Sistemas de defesa - estas infraestruturas de defesa, conhecidas como sistemas de comando e controle, mas também as redes de comunicação associadas a eças, são fortemente dependentes das tecnologias digitais; e, desse modo, é crucial que eles sejam projetados e cuidadosamente protegidos; Um excelente exemplo de boas práticas na área pode ser encontrado no Manual de Tallinn 2.0[8].

Já estamos testemunhando uma difusão significativa de tecnologias e dispositivos TIC em muitos aspectos da vida cotidiana, a um ritmo cada vez mais acelerado. O conceito de Internet das Coisas (IoT)[9] está amplamente presente em nossas atividades diárias e impacta significativamente três áreas: casa, saúde e mobilidade/transporte.

O contexto da União Europeia

A identificação dos desafios colocados pela transformação digital deixou claro que a capacidade de sobrevivência da nossa sociedade é algo que deve ser considerado de uma forma muito séria. Infelizmente, muitos atores relevantes em nossa sociedade não estão cientes das muitas dimensões que a transformação digital representa. Especialmente nos altos cargos de gestão, em muitas organizações de grande porte e também nas PMEs, não há uma compreensão adequada de todas as implicações da transformação digital e da quarta revolução industrial[10]. A perspectiva de que há necessidade de investir em tecnologia e também na proteção das redes, sistemas de informação, aplicações e capital humano envolvidos nesse processo é uma visão que poucos têm.

Assim, na União Europeia (UE), tem sido feito um esforço contínuo para construir um conjunto abrangente de processos, incluindo medidas e iniciativas legislativas para melhorar a

that, in an initial phase and in addition to the EU Cybersecurity Strategy of 2013, the most important action lines that have been pursued are: i) the R&D programs, namely Horizon 2020 that is the biggest EU Research and Innovation program; ii) the GDPR is the core of Europe's digital privacy legislation; iii) the NIS Directive (stands for Network and Information Systems Security) that is the at the core of cybersecurity measures.

The NIS Directive is, in the area of cybersecurity, the most relevant legal framework. Indeed the Directive identifies and creates a legal environment comprising three crucial areas:

- The establishment of a network of national CSIRTs (Computer Security Incident Response Teams) to give a major boost to the cooperation in response to cybersecurity incidents. In each member state a National CSIRT serves as the privileged organization to identify and process the response to incidents in close cooperation with the corresponding CSIRT in other(s) member state(s); this is crucial since security incidents frequently originate – potentially - in jurisdictions different from the one where the impact occurs; of course cooperation with CSIRTs operated by the private sector still continues, but each member state must have a well-known point of contact,

- The identification of essential services in a number of sectors: energy (electricity, gas, oil), transportation (terrestrial, maritime, aerial and rail), infrastructures of the financial system, banking system, health, , distribution of drinkable water and the digital infrastructures (IXP, DNS servers and Internet top-level domains). These essential services are, mostly, operated by the private sector and the Directive defines that incident reporting mechanisms have to be implemented and, if certain thresholds for the magnitude of the incident are exceeded there can be penalties to the entity that failed to protect the essential services, if that was the case.

- The digital services, identified as cloud services, online search services and online marketplaces, also have a notification of incidents mechanism, but due to their nature, a European wide mechanism is foreseen.

Each member state had to transpose the Directive to its legal national framework, in a period of up to two years of the publication of the Directive in the Official Journal (July 2016). Naturally there is a strong expectation around the observation of how this cybersecurity framework will impact the European institutions.

The EU Cybersecurity Act

In September 2017, in a speech in the European Parliament, President Juncker announced a further elaboration of how the EU deals with cybersecurity, presenting the EU Cybersecurity Act[11]. This act represents a major upgrade on how the EU will face the challenges of a world where, in addition to the aspects covered in the NIS Directive, there is the problem of the Internet of Things (IoT), the certification of products and services so that they follow several grades of compliance (to be chosen depending on the application area) and the new challenges resulting from the fourth industrial revolution. This includes, for sure, the implications of the way how social networks operate, the underlying algorithms and data protection aspects (GDPR and associated issues) that must be taken very seriously in the digitally connected world.

Industry 4.0

The fourth industrial revolution has a special impact on how the industry operates today. Industry 4.0 is quite frequently considered by some authors as superimposed to the fourth industrial revolution. We do not share this vison. Industry 4.0 is a subset of the fourth industrial revolution and refers to a major redesign of how existing industries operate, using an orientation more typical of ICT services, where machines have their capacities augmented with many sensors and actuators – replacing human operators – connected in the plant and with other plants located around the world and making several decisions on their own (better say, controlled by advanced algorithms). The supply chain of these connected factories is very susceptible to a varied set of problems, and cybersecurity must be at the center of the design of Industry 4.0 production lines. It is expected that Industry 4.0 shall be characterized by a significant increase in machine-to-machine (M2M) interactions. In this environment there are many challenges, but we shall focus only on two that we believe

compreensão dos desafios e enquadrar o futuro dentro da UE. Acreditamos que, numa fase inicial e adicionalmente à Estratégia de Cibersegurança da UE de 2013, as linhas de ação mais importantes que foram seguidas são: i) os programas de P&D, particularmente o Horizonte 2020, que é o maior programa de pesquisa e inovação da UE; ii) o GDPR, que é o cerne da legislação de privacidade digital da Europa; iii) a Diretiva NIS (sigla em inglês para Segurança de Redes e Sistemas de Informação), que é o cerne das medidas de cibersegurança.

A Diretiva NIS é, no domínio da cibersegurança, o mais relevante arcabouço jurídico. Com efeito, a diretiva identifica e cria um ambiente jurídico composto por três áreas cruciais:

- O estabelecimento de uma rede de CSIRTs (Equipes de Resposta a Incidentes de Segurança de Computadores) para dar grande impulso à cooperação em resposta a incidentes de cibersegurança. Em cada Estado-membro, uma CSIRT Nacional serve como organização privilegiada para identificar e processar a resposta a incidentes em estreita cooperação com a CSIRT correspondente em outro(s) Estado(s)-membro(s); isso é crucial, uma vez que os incidentes de segurança, frequentemente, são originados - potencialmente - em jurisdições diferentes daquela em que o impacto ocorreu; é claro que a cooperação com CSIRTs operadas pelo setor privado vai continuar, mas cada Estado-membro deve ter um ponto de contato bem conhecido,

- Identificação de serviços essenciais em vários setores: energia (eletricidade, gás, petróleo), transportes (terrestre, marítimo, aéreo e ferroviário), infraestruturas do sistema financeiro, sistema bancário, saúde, distribuição de água potável e infraestruturas digitais (IXP, servidores DNS e domínios de alto nível da Internet). Esses serviços essenciais são, na maioria das vezes, operados pelo setor privado. A Diretiva define que o mecanismo de notificação de incidentes deve ser implementado e, caso certos limites para a magnitude do incidente sejam excedidos, pode haver penalidades para a entidade que não protegeu o serviço essencial, se esse for o caso.

- Os serviços digitais, identificados como serviços em nuvem, serviços de pesquisa online e *marketplaces* online, têm também um mecanismo de notificação de incidentes, mas devido à sua natureza, está previsto um mecanismo a nível europeu.

Cada Estado-Membro teve de transpor a Diretiva para o seu arcabouço jurídico nacional, o que deveria ser concluído no prazo de dois anos após a publicação da diretiva no Diário Oficial (julho de 2016). Naturalmente, há uma forte expectativa em torno da observação de como essa estrutura de cibersegurança impactará as instituições europeias.

A lei da cibersegurança da UE

Em setembro de 2017, num discurso no Parlamento Europeu, o Presidente Juncker anunciou um novo avanço no modo como a UE lida com a cibersegurança, apresentando a Lei da Cibersegurança da UE[11]. Esta Lei representa um importante avanço em relação à forma como a UE irá enfrentar os desafios de um mundo onde, para além dos aspectos abrangidos pela Diretiva NIS, existe o problema da Internet das Coisas (IoT), a certificação de produtos e serviços de modo a que sigam diversos graus de conformidade (a serem escolhidos dependendo da área de aplicação) e os novos desafios resultantes da quarta revolução industrial. Isso certamente inclui as implicações do modo como as redes sociais operam, algoritmos subjacentes e aspectos da proteção de dados (GDPR e questões associadas) que devem ser levados muito a sério no mundo digitalmente conectado.

Indústria 4.0

A quarta revolução industrial tem um impacto especial na maneira como a indústria opera hoje em dia. A indústria 4.0 é frequentemente considerada por alguns autores como sobreposta à quarta revolução industrial. Nós não compartilhamos essa visão. A Indústria 4.0 é um subconjunto da quarta revolução industrial e refere-se a um grande redesenho de como as indústrias existentes operam, usando uma orientação mais típica dos serviços de TIC, onde as máquinas têm suas capacidades aumentadas com muitos sensores e atuadores - substituindo operadores humanos - conectados na fábrica e com outras fábricas localizadas em nível mundial e tomando várias decisões por conta própria (melhor dizendo, controladas por algoritmos avançados). A cadeia de suprimentos dessas fábricas conectadas é muito suscetível a um conjunto variado de problemas, e a cibersegurança deve estar no centro do projeto das linhas de produção da Indústria 4.0. Espera-se que a Indústria 4.0 seja caracterizada por um aumento significativo

are the ones requiring more attention: i) if cybersecurity is not implemented at all or is implement with design flaws, due to poor engineering practices, there is a likelihood that the production chains can be the target of cybercrimes (e.g., DDoS Attacks[12]) to disrupt the system or to steal intellectual property (as already happens today[13]); ii) the algorithms and procedures implemented in the automated industrial processes must be protected against industrial property theft and other forms of manipulation of the supply chain.

Other Domains of Relevance

We already mentioned that the prefix cyber is now used in many contexts and this is due to the fact that the digital transformation already started to be deployed and is widely used in our society. Now we shall highlight in a very brief way, due to limitations of this text, aspects that are very demanding and require special attention.

Cyberespionage is growing at a pace that should worry all nations. Indeed there are groups specialized in stealing State critical information to be used to target specific user groups or even countries, creating quite complex political scenarios. The identification of the origin and who mandates these groups in rather difficult, although there is a large confidence of their masters, but proofs are difficult to gather due to the nature of the ICT technologies used (e.g. APT28 – Advanced Persistent Threat 28). We call these groups cybermercenaries, by comparison with the working methods of the traditional mercenaries.

Future Challenges

The future is already here, so some of the aspects that we shall present are already being dealt in several fora, but there is a significant lack in their use or deployment in the relevant environments.

In the IoT realm, our society shall be faced with a significant presence of connected devices in our daily life, thus representing a new set of challenges that must be tackled in a very demanding way. It is crucial that the user, either professional or individual, has significant confidence that the system to be used has been certified by some independent authority.

The increased relevance of the algorithms implemented in the systems (13), that are increasingly software based, makes it essential that they are conformant with widely accepted norms and auditable by independent entities especially when AI systems are used[14].

There is an increased probability that new skills are necessary and job losses may happen for workers that have more difficulties in getting the new competences necessary in a society that is changing at a faster pace[15]. Also robot-based systems[16] may create problems to repetitive and low skilled jobs. It is still unclear if we can upgrade the skills of our labor force to the needs of the coming years, at an adequate pace. So the human capital is a central problem, ranging from the end-user to the ICT professional

The dependency of the infrastructures of our society, either the ones used by the overall population (as we have seen, named essential services in the NIS Directive) or infrastructures of defense systems, specially command and control systems, is a major problem and all governments must carry out all efforts to have special care with these systems.

All these areas require cybersecurity by design or the systems and devices we use will not succeed in ensuring a secure cyberspace.

Also for organizations and enterprises, the effect of digital transformation is leading to situations where all relevant data is now imbedded in computer systems, servers or in the cloud. Even critical information is handled digitally and from the lowest organizational levels to top management a security approach to this digital world is wanting, frequently referred to as “a cybersecurity mindset”.

New types of crimes[17] – cybercrimes – are already happening in large scale and many of them arise from shortfalls of digital identity[18]. Identity theft is a major problem and stronger authentication mechanisms are being implemented and must be used. But the human behavior is a critical problem and governments have a special role in providing more secure authentication systems for the citizens and securing public data using the most advanced technologies and practices.

nas interações máquina-máquina (M2M). Nesse ambiente, há muitos desafios, mas nos concentraremos apenas em dois que acreditamos ser os que exigem mais atenção: i) se a cibersegurança não for implementada ou se for implementada com falhas de design, devido a práticas de engenharia inadequadas, há a probabilidade de as cadeias produtivas serem alvo de cibercrimes (por exemplo, ataques DDoS[12]) para corromper o sistema ou roubar propriedade intelectual (como já acontece hoje em dia[13]); ii) os algoritmos e procedimentos implementados nos processos industriais automatizados devem ser protegidos contra roubo de propriedade industrial e outras formas de manipulação da cadeia de suprimentos.

Outras Áreas Relevantes

Já mencionamos que o prefixo ciber é atualmente usado em diversos contextos e isso se deve ao fato de que a transformação digital já começou a ser implantada e é amplamente utilizada em nossa sociedade. Agora, vamos destacar de uma forma muito breve, devido às limitações deste texto, aspectos que requerem atenção especial.

A ciberespionagem está crescendo a um ritmo que deve preocupar todas as nações. De fato, existem grupos especializados em roubar informações críticas de Estado a serem usadas para manipular grupos de usuários específicos ou mesmo países, criando cenários políticos bastante complexos. A identificação da origem e de quem dá as ordens a esses grupos é bastante difícil, embora exista uma grande confiança de seus mestres, mas as provas são difíceis de coletar devido à natureza das tecnologias de TIC usadas (por exemplo, APT28 - Advanced Persistent Threat 28 / Ameaça Persistente Avançada). Chamamos esses grupos de cibermercenários, por comparação com os métodos de trabalho dos mercenários tradicionais.

Desafios Futuros

O futuro já chegou, então alguns dos aspectos que apresentaremos já estão sendo tratados em vários fóruns, mas há uma significativa falha em seu uso ou implantação nos ambientes relevantes.

No mundo da IoT, nossa sociedade deve se deparar com uma presença significativa de dispositivos conectados em nossa vida diária, representando, assim, um novo conjunto de desafios que devem ser enfrentados de uma maneira exaustiva. É crucial que o usuário, profissional ou individual, tenha profunda confiança de que o sistema a ser utilizado foi certificado por alguma autoridade independente.

A maior relevância dos algoritmos implementados nos sistemas (13), cada vez mais baseados em software, exige que estejam em conformidade com as normas amplamente aceitas e que sejam auditáveis por entidades independentes, especialmente quando são usados sistemas de IA[14].

Há uma maior probabilidade de que novas habilidades sejam necessárias e que o desemprego aumente entre os trabalhadores que têm mais dificuldade em obter as novas competências necessárias em uma sociedade que está mudando a um ritmo mais acelerado[15]. Sistemas robóticos[16] também podem criar desafios aos empregados em trabalhos repetitivos e pouco qualificados. Ainda não está claro se podemos melhorar as habilidades de nossa força de trabalho para atender às necessidades dos próximos anos a ritmo adequado. Portanto, o capital humano é um problema central, desde o usuário final até o profissional de TIC.

A dependência das infraestruturas da nossa sociedade, quer as utilizadas pela população em geral (como vimos, os serviços essenciais indicados na Diretiva NIS) ou as infraestruturas dos sistemas de defesa, especialmente os sistemas de comando e controle, é um grande problema e todos os governos devem realizar todos os esforços possíveis para cuidar de modo especial desses sistemas.

Todas essas áreas exigem a implementação da cibersegurança desde seu projeto, caso contrário, os sistemas e dispositivos que usamos não conseguirão garantir um ciberespaço seguro.

Também para organizações e empresas, o impacto da transformação digital está levando a situações em que todos os dados relevantes estão embutidos em sistemas de computadores, servidores ou na nuvem. Até mesmo informações críticas são tratadas digitalmente e, desde os níveis mais básicos da organização até os altos cargos da administração, falta uma abordagem de segurança eficiente para esse mundo digital. Essa abordagem é frequentemente referida como “uma mentalidade de cibersegurança” (cybersecurity mindset).

Novos tipos de crimes[17] - cibercrimes - já estão ocorrendo em grande escala e muitos deles decorrem de falhas de identidade digital[18]. O

Conclusions

Let's recall that the Oxford dictionary[19] defines cybersecurity as "The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this". In our opinion this definition is incomplete since it focuses on "electronic data" alone.

As we tried to present some of our ideas we explained that the penetration of ICT is so pervasive in our daily lives, at both the organizational and personal level, we must rethink these past concepts. This can be a problem to the survivability of our society as it has developed in the last century.

The solution to our problems is not only a problem that can be solved by one actor, since it is a domain of shared responsibilities. The use of ICT, extensive in our society due to the convergence of the informatics, communications and media industries, results in a digital transformation that is shaping our way of living. From essential services such as energy, transport, banking and financial systems, the health sector, or in the use of ICT in the provision of public services, in e-Commerce or leisure, the need of increasing cybersecurity awareness in our society is critical.

Cybersecurity is not only a technical and technological problem, but has multiple dimensions within organizational models, new legal requirements, affecting the economic impact of organizations and the staff skills in all types of organizations. The algorithms used in ICT systems have to be clearly documented and auditable in a transparent way.

New types of crimes are also enabled by this new digital society, and a key factor in fighting these crimes is the capacity to understand the attack vectors used by criminals. The protection of the digital identity is one of the central problems requiring solutions, since e-identity is the entry point of many crimes. In this regard, cybersecurity measures must be understood and put into practice by all, sometimes posing limitations on our daily routines. Yet, these limitations are an essential factor to a secure presence in a digitally transformed society.

roubo de identidade é um grande problema e mecanismos de autenticação mais sólidos estão sendo implementados e devem ser usados. Mas o comportamento humano é um problema crítico e os governos têm um papel fundamental no fornecimento de sistemas de autenticação mais seguros para os cidadãos e na proteção de dados públicos usando as mais avançadas tecnologias e práticas.

Conclusões

Lembremos que o dicionário Oxford[19] define a cibersegurança como "o estado de estar protegido contra o uso criminoso ou não autorizado de dados eletrônicos, ou as medidas tomadas para alcançar isso". Em nossa opinião, essa definição é incompleta, pois se concentra apenas em "dados eletrônicos".

À medida que tentamos apresentar algumas de nossas ideias, explicamos que a penetração das TIC é tão difundida em nossas vidas diárias, tanto no nível organizacional quanto no pessoal, que precisamos repensar esses conceitos do passado. Isso pode ser um problema da sobrevivência da nossa sociedade que se desenvolveu no século passado.

A solução dos nossos problemas não é apenas um problema que pode ser resolvido por um ator, pois é um domínio de responsabilidades compartilhadas. O uso das TIC, extensivo em nossa sociedade devido à convergência das indústrias de informática, comunicação e mídia, resulta em uma transformação digital que está moldando nosso modo de viver. De serviços essenciais como energia, transporte, sistemas bancários e financeiros, setor de saúde, ao uso de TIC na prestação de serviços públicos, no comércio eletrônico ou no lazer, é necessário e fundamental aumentar a conscientização sobre cibersegurança em nossa sociedade.

A cibersegurança não é apenas um problema técnico e tecnológico, mas tem múltiplas dimensões dentro dos modelos organizacionais, novos requisitos legais, afetando o impacto econômico das organizações e as habilidades das equipes em todos os tipos de organizações. Os algoritmos usados nos sistemas de TIC devem ser claramente documentados e auditáveis de forma transparente.

Novos tipos de crimes também são viabilizados por essa nova sociedade digital, e um fator-chave no combate a esses crimes é a capacidade de entender os vetores de ataque usados pelos criminosos. A proteção da identidade digital é um dos problemas centrais que exigem soluções, uma vez que a identidade eletrônica é o ponto de entrada de muitos crimes. Nesse sentido, medidas de cibersegurança devem ser entendidas e colocadas em prática por todos, embora isso imponha, muitas vezes, limitações em nossas rotinas diárias. No entanto, essas limitações são um fator essencial para uma presença segura em uma sociedade transformada digitalmente.

1 Gibson, William. Neuromancer. London : Orion Publishing, 1984.

2 Barry, M. Leiner, et al. The past and future history of the Internet. Communications of the ACM. 2 1997, pp. 102-108.

3 European Commision. eEurope 2002. eEurope 2002. [Online] 2000. https://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:52000DC0330&rid=13.

4 —. A Digital Single Market Strategy for Europe. Brussels : European Commission, 2015.

5 Cybersecurity Strategy of the European Union. Brussels : European Commision, 2013.

6 Wikipedia. SCADA Systems. Wikipedia - SCADA Systems. [Online] 2019. https://en.wikipedia.org/wiki/SCADA.

7 European Commission. Principles of the GDPR. European Commission - Principles of the GDPR. [Online] 2017. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr_en.

8 NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual 2.0. Canbridge : Cambridge University Press, 2017.

9 Hakim, Cassimally and Adrian, McEwen. Designing the Internet of Things. New Jersey : John Wiley & Sons., 2013.

10 World Economic Forum. World Economic Forum - Forth Industrial Revolution. The Fourth Industrial Revolution: what it means, how to respond. [Online] 01 14, 2016. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

11 European Union. EU Cybersecurity Act. EU Cybersecurity Act. [Online] 06 26, 2019. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

12 Wikipedia. Denial of Service Attack. [Online] Wikipedia, 2018. https://en.wikipedia.org/wiki/Denial-of-service_attack.

13 Goodman, Marc. Future Crimes. Uxbridge : Bantam Press, 2015.

14 Domingos, Pedro. The Master Algorithm. s.l. : PENGUIN BOOKS LTD, 2017.

15 European Commission. A European Approach to Artificial Intelligence. A European Approach to Artificial Intelligence. [Online] 2019. https://ec.europa.eu/digital-single-market/en/artificial-intelligence.

16 OECD. Putting Faces to the Jobs at Risk of Automation. Paris : OECD, 2018.

17 European Parliament. Motion for a European Parliament Resolution on a comprehensive European industrial policy on artificial intelligence and robotics. European Parliament. [Online] 01 30, 2019. http://www.europarl.europa.eu/doceo/document/A-8-2019-0019_EN.html#title1.

18 Windley, Phillip. Digital Identity. California : O'Reilley Media, 2007.

19 Oxford University Press. Definition Cybersecurity. [Online] Oxford University, 2018. [Cited: 10 22, 2018.] https://en.oxforddictionaries.com/definition/cybersecurity.

20 ENISA. ENISA Threat Landscape Report 2018. ENISA Threat Landscape Report 2018. [Online] 01 28, 2019. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

21 Singer, P.W. and Friedman, Allan. Cybersecurity and Cyberwar: What Everyone Needs to Know. s.l. : Oxford University Press, 2014.

1 Gibson, William. Neuromancer. London : Orion Publishing, 1984.

2 Barry, M. Leiner, et al. The past and future history of the Internet. Communications of the ACM. 2 1997, pp. 102-108.

3 European Commision. eEurope 2002. eEurope 2002. [Online] 2000. https://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:52000DC0330&rid=13.

4 —. A Digital Single Market Strategy for Europe. Brussels : European Commission, 2015.

5 Cybersecurity Strategy of the European Union. Brussels : European Commision, 2013.

6 Wikipedia. SCADA Systems. Wikipedia - SCADA Systems. [Online] 2019. https://en.wikipedia.org/wiki/SCADA.

7 European Commission. Principles of the GDPR. European Commission - Principles of the GDPR. [Online] 2017. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr_en.

8 NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual 2.0. Canbridge : Cambridge University Press, 2017.

9 Hakim, Cassimally and Adrian, McEwen. Designing the Internet of Things. New Jersey : John Wiley & Sons., 2013.

10 World Economic Forum. World Economic Forum - Forth Industrial Revolution. The Fourth Industrial Revolution: what it means, how to respond. [Online] 01 14, 2016. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

11 European Union. EU Cybersecurity Act. EU Cybersecurity Act. [Online] 06 26, 2019. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

12 Wikipedia. Denial of Service Attack. [Online] Wikipedia, 2018. https://en.wikipedia.org/wiki/Denial-of-service_attack.

13 Goodman, Marc. Future Crimes. Uxbridge : Bantam Press, 2015.

14 Domingos, Pedro. The Master Algorithm. s.l. : PENGUIN BOOKS LTD, 2017.

15 European Commission. A European Approach to Artificial Intelligence. A European Approach to Artificial Intelligence. [Online] 2019. https://ec.europa.eu/digital-single-market/en/artificial-intelligence.

16 OECD. Putting Faces to the Jobs at Risk of Automation. Paris : OECD, 2018.

17 European Parliament. Motion for a European Parliament Resolution on a comprehensive European industrial policy on artificial intelligence and robotics. European Parliament. [Online] 01 30, 2019. http://www.europarl.europa.eu/doceo/document/A-8-2019-0019_EN.html#title1.

18 Windley, Phillip. Digital Identity. California : O'Reilley Media, 2007.

19 Oxford University Press. Definition Cybersecurity. [Online] Oxford University, 2018. [Cited: 10 22, 2018.] https://en.oxforddictionaries.com/definition/cybersecurity.

20 ENISA. ENISA Threat Landscape Report 2018. ENISA Threat Landscape Report 2018. [Online] 01 28, 2019. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

21. Singer, P.W. and Friedman, Allan. Cybersecurity and Cyberwar: What Everyone Needs to Know. s.l. : Oxford University Press, 2014.

5/6

KONRAD ADENAUER STIFTUNG

Incorporação de gênero na segurança internacional da América do Sul: Big Data, Regionalismo e Difusão de Normas

Gender Mainstreaming in South America's International Security: Big Data, Regionalism and Norm Diffusion

Mariana Kalil

CEBRI
BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS

COLEÇÃO DE POLICY PAPERS
THE POLICY PAPERS COLLECTION

XVIFORTE

A Conferência de Segurança Internacional do Forte de Copacabana é um projeto euro-brasileiro organizado em conjunto pela Fundação Konrad Adenauer (KAS) e pelo Centro Brasileiro de Relações Internacionais (CEBRI), com apoio da Delegação da União Europeia no Brasil. A conferência é concebida como um fórum de diálogo entre a América do Sul e a Europa. Seu objetivo é reunir especialistas do setor governamental, acadêmico e privado para discutir assuntos atuais no âmbito de segurança que sejam de interesse comum aos parceiros dos dois lados do Atlântico. Desde seu início em 2003, a conferência se transformou, de uma reunião relativamente pequena, no maior fórum de segurança da América Latina. Na sua 16ª edição, a conferência de 2019 tem como tema 'A Quarta Revolução Industrial: Impactos na Segurança Internacional e a Reformulação da Ordem Global'. A conferência é aberta ao público e os participantes são incentivados a participar ativamente das discussões. Esta coleção de Policy Papers reflete os temas centrais do evento e pretende identificar desafios, bem como fazer recomendações políticas para o futuro. As edições anteriores da publicação sobre Segurança Internacional da Conferência do Forte de Copacabana podem ser acessadas na página oficial da KAS Brasil (www.kas.de/brazil).

The Forte de Copacabana International Security Conference is a joint Euro-Brazilian project organised by the Konrad Adenauer Foundation (KAS) in partnership with the Brazilian Center for International Relations (CEBRI) and supported by the Delegation of the European Union to Brazil. The conference is conceived as a forum for dialogue between South America and Europe. It aims to bring together experts from a wide range of government, academic and private-sector backgrounds to discuss current security-related issues which are of interest to the partners on both sides of the Atlantic. Since its inception in 2003, the conference has emerged from a relatively small gathering to Latin America's largest security forum to date. The topic of the 16th edition of the conference is 'The Fourth Industrial Revolution: Impacts on International Security and the Reshaping of Global Order'. The conference is open to the public and the audience is encouraged to actively engage in discussions. This collection of Policy Papers reflects the major themes of the event and intends to identify challenges as well as make policy recommendations for the future. Previous volumes of the Forte de Copacabana International Security Conference publication can be accessed on the KAS-Brazil Office website (www.kas.de/brazil).

www.kas.de/brasil

Editor Editor
Anja Czymmeck

Coordenação editorial Project Coordination
Ariane Costa
Reinaldo Themoteo

Colaboração Editorial Support
Monique Sochaczewski

Tradução e revisão Translation and Revision
Leslie Sasson Cohen

Projeto Gráfico Design
Charles Steiman
Daniela Knorr

Impressão Print
Stamppa

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

COLEÇÃO DE POLICY PAPERS
THE POLICY PAPERS COLLECTION

1/6
Cibersegurança na América Latina
Cybersecurity in Latin America
Monica Herz

2/6
A quarta revolução industrial: Impactos na Segurança Internacional e a Reestruturação da Ordem Mundial - A perspectiva europeia
The Fourth Industrial Revolution: Impacts on International Security and the Reshaping of Global Order – The European Perspective
Kai Michael Kenkel

3/6
Inteligência artificial (IA) no balanço de poder na política internacional: uma perspectiva sul-americana
Artificial intelligence (AI) in the balance of power in world politics: a South American perspective
Jorge H. C. Fernandes

4/6
A Cibersegurança em um mundo conectado
Cybersecurity in a connected word
Pedro Veiga

5/6
Incorporação de gênero na segurança internacional da América do Sul: Big Data, Regionalismo e Difusão de Normas
Gender Mainstreaming in South America's International Security: Big Data, Regionalism and Norm Diffusion
Mariana Kalil

6/6
O Fator Gênero na Segurança Internacional
A Perspectiva Europeia
The Gender Factor in International Security
A European Perspective
Irene Giner-Reichl

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.

A Delegação da União Europeia (UE) no Brasil é uma das mais de 130 Delegações da UE no mundo. A Delegação da UE no Brasil está focada na promoção das relações políticas e econômicas entre a UE e o Brasil, de acordo com a parceria estratégica EU–Brasil estabelecida em 2007. A UE e o Brasil estabeleceram relações diplomáticas em 1960, criando estreitos laços históricos, culturais, econômicos e políticos. Dentre os tópicos centrais da parceria estratégica entre a UE e o Brasil 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. Mais de 30 diálogos formais no setor político foram iniciados entre a União Europeia e autoridades brasileiras para enfrentar esses desafios. Além disso, a União Europeia e o Brasil são parceiros comerciais importantes e os países da União Europeia recebem mais de 20% da exportação brasileira. A União Europeia também é o maior investidor estrangeiro no Brasil com cerca de 60% do investimento estrangeiro.

The European Union (EU) Delegation to Brazil is one of over 130 EU Delegations around the world. The EU Delegation to Brazil is focused on promoting political and economic relations between the EU and Brazil, in line with the EU–Brazil Strategic Partnership established in 2007. The EU and Brazil established diplomatic relations already in 1960 building on close historical, cultural, economic and political ties. Central topics of the EU–Brazil Strategic Partnership 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. Over 30 formal sector-policy dialogues between the European Union and Brazilian authorities have been initiated to address these challenges. The European Union and Brazil are also important trading partners and the countries of the European Union account for over 20% of Brazil's exports. The European Union is also the largest foreign investor in Brazil with around 60% of the foreign investment originating from the European Union.

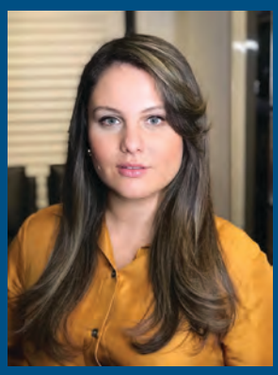
CEBRI
BRAZILIAN CENTER FOR
INTERNATIONAL RELATIONS

Independente, apartidário e multidisciplinar, o Centro Brasileiro de Relações Internacionais (CEBRI) é uma instituição sem fins lucrativos, que atua para influenciar positivamente a construção da agenda internacional do país. Fundado há 20 anos por um grupo de empresários, diplomatas e acadêmicos, o CEBRI tem ampla capacidade de articulação, engajando os setores público e privado, a academia e a sociedade civil. Além disso, conta com um Conselho Curador atuante e formado por figuras proeminentes, e com uma rede de mantenedores constituída por instituições, empresas e indivíduos de múltiplos segmentos.

O CEBRI promove a expansão e aprofundamento do debate sobre a política externa brasileira e a inserção do Brasil no mundo, pautado na formulação de políticas públicas e no fomento de diálogo entre os mais relevantes atores brasileiros e globais. O reconhecimento de sua importância internacional é atestado pelo ranking do Programa de Think Tanks e Sociedade Civil da Universidade da Pensilvânia, que destacou o CEBRI como o segundo melhor think tank do Brasil e o quarto melhor da América Latina.

Independent, nonpartisan and multidisciplinary, the Brazilian Center for International Relations (CEBRI) is a non-profit institution that acts to have a positive influence on the construction of the country's international agenda. Founded 20 years ago by a group of business leaders, diplomats and academics, CEBRI has the ability to engage the public and private sectors, academia and civil society. In addition, it counts on an engaged Board of Trustees formed by prominent figures and on a diverse network of sponsors made up of institutions, companies and individuals from multiple sectors.

CEBRI promotes the expansion and deepening of debates on Brazilian foreign policy and Brazil's international insertion, marked by the formulation of public policies and the promotion of dialogue amongst the most relevant Brazilian and global stakeholders. The recognition of its international importance is evidenced by the University of Pennsylvania's Think Tanks and Civil Societies Program, which ranked CEBRI as Brazil's second best think tank and the fourth best in Latin America.



Mariana Kalil
Mariana Kalil é professora da Cátedra de Geopolítica da Escola Superior de Guerra. Com Ph.D. e Mestrado em Relações Internacionais pela Universidade de Brasília (UnB), atualmente é Diretora de Publicidade da Seção de Teoria da International Studies Association (ISA), parte da Força-Tarefa da Seção de Estudos de Segurança Internacional (ISSS - ISA) sobre Diversidade em Estudos de Segurança , além de ter sido vice-presidente, diretora de comunicações e representante da América Latina no Global South Caucus da ISA. Suas publicações, aulas e interesses giram em torno de Teoria, Metodologia, Segurança e Defesa, Política Externa, Ameaças Não Convencionais e Crime Transnacional, Manutenção da Paz e Multilateralismo, Gênero, Redes Sociais e Big Data, além de Inteligência.

Mariana Kalil is Professor of the Geopolitics Chair of the Brazilian National War College. With Ph.D. and MSc degrees in International Relations from the University of Brasília (UnB), currently she is Publicity Officer at the International Studies Association's (ISA) Theory Section, part of the International Security Studies Section (ISSS - ISA) Task Force on Diversity in Security Studies, besides having been Vice-Chair, Communications Director and Latin America Rep at ISA's Global South Caucus. Her publications, classes, and interests revolve around Theory, Methodology, Security and Defense, Foreign Policy, Non-Conventional Threats and Transnational Crime, Peace Keeping and Multilateralism, Gender, Social Networks and Big Data, as well as Intelligence.

.

Incorporação de gênero na segurança internacional da América do Sul: Big Data, Regionalismo e Difusão de Normas

Gender Mainstreaming in South America's International Security: Big Data, Regionalism and Norm Diffusion

Mariana Kalil

Escola Superior de Guerra

Brazilian National War College

Introdução

A chegada da quarta revolução industrial vem alterando a forma como a política é feita. O Big Data, cada vez mais, fornece fontes diferentes de insumos, além de ferramentas de monitoramento e avaliação. Consequentemente, a análise de dados nunca foi tão relevante para a tomada de decisões.

Para abordar a questão de gênero na Segurança Internacional da América do Sul no século XXI, cabe, portanto, buscar dados sobre como o gênero é percebido nas sociedades sul-americanas. Nossa amostra de países resulta da análise de outro conjunto de dados sobre segurança internacional na região. Encontramos na Argentina, no Chile, na Colômbia, no Peru e no Brasil as amostras mais representativas do status quo da relação entre a América do Sul e segurança internacional e foi resultado da análise de todos os dados dos países da América do Sul sobre:

- O gasto médio com defesa (2008 - 2016);
- O número de militares por 10.000 cidadãos;
- O percentual de mulheres nas Forças Armadas;

Introduction

The coming of the fourth industrial revolution has been altering the way policy is made. Big data has increasingly provided different sources for inputs, as well as monitoring and evaluation. Consequently, data analysis has never been so relevant for decision-making.

To address the gender factor in South America's International Security in the twenty-first century, it is hence fitting to go after data on how gender is perceived across South American societies. Our countries sample results from the analysis of another body of data concerning international security within the region. We have found in Argentina, Chile, Colombia, Peru and Brazil the most representative samples of the status quo of South America's relationship with international security. This has been accomplished by examining all South American countries' data on:

- The average defense expenditure (2008 – 2016);
- The number of military personnel per 10.000 citizens;
- The percentage of women in the Armed Forces;

- The accessibility to women of total or partial roles within the Forces;

- The number of women who have occupied leadership roles in top directly-related to international security decision-making positions – Presidency, Ministry of Defense, Ministry of Foreign Affairs; and

- The current percentage of women in the federal legislative bodies.

(Source: Atlas Comparativo de la Defensa 2016)

In turn, the most representative open source data on how South American people view gender has been which topics are related to "Woman" and "Gender" in their profile on Google searches[1]. Contrasting this with a Western European sample, besides United States', as well as a worldwide trend has provided grounds for a diagnosis, conclusions and recommendations over the gender factor in South America's international security.

The Gender Factor in International Security: a Diagnosis of South American Societies

The late UNASUR's Defense Council and Security Council provide prolific sources on how South American countries dealt with gender issues in the scope of international security from the first decade of the twenty-first century until 2017. At UNASUR in general, and particularly thenceforth the creation of the Defense Council (2008), the organization had been the locus for regional affirmation of each country's and the collective perspectives on many issues. On international security, they have been the most clear-cut in affirming their national and regional calls given particularly the Defense Council denouncing posture over external influence in the region (Kalil 2015). The Security Council encompasses cooperation regarding non-conventional threats to international security and the regional attempt to cooperate among the judiciary branches, as well as the national and local police forces.

- A total of 89 documents provided by UNASUR's repository on the proceedings within these two Councils were analyzed. Searching for whether and how they included gender issues has been revealing particularly when contrasted with how South American people think of gender. Google Trends provides the following insights:

- Career, Health, Identity and Sexuality (I&S), Politics and Policy (P&P), Race, as well as Violence are the most recurring related-themes worldwide when the topics "Gender" and "Woman" are googled;

- In South American societies, with the exception of Argentina, gender issues are strongly approached under the rigid and traditional dichotomy of male and female stereotypes;

- In South American societies, with the exception of Chile, the category Violence is central to how people deal with gender issues;

- In South American societies, sexuality and identity are markedly binary and emphasize biological traces;

- In South American societies, there is a general concern over how gender issues are treated in P&P by the State;

- In South America, Argentinians are the most progressive people when gender is concerned;

- Consistent with their State representatives' gender profile[2], the Brazilian and the Chilean are the least progressive peoples in South America[3];

- In South America, there is an expectation the State will act as a gatekeeper of gender issues[4];

- In Chile and in Brazil, the topic "ideology" weighs in on P&P and yield further costs to approaching gender issues in a progressivist manner.

(Source: Google Trends 2019 – data treated by the author)

In South America, thus, the prevailing treatment of gender issues drastically differs from how Western Europe and the United States approach the matter. While liberalism has entailed a more individualistic perspective in the United States, it has paired with the welfare state to produce a Western European scenario where the European Union, United Nations' agencies, and the

- A acessibilidade das mulheres a papéis totais ou parciais dentro das Forças Armadas;

- O número de mulheres que ocuparam cargos de liderança diretamente relacionados a posições de tomada de decisões sobre segurança internacional - Presidência, Ministério da Defesa, Ministério das Relações Exteriores; e

- O percentual atual de mulheres nos órgãos legislativos federais

(Fonte: Atlas Comparativo de la Defensa 2016)

Por outro lado, os dados de código aberto mais representativos sobre como as pessoas da América do Sul veem o gênero foram os tópicos relacionados a "Mulher" e "Gênero" em seu perfil de pesquisas do Google[1]. Contrapondo isso com uma amostra da Europa Ocidental, além da tendência dos Estados Unidos, bem como mundial, forneceu base para um diagnóstico, conclusões e recomendações sobre a questão de gênero na segurança internacional da América do Sul.

A questão de gênero na segurança internacional: um diagnóstico das sociedades sul-americanas

Os extintos Conselho de Defesa e Conselho de Segurança da UNASUL fornecem fontes prolíficas sobre como os países da América do Sul lidam com questões de gênero no âmbito da segurança internacional desde a primeira década do século XXI até 2017. A UNASUL em geral, e particularmente a partir da criação do Conselho de Defesa (2008), a organização foi o espaço para a afirmação regional de cada país e as perspectivas coletivas sobre muitas questões. Quanto à segurança internacional, eles têm sido claros na afirmação de seus apelos nacionais e regionais, especialmente junto à postura denunciante do Conselho de Defesa em relação à influência externa na região (Kalil 2015). O Conselho de Segurança engloba a cooperação em relação a ameaças não convencionais à segurança internacional e a tentativa regional de cooperação entre os Poderes Judiciários, bem como entre as forças policiais nacionais e locais.

Um total de 89 documentos fornecidos pelo repositório da UNASUL sobre os procedimentos nesses dois Conselhos foram analisados. A pesquisa sobre se e como eles incluíram questões de gênero tem sido particularmente reveladora quando contrastada com a forma como as pessoas sul-americanas pensam sobre gênero. O Google Trends fornece a seguinte visão:

- Carreira, Saúde, Identidade e Sexualidade (I&S), Política e Políticas (P&P), Raça, bem como Violência são os temas relacionados mais recorrentes em todo o mundo quando os tópicos "Gênero" e "Mulher" são pesquisados;

- Nas sociedades sul-americanas, com exceção da Argentina, as questões de gênero são fortemente abordadas sob a rígida e tradicional dicotomia de estereótipos masculinos e femininos;

- Nas sociedades sul-americanas, com exceção do Chile, a categoria Violência é fundamental para o modo como as pessoas lidam com questões de gênero;

- Nas sociedades sul-americanas, a sexualidade e a identidade são marcadamente binárias e enfatizam traços biológicos;

- Nas sociedades sul-americanas, há uma preocupação geral sobre como as questões de gênero são tratadas na política e pelas políticas do Estado;

- Na América do Sul, os argentinos são os mais progressistas quando se trata de gênero;

- Em consonância com o perfil de gênero de seus representantes governamentais[2], o brasileiro e o chileno são os povos menos progressistas da América do Sul[3];

- Na América do Sul, há uma expectativa de que o Estado agirá como um guardião das questões de gênero[4];

- No Chile e no Brasil, o tópico "ideologia" influencia o item P&P e gera custos adicionais para abordar as questões de gênero de maneira progressista.

(Fonte: Google Trends 2019 – dados processados pelo autor)

Na América do Sul, portanto, o tratamento das questões de gênero difere drasticamente de como a Europa Ocidental e os Estados Unidos abordam o assunto. Embora o liberalismo tenha implicado uma perspectiva mais individualista nos Estados Unidos, ele se uniu ao Estado de bem-estar social para produzir um cenário

Organization for Economic Cooperation and Development are key stakeholders to gender issues particularly where Policy and Politics are concerned. Moreover, in Western Europe, there is a recurring attention to the evolution and the relevance of science in gender issues, and topics such as "Theory" and "Gender Studies" are constants throughout google searches of "Woman" and "Gender" as topics across the United Kingdom, Germany, France, and Belgium from January 2004 until June 2019.

The US and Western Europe concentrate most of the searches on the topics "Woman" and "Gender", hence the bias of the worldwide sample. In those regions, the searches do not relate these topics to dichotomous views of male and female, nor do they perceive the State as the gatekeeper of gender issues. In the US and in Western Europe, the occurrence of the topic "mainstreaming" associated to other positive codes point toward a common ground on the imperative of promoting gender equality and on the mere existence of a reality where there are gender nuances. The scenario is drastically different in South America. However, documents from UNASUR's Defense Council and Security Council show a process of norm diffusion (Acharya 2004; Archivo Digital de UNASUR 2019). The next part focuses on the content of proceedings within these Councils.

Big Data & UNASUR: Explaining the Failure of Gender Mainstreaming in South American International Security

The decontextualized appropriation of processes of gender mainstreaming developed within the United Nations ran its own course within UNASUR, a phenomenon of South American regionalism. However, it hints toward one of the reasons the organization was accused of being a product of ideas that are artificial, foreign to South American peoples' "actual" identities. The nationalist wave that dismantled UNASUR argues that the organization followed a "globalism" – hereby also referred as "moral cosmopolitanism" – based on values encroached at the UN allegedly seeking to pervert the countries' self-determination. One of these exogenous values is precisely feminism. The contextualization of UNASUR's attempts to mainstream gender in South America's Armed Forces and security forces allows for recommendations on how to refine good practices and advance the gender agenda in the region in spite of current backlashes.

The study of norm diffusion allows for a better grasp of what went wrong at UNASUR's attempt to mainstream gender in South America, culminating with the its own demise. Acharya (2004) thus introduces risks norm diffusers run when they do not contextualize their proposals:

> The moral cosmopolitanism perspective has contributed to two unfortunate tendencies. First, by assigning causal primacy to "international prescriptions," it ignores the expansive appeal of "norms that are deeply rooted in other types of social entities – regional, national, and subnational groups." Moreover, this perspective sets up an implicit dichotomy between good global or universal norms and bad regional or local norms. (...)
>
> Second, moral cosmopolitanists view norm diffusion as teaching by transnational agents, thereby downplaying the agency role of local actors (Acharya 2004: 242).

At UNASUR's Defense and Security Councils, the region's own representatives assumed a moral cosmopolitanist perspective. Not necessarily by their own desire, since, much in accordance with the public opinion mood over gender issues, the political stances of both international security-related councils at UNASUR delegated the matter of gender to their executive bodies, neither even mentioning the gender factor in any of their annual or bi-annual Strategic Plans.

Particularly the Defense Council further delegated gender matters to the Center for Strategic Studies in Defense. Hence, there is an original sin in this Council's attempt to mainstream gender throughout South America's Armed Forces: it withdrew these focal points from other political and executive bodies, ghettoizing rather than mainstreaming the gender factor. This has had implications within the Council. The proceedings of the Council's War College meetings, for instance, do not mention the gender factor.

Both councils restricted gender mainstreaming to diversifying the composition of the Armed Forces and

na Europa Ocidental onde a União Europeia, as agências das Nações Unidas e a Organização para a Cooperação e Desenvolvimento Econômico são os principais stakeholders em questões de gênero, particularmente no que se refere à política (P&P). Além disso, há, na Europa Ocidental, uma atenção recorrente à evolução e à relevância da ciência em questões de gênero, e tópicos como "Teoria" e "Estudos de gênero" são constantes em todas as pesquisas no Google sobre os tópicos "Mulher" e "Gênero" em todo o Reino Unido, Alemanha, França e Bélgica, de janeiro de 2004 a junho de 2019.

Os EUA e a Europa Ocidental concentram a maioria das buscas sobre os tópicos "Mulher" e "Gênero", e daí advém o viés da amostra mundial. Nessas regiões, as buscas não relacionam esses tópicos a visões dicotômicas de homens e mulheres, nem percebem o Estado como o guardião das questões de gênero. Nos EUA e na Europa Ocidental, a ocorrência do tópico "mainstreaming" (incorporação) associado a outros códigos positivos aponta para uma base comum sobre o imperativo de promover a igualdade de gênero e para a mera existência de uma realidade onde existem nuances de gênero. O cenário é drasticamente diferente na América do Sul. No entanto, documentos do Conselho de Defesa da UNASUL e do Conselho de Segurança mostram um processo de difusão de normas (Acharya 2004; Archivo Digital de UNASUR 2019). A próxima parte enfoca o conteúdo dos procedimentos dentro desses Conselhos.

Big Data e UNASUL: Explicando o fracasso da incorporação (mainstreaming) da perspectiva de gênero na segurança internacional sul-americana

A apropriação descontextualizada de processos de mainstreaming de gênero desenvolvidos dentro das Nações Unidas seguiu seu próprio curso dentro da UNASUL, um fenômeno do regionalismo sul-americano. No entanto, sugere uma das razões pelas quais a organização foi acusada de ser produto de ideias artificiais e estranhas às identidades "reais" dos povos sul-americanos. A onda nacionalista que desmantelou a UNASUL argumenta que a organização seguiu um "globalismo" - aqui também chamado de "cosmopolitismo moral" - baseado em valores usurpados da ONU, supostamente buscando corromper a autodeterminação dos países. Um desses valores exógenos é precisamente o feminismo. A contextualização das tentativas da UNASUL de integrar o gênero nas Forças Armadas e nas forças de segurança da América do Sul permite propor recomendações sobre como refinar as boas práticas e avançar a agenda de gênero na região, apesar da atua resistência.

O estudo da difusão de normas permite uma melhor compreensão do que deu errado na tentativa da UNASUL de incorporar as questões de gênero na América do Sul, culminando com a sua própria extinção. Acharya (2004) introduz, assim, os riscos que os difusores de normas de riscos correm quando não contextualizam suas propostas.

> A perspectiva do cosmopolitismo moral contribuiu para duas tendências infelizes. Primeiro, ao atribuir primazia causal a "prescrições internacionais", ignora o apelo expansivo de "normas que estão profundamente enraizadas em outros tipos de entidades sociais - grupos regionais, nacionais e subnacionais". Além disso, essa perspectiva estabelece uma dicotomia implícita entre normas globais ou universais boas e normas regionais ou locais ruins. (...)
>
> Em segundo lugar, os cosmopolitas morais veem a difusão da norma como ensinamento pelos agentes transnacionais, minimizando, assim, o papel de agência dos atores locais. (Acharya 2004: 242).

Nos Conselhos de Defesa e de Segurança da UNASUL, os próprios representantes da região assumiram uma perspectiva cosmopolita moral. Não necessariamente por vontade própria, já que, de acordo com a opinião pública sobre as questões de gênero, as posições políticas de ambos os conselhos da UNASUL delegaram a questão de gênero a seus órgãos executivos, sem mencionar o fator gênero em qualquer um dos seus Planos Estratégicos anuais ou bianuais.

Particularmente, o Conselho de Defesa foi além e delegou as questões de gênero ao Centro de Estudos Estratégicos em Defesa. Há, portanto, uma falha primordial na tentativa do Conselho de integrar a questão de gênero nas Forças Armadas da América do Sul: retirou esses pontos focais de outros órgãos políticos e executivos, confinando em vez de incorporando o fator gênero. Isso teve implicações no Conselho. Os resultados das reuniões da Escola Superior de Guerra do Conselho, por exemplo, não mencionam o fator gênero.

of domestic security forces through the insertion of women in these bodies, replicating efforts made in the case of the countries' participation in the military component of MINUSTAH. The presence of women in positions of power within the security and the military hierarchies, as well as in combat roles was formally included. Data was raised and goals were set withdrawn from political considerations.

This attempt to diffuse gender mainstreaming helps explain the sentiment of an internationalist gender ideology among the conservative nationalist wave in South America. The internationalist component also results from these groups' – particularly the Armed Forces – experience with the United Nations' standards in peace operations, particularly the common experience some of them shared in Haiti.

The vocabulary and the strategy of gender mainstreaming carried out within both councils at UNASUR does follow the prescriptive norm displayed at the United Nations' handbook (2002). The prescriptive norm might have been taken for granted given a pragmatic attempt to fit in or a belief in moral cosmopolitanism. Under a moral cosmopolitanist perspective, the prescriptive norm is better because it is more efficient and it is useful. Norm takers, hence, do not have any role in contextualizing them (Acharya 2004). However, at both UNASUR's Councils, the norm takers ignored a complementary part of the UN's handbook that would have contextualized the policy, perhaps avoiding an authoritarian feel among its recipients.

Moreover, even congruence, a top-bottom "fit between international norms and domestic norms" (Idem: 243), was overlooked by the Councils´ social infrastructure. This seems to have been the case, since gender mainstreaming was relegated to executive and academic bodies where norm diffusers themselves, isolated from the overall process, working under a specific mandate, and perhaps outliers themselves within their own populations, hence not representative of the trends hereby presented. In the case of the Justice Council, this is even more transparent, as gender mainstreaming was delegated to Argentinian representatives, and Argentina is the most progressive country in South America in terms of gender according to our big data analysis.

The most recent regional attempt to mainstream gender regionally, hence, has carried blind spots concerning the process of norm diffusion. There have been political consequences to this slip. Nationally, this negligence over the agency of the actual norm taker has been unfortunate notably in the cases of Chile and Brazil, the two most conservative societies in matters of gender, whose Armed Forces and security forces are historically some of the pinnacles of each of their conservatism, and whose Armed Forces had already been exposed to a "globalist" or a "moral cosmopolitanist" "gender ideology", as they call it, under the guise of the United Nations, as they were the two countries who contributed with the largest number of troops to MINUSTAH. The hierarchical characteristic of the Armed Forces, as well as of several of South America's domestic security forces combined with the relatively recent experience in civilian oversight of the military make up the context upon which the diffusion of gender mainstreaming took place.

Even though the Councils' representatives were nationals from each of the South American countries, they failed to invest gender mainstreaming with the characteristics of their own nations: they failed to localize the norm.

> I define localization as the active construction (through discourse, framing, grafting, and cultural selection) of foreign ideas by local actors, which results in the former developing significant congruence with local beliefs and practices. Wolters, a leading proponent of localization in Southeast Asian studies, calls this a "local statement... into which foreign elements have retreated (Acharya 2004: 245)."

UNASUR then did not bring the countries' Armed Forces' and security forces' peculiarities to the table, which would entail several steps of what the UN handbook actually states – and which takes time to be applied, since it must consider the ripeness of the context. For several reasons including the still fragile logic of civilian oversight of the military in South America, UNASUR's political bodies received the results from the executive bodies and passed them on as good practices that would yield better national and regional credentials and thus should be applied.

Ambos os conselhos restringiram a incorporação (mainstreaming) do fator de gênero à diversificação da composição das Forças Armadas e das forças de segurança internas por meio da inserção de mulheres nesses órgãos, replicando os esforços feitos no caso da participação dos países no componente militar da MINUSTAH. A presença de mulheres em posições de poder dentro das hierarquias de segurança e militar, bem como em papéis de combate foi formalmente incluída. Os dados foram levantados e as metas foram estabelecidas à margem de considerações políticas.

Essa tentativa de dispersar a incorporação da questão de gênero ajuda a explicar o sentimento de haver uma ideologia de gênero internacionalista entre a onda nacionalista conservadora na América do Sul. O componente internacionalista também resulta da experiência desses grupos - particularmente das Forças Armadas - com os padrões das Nações Unidas em operações de paz, particularmente a experiência comum que alguns deles compartilharam no Haiti.

O vocabulário e a estratégia de incorporação de gênero realizada em ambos os conselhos da UNASUL seguem a norma prescritiva apresentada no manual das Nações Unidas (2002). A norma prescritiva pode ter sido assumida como certa, devido a uma tentativa pragmática de se encaixar ou uma crença no cosmopolitismo moral. Sob uma perspectiva moral cosmopolita, a norma prescritiva é melhor porque é mais eficiente e útil. Os disseminadores de normas, portanto, não têm nenhum papel em contextualizá-las (Acharya 2004). No entanto, em ambos os Conselhos da UNASUL, os disseminadores de normas ignoraram uma parte complementar do manual da ONU que contextualizava a política e poderia, talvez, evitar o sentimento autoritário entre seus destinatários.

Além disso, mesmo a congruência, um "ajuste de cima para baixo entre as normas internacionais e as normas domésticas" (Idem: 243) foi negligenciada pela infraestrutura social dos Conselhos. Esse parece ter sido o caso, já que a incorporação (mainstreaming) de gênero foi relegada a órgãos executivos e acadêmicos, sendo eles mesmos os difusores de normas, isolados de todo o processo, trabalhando sob um mandato específico, e talvez até eles mesmos, marginalizados em suas próprias populações, não sendo, portanto, representativos das tendências aqui apresentadas. No caso do Conselho de Justiça, isso é ainda mais transparente, uma vez que a incorporação (mainstreaming) de gênero foi delegada a representantes argentinos, e a Argentina é o país mais progressista da América do Sul em termos de gênero, de acordo com nossa análise de big data.

A tentativa regional mais recente de integrar regionalmente o gênero, portanto, tem gerado pontos cegos em relação ao processo de difusão da norma. Houve consequências políticas desse lapso. Em âmbito nacional, essa negligência em relação à instrumentalização do disseminador de normas foi lamentável, especialmente nos casos do Chile e do Brasil, as duas sociedades mais conservadoras em questões de gênero da região e cujas Forças Armadas e forças de segurança são, historicamente, os pináculos de seu conservadorismo, além de terem sido expostas a uma "ideologia de gênero" "globalista" ou de cunho "moral cosmopolita", como eles dizem, sob a máscara das Nações Unidas, uma vez que são os dois países que contribuíram com o maior número de tropas para o MINSUTAH. A característica hierárquica das Forças Armadas, bem como de várias forças de segurança domésticas da América do Sul, combinada com a experiência relativamente recente na supervisão civil dos militares, compõem o contexto no qual a difusão da incorporação de gênero ocorreu.

Embora os representantes dos Conselhos fossem nacionais de cada um dos países sul-americanos, eles não conseguiram inserir a incorporação de gênero nas características de suas próprias nações: não conseguiram localizar a norma, ou seja, torna-la local.

> Eu defino a localização como a construção ativa (através do discurso, enquadramento, enxerto e seleção cultural) de ideias estrangeiras por atores locais, o que resulta no desenvolvimento pelo primeiro de uma congruência significativa com as crenças e práticas locais. Wolters, um dos principais defensores da localização em estudos do Sudeste Asiático, chama isso de "declaração local ... na qual os elementos estrangeiros recuaram" (Acharya 2004: 245).

A UNASUL, portanto, não trouxe as peculiaridades das Forças Armadas e das forças de segurança para a mesa, o que implicaria várias etapas do que o manual da ONU afirma - e que leva tempo para ser aplicado, já que deve considerar a maturidade do contexto. Por várias razões, incluindo a lógica ainda frágil da supervisão civil dos militares na América do Sul, os

The juxtaposition of internationally acclaimed good – efficient and useful – practices over gender issues to international security bodies in South America has overlooked the need to complement them "with inputs designed to address specific gaps or problems faced in the promotions of gender equality", as well as the fundamental role experts and catalysts play in the "implementation of gender mainstreaming". The working groups or the focal points within UNASUR's councils were isolated from the other working groups and from the overall political process undertaken in accordance with their Strategic Plans. They have also worked separately from national bureaucratic contexts, overlooking the catalysts' role in deepening "awareness, knowledge, commitment and capacity of all professional staff [within the bureaucracy it sought to influence]. (UN Handbook 2002)"

The intent to mainstream gender across South America's international security through a top-bottom strategy where the recipients of the new policies were precisely the most conservative populations in South American societies has also overlooked the instrumental requirement of the support of "gender focal points and gender units throughout the system". It has failed to localize gender mainstreaming. These dynamics help explain the sentiment of an internationalist gender ideology among the conservative nationalist movements in South America. If gender is to be mainstreamed in South American perspectives, as well as practices in international security, it is imperative it is localized. The next part concludes this paper with recommendations over how to localize gender mainstreaming as a norm in South America.

Recommendations

Acharya (2004) helps understand why investing in catalysts and in gender focal points throughout the system is key to successfully mainstreaming gender – or diffusing any good practice – in South America. The idea of a local initiative would be central to convincing a society of the need to play by certain rules. This opens the doors to finding catalysts who are capable of performing a "cultural selection: borrowing [from the international norm] only those ideas that are, or can be made congruent with local beliefs and that may enhance the prestige of the borrower (Idem: 246). Acharya underlines the importance of elevating "the profile and prestige of local actors and beliefs" in this process not only as a form of co-opting these actors but of granting the norm taker protagonist agency throughout the process.

The UN 2002 Handbook and its corollaries do point out in these directions (UN Handbook 2002; Manual para la incorporación de la perspectiva de género en la programación común a escala nacional 2018). Yet, UNASUR itself has not followed them. Creating catalysts and focal units within the main regional and national stakeholders on gender mainstreaming would hence represent an opportunity for cooperation between South America and Europe. In light of the Western European countries' context, and of their recognition of the European Union's central role in safeguarding better practices in gender issues on and beyond international security, these countries and the EU could provide training to South American civil servants and military personnel, as well as invest in raising awareness and creating national and regional knowledge on the gender factor.

KAS has a rather strategic presence within the international security community particularly in Brazil. This type of platform represents an opportunity for the implementation of said recommendations. Bringing about change, creating a more peaceful world, and a sustainable co-existence on Earth is currently as challenging as it has ever been since 9/11, especially in societies where the gender factor is perceived as dichotomous as in South America.

órgãos políticos da UNASUL receberam os resultados dos órgãos executivos e os transmitiram como boas práticas que renderiam melhores credenciais nacionais e regionais e, portanto, deveriam ser aplicadas.

A justaposição de boas – eficientes e úteis - práticas internacionalmente aclamadas sobre questões de gênero a órgãos de segurança internacionais na América do Sul negligenciou a necessidade de complementá-las "com insumos destinados a abordar lacunas específicas ou problemas enfrentados na promoção da igualdade de gênero", bem como o papel fundamental que os especialistas e catalisadores desempenham na "implementação da incorporação (mainstreaming) de gênero". Os grupos de trabalho ou os pontos focais dos conselhos da UNASUL foram isolados dos outros grupos de trabalho e do processo político geral realizado de acordo com seus Planos Estratégicos. Eles também trabalharam separadamente dos contextos burocráticos nacionais, negligenciando o papel dos catalisadores no aprofundamento da "conscientização, conhecimento, compromisso e capacidade de todo o pessoal profissional [dentro da burocracia que buscava influenciar]. (Manual da ONU, 2002)"

A intenção de incorporar o gênero na segurança internacional da América do Sul por meio de uma estratégia que vem de cima para baixo, onde os beneficiários das novas políticas seriam precisamente as populações mais conservadoras nas sociedades sul-americanas, também negligenciou a exigência instrumental do apoio aos "pontos focais de gênero e unidades de gênero em todo o sistema ". Não conseguiu dar à incorporação (mainstreaming) de gênero uma cor local. Essas dinâmicas ajudam a explicar a percepção de uma ideologia de gênero internacionalista entre os movimentos nacionalistas conservadores na América do Sul. Se o gênero deve ser incorporado nas perspectivas da América do Sul, assim como as práticas de segurança internacional, é imperativo que seja adaptado e localizado. A próxima parte conclui este artigo com recomendações sobre como tornar a incorporação de gênero algo local na forma de norma na América do Sul.

Recomendações

Acharya (2004) ajuda a entender por que investir em catalisadores e em pontos focais de gênero em todo o sistema é fundamental para incorporar com sucesso o gênero - ou difundir qualquer boa prática - na América do Sul. A ideia de uma iniciativa local seria fundamental para convencer a sociedade da necessidade de agir de acordo com certas regras. Isso abriria as portas para encontrar catalisadores capazes de realizar uma "seleção cultural: tomando emprestado [da norma internacional] apenas aquelas ideias que sejam, ou que poderiam ser, congruentes com as crenças locais e que poderiam aumentar o prestígio desses catalizadores" (Idem: 246). Acharya sublinha a importância de elevar "o perfil e o prestígio dos atores e das crenças locais" neste processo, não apenas como uma forma de cooptar esses atores, mas também de conceder protagonismo aos disseminadores durante todo o processo.

O Manual das Nações Unidas de 2002 e seus corolários apontam nessas direções (Manual das Nações Unidas 2002 Manual para la incorporación de la perspectiva de género en la programación común a escala nacional 2018). No entanto, a própria UNASUL não seguiu essas diretrizes. A criação de catalisadores e unidades focais nas principais partes interessadas regionais e nacionais sobre a incorporação da perspectiva de gênero representaria, portanto, uma oportunidade de cooperação entre a América do Sul e a Europa. Considerando o contexto dos países da Europa Ocidental e o reconhecimento do papel central da União Europeia na salvaguarda de melhores práticas em questões de gênero, para além da segurança internacional, esses países e a UE poderiam fornecer formação a funcionários públicos e militares da América do Sul, além de investir na conscientização e na criação de conhecimento nacional e regional sobre a questão de gênero.

A KAS tem uma presença bastante estratégica dentro da comunidade de segurança internacional, particularmente no Brasil. Esse tipo de plataforma representa uma oportunidade para a implementação dessas recomendações. Trazer mudanças, criar um mundo mais pacífico e uma coexistência sustentável na Terra é atualmente tão ou mais desafiador do que tem sido desde o 11 de setembro, especialmente em sociedades onde o fator de gênero é percebido como dicotômico como na América do Sul.

1 According to UNESCO, North America (81%) and Europe (80,2%) are the regions where most people have internet access – phone or home-based –, followed by Oceania (69,6%) and South America (65,3%) (Leaning 2016).

2 Chile and Brazil are currently among the South American countries with the least number of woman representatives in federal legislative bodies. Also, they rank the lowest among South Americans who have had women – in the case of Chile, particularly different women – in the Presidency, as Ministers of Defense and of Foreign Affairs.

3 This has been established by contrasting whether and how each category (Career, Health, I&S, P&P, Violence) deviates from dichotomous relationships between male and female stereotypes. The conclusion is also compatible with their rank among the South American countries with the least women having occupied the top positions in the Presidency, the Ministry of Defense, and the Ministry of Foreign Affairs.

4 This conclusion comes from a comparison with the Western European sample, where gender issues are particularly associated to international organizations, and to the United States, as well as the world-wide sample, where the category P&P is strongly related to the State only where the production of statistics and indexes is concerned – even the category Health tips off toward private concerns.

References:

Acharya, Amitav. 2004. How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism. International Organization, Vol. 58, No. 2 (Spring), pp. 239 – 275.

Archivo Digital de UNASUR 2019. Available at: https://intranet.unasursg.org/

Atlas Comparativo de la Defensa 2016. Available at: https://www.resdal.org/atlas-2016.html

Google Trends 2019. Available at: https://trends.google.com/trends/

Kalil, Mariana. 2015. Teoria Não Ocidental & Política Externa Brasileira: provocações de uma análise comparada das motivações para a posição coincidente brasileiro-argentina em torno da criação do Conselho Sul-Americano de Defesa. Revista da Escola de Guerra Naval, Vol. 21, No. 1, pp. 197 – 222.

Leaning, Marcus. 2016. Internet Continental Comparison. Available at: https://en.unesco.org/sites/default/files/milweek17_marcus_leaning.pdf

Manual para la incorporación de la perspectiva de género en la programación común a escala nacional. 2018. New York: United Nations Sustainable Development Group.

UN Handbook. 2002. Gender Mainstreaming: An Overview. New York: Office of the Special Adviser on Gender Issues.

1 De acordo com a UNESCO, América do Norte (81%) e Europa (80,2%) são as regiões onde a maioria da população tem acesso à internet – no telephone cellular ou em casa – seguidas por Oceania (69,6%) e América do Sul (65,3%) (Leaning 2016).

2 Chile e Brasil estão entre os países sul-americanos com o menor número de mulheres no Legislativo federal. Eles também ocupam as mais baixas classificações entre os sul-americanos que já tiveram mulheres na presidência, no ministério da defesa e no ministério das relações exteriores – no caso particular do Chile, mulheres diferentes.

3 Isso foi estabelecido contrastando ´se´ e ´como´ cada categoria (Carreira, Saúde, I&S, P&P, Violência) se desvia das relações dicotômicas entre estereótipos masculinos e femininos. A conclusão também é compatível com sua posição entre os países da América do Sul com o menor número de mulheres ocupando os cargos mais altos na Presidência, no Ministério da Defesa e no Ministério das Relações Exteriores.

4 Esta conclusão vem de uma comparação com a amostra da Europa Ocidental, onde as questões de gênero estão particularmente associadas a organizações internacionais, e aos Estados Unidos, bem como à amostra mundial, onde a categoria P&P está fortemente relacionada ao Estado, mas somente no que se refere à produção de estatísticas e índices - até mesmo a categoria Saúde aponta para preocupações privadas.

Referências

Acharya, Amitav. 2004. How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism. International Organization, Vol. 58, No. 2 (Spring), pp. 239 – 275.

Archivo Digital de UNASUR 2019. Available at: https://intranet.unasursg.org/

Atlas Comparativo de la Defensa 2016. Available at: https://www.resdal.org/atlas-2016.html

Google Trends 2019. Available at: https://trends.google.com/trends/

Kalil, Mariana. 2015. Teoria Não Ocidental & Política Externa Brasileira: provocações de uma análise comparada das motivações para a posição coincidente brasileiro-argentina em torno da criação do Conselho Sul-Americano de Defesa. Revista da Escola de Guerra Naval, Vol. 21, No. 1, pp. 197 – 222.

Leaning, Marcus. 2016. Internet Continental Comparison. Available at: https://en.unesco.org/sites/default/files/milweek17_marcus_leaning.pdf

Manual para la incorporación de la perspectiva de género en la programación común a escala nacional. 2018. New York: United Nations Sustainable Development Group.

UN Handbook. 2002. Gender Mainstreaming: An Overview. New York: Office of the Special Adviser on Gender Issues.

XVIFORTE

6/6

KONRAD ADENAUER STIFTUNG

O Fator Gênero na Segurança Internacional A Perspectiva Europeia

The Gender Factor in International Security A European Perspective

Irene Giner-Reichl

CEBRI
BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS

COLEÇÃO DE POLICY PAPERS
THE POLICY PAPERS COLLECTION

XVIFORTE

A Conferência de Segurança Internacional do Forte de Copacabana é um projeto euro-brasileiro organizado em conjunto pela Fundação Konrad Adenauer (KAS) e pelo Centro Brasileiro de Relações Internacionais (CEBRI), com apoio da Delegação da União Europeia no Brasil. A conferência é concebida como um fórum de diálogo entre a América do Sul e a Europa. Seu objetivo é reunir especialistas do setor governamental, acadêmico e privado para discutir assuntos atuais no âmbito de segurança que sejam de interesse comum aos parceiros dos dois lados do Atlântico. Desde seu início em 2003, a conferência se transformou, de uma reunião relativamente pequena, no maior fórum de segurança da América Latina. Na sua 16ª edição, a conferência de 2019 tem como tema 'A Quarta Revolução Industrial: Impactos na Segurança Internacional e a Reformulação da Ordem Global'. A conferência é aberta ao público e os participantes são incentivados a participar ativamente das discussões. Esta coleção de Policy Papers reflete os temas centrais do evento e pretende identificar desafios, bem como fazer recomendações políticas para o futuro. As edições anteriores da publicação sobre Segurança Internacional da Conferência do Forte de Copacabana podem ser acessadas na página oficial da KAS Brasil (www.kas.de/brazil).

The Forte de Copacabana International Security Conference is a joint Euro-Brazilian project organised by the Konrad Adenauer Foundation (KAS) in partnership with the Brazilian Center for International Relations (CEBRI) and supported by the Delegation of the European Union to Brazil. The conference is conceived as a forum for dialogue between South America and Europe. It aims to bring together experts from a wide range of government, academic and private-sector backgrounds to discuss current security-related issues which are of interest to the partners on both sides of the Atlantic. Since its inception in 2003, the conference has emerged from a relatively small gathering to Latin America's largest security forum to date. The topic of the 16th edition of the conference is 'The Fourth Industrial Revolution: Impacts on International Security and the Reshaping of Global Order'. The conference is open to the public and the audience is encouraged to actively engage in discussions. This collection of Policy Papers reflects the major themes of the event and intends to identify challenges as well as make policy recommendations for the future. Previous volumes of the Forte de Copacabana International Security Conference publication can be accessed on the KAS-Brazil Office website (www.kas.de/brazil).

www.kas.de/brasil

Editor Editor
Anja Czymmeck

Coordenação editorial Project Coordination
Ariane Costa
Reinaldo Themoteo

Colaboração Editorial Support
Monique Sochaczewski

Tradução e revisão Translation and Revision
Leslie Sasson Cohen

Projeto Gráfico Design
Charles Steiman
Daniela Knorr

Impressão Print
Stamppa

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

COLEÇÃO DE POLICY PAPERS
THE POLICY PAPERS COLLECTION

1/6
Cibersegurança na América Latina
Cybersecurity in Latin America
Monica Herz

2/6
A quarta revolução industrial: Impactos na Segurança Internacional e a Reestruturação da Ordem Mundial - A perspectiva europeia
The Fourth Industrial Revolution: Impacts on International Security and the Reshaping of Global Order – The European Perspective
Kai Michael Kenkel

3/6
Inteligência artificial (IA) no balanço de poder na política internacional: uma perspectiva sul-americana
Artificial intelligence (AI) in the balance of power in world politics: a South American perspective
Jorge H. C. Fernandes

4/6
A Cibersegurança em um mundo conectado
Cybersecurity in a connected word
Pedro Veiga

5/6
Incorporação de gênero na segurança internacional da América do Sul: Big Data, Regionalismo e Difusão de Normas
Gender Mainstreaming in South America's International Security: Big Data, Regionalism and Norm Diffusion
Mariana Kalil

6/6
O Fator Gênero na Segurança Internacional
A Perspectiva Europeia
The Gender Factor in International Security
A European Perspective
Irene Giner-Reichl

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.

A Delegação da União Europeia (UE) no Brasil é uma das mais de 130 Delegações da UE no mundo. A Delegação da UE no Brasil está focada na promoção das relações políticas e econômicas entre a UE e o Brasil, de acordo com a parceria estratégica EU–Brasil estabelecida em 2007. A UE e o Brasil estabeleceram relações diplomáticas em 1960, criando estreitos laços históricos, culturais, econômicos e políticos. Dentre os tópicos centrais da parceria estratégica entre a UE e o Brasil 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. Mais de 30 diálogos formais no setor político foram iniciados entre a União Europeia e autoridades brasileiras para enfrentar esses desafios. Além disso, a União Europeia e o Brasil são parceiros comerciais importantes e os países da União Europeia recebem mais de 20% da exportação brasileira. A União Europeia também é o maior investidor estrangeiro no Brasil com cerca de 60% do investimento estrangeiro.

The European Union (EU) Delegation to Brazil is one of over 130 EU Delegations around the world. The EU Delegation to Brazil is focused on promoting political and economic relations between the EU and Brazil, in line with the EU–Brazil Strategic Partnership established in 2007. The EU and Brazil established diplomatic relations already in 1960 building on close historical, cultural, economic and political ties. Central topics of the EU–Brazil Strategic Partnership 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. Over 30 formal sector-policy dialogues between the European Union and Brazilian authorities have been initiated to address these challenges. The European Union and Brazil are also important trading partners and the countries of the European Union account for over 20% of Brazil's exports. The European Union is also the largest foreign investor in Brazil with around 60% of the foreign investment originating from the European Union.

CEBRI
BRAZILIAN CENTER FOR
INTERNATIONAL RELATIONS

Independente, apartidário e multidisciplinar, o Centro Brasileiro de Relações Internacionais (CEBRI) é uma instituição sem fins lucrativos, que atua para influenciar positivamente a construção da agenda internacional do país. Fundado há 20 anos por um grupo de empresários, diplomatas e acadêmicos, o CEBRI tem ampla capacidade de articulação, engajando os setores público e privado, a academia e a sociedade civil. Além disso, conta com um Conselho Curador atuante e formado por figuras proeminentes, e com uma rede de mantenedores constituída por instituições, empresas e indivíduos de múltiplos segmentos.

O CEBRI promove a expansão e aprofundamento do debate sobre a política externa brasileira e a inserção do Brasil no mundo, pautado na formulação de políticas públicas e no fomento de diálogo entre os mais relevantes atores brasileiros e globais. O reconhecimento de sua importância internacional é atestado pelo ranking do Programa de Think Tanks e Sociedade Civil da Universidade da Pensilvânia, que destacou o CEBRI como o segundo melhor think tank do Brasil e o quarto melhor da América Latina.

Independent, nonpartisan and multidisciplinary, the Brazilian Center for International Relations (CEBRI) is a non-profit institution that acts to have a positive influence on the construction of the country's international agenda. Founded 20 years ago by a group of business leaders, diplomats and academics, CEBRI has the ability to engage the public and private sectors, academia and civil society. In addition, it counts on an engaged Board of Trustees formed by prominent figures and on a diverse network of sponsors made up of institutions, companies and individuals from multiple sectors.

CEBRI promotes the expansion and deepening of debates on Brazilian foreign policy and Brazil's international insertion, marked by the formulation of public policies and the promotion of dialogue amongst the most relevant Brazilian and global stakeholders. The recognition of its international importance is evidenced by the University of Pennsylvania's Think Tanks and Civil Societies Program, which ranked CEBRI as Brazil's second best think tank and the fourth best in Latin America.

Irene Giner-Reichl
Irene Giner-Reichl pertence ao Serviço Diplomático Austríaco desde 1982. Sobretudo, ela trabalhou nas áreas de Desenvolvimento Econômico e Social, Meio Ambiente, Energia e Cooperação para o Desenvolvimento. Desde julho de 2017, é Embaixadora da Áustria no Brasil e no Suriname, com sede em Brasília. Dra. Irene Giner-Reichl é presidente do Global Forum on Sustainable Energy (GFSE) que foi fundado em 1999. É uma plataforma público-privada para o diálogo sobre energia a serviço do desenvolvimento sustentável (vide também www.gfse.at). Ela também é co-fundadora da GWNET (Global Women's Network for the Energy Transition, www.globalwomennet.org), uma rede para promover a participação igualitária das mulheres no setor de energia. Desde 2013, é vice-presidente do Renewable Energy Policy Network REN21 (www.ren21.org). Ela é autora de vários artigos sobre questões globais em publicações acadêmicas e de assuntos gerais, austríacas e internacionais, e ensina, há muitos anos, na Academia Diplomática em Viena sobre questões de Segurança Humana e Política de Desenvolvimento.

Irene Giner-Reichl has been with the Austrian Diplomatic Service since 1982. She has worked in the areas of Economic and Social Development, Environment, Energy and Development Cooperation. Since July 2017, she is the Austrian Ambassador to Brazil and Suriname, based in Brasilia. Dr. Irene Giner-Reichl is chair of the Global Sustainable Energy Forum (GFSE), which was founded in 1999. It is a public-private platform for dialogue on energy and sustainable development services (see also www.gfse.at). She is also co-founder of GWNET (Global Women's Network for the Energy Transition, www.globalwomennet.org), a network that aims to promote women's equal participation in the energy sector. Since 2013, she has been vice president of the REN21 Renewable Energy Policy Network (www.ren21.org). She has authored several articles on global issues in Austrian and international academic and general affairs publications and has taught for many years at the Diplomatic Academy in Vienna on issues of Human Security and Development Policy.

O Fator Gênero na Segurança Internacional A Perspectiva Europeia

The Gender Factor in International Security A European Perspective

Irene Giner-Reichl

Embaixadora da Áustria no Brasil*

*Austrian Ambassador to Brazil**

"O gênero é importante quando se trata de quem morre, quem está ferido e como está ferido, quem vive, quem é afetado e de que maneira é afetado, e como é sua vida e sua subsistência durante a crise e depois dela".

(Proctor and Mazurana, 2017)[1]

Gender matters when it comes to who dies, who is injured and how, who lives, who is affected and in what ways, and what their lives and livelihoods are like during and after crisis"

(Proctor and Mazurana, 2017)[1].

Introdução

As questões de gênero têm ganhado importância uma vez que as discussões sobre segurança nacional e internacional ocorrem cada vez mais sob o âmbito de conceitos abrangentes de segurança - como a abordagem adotada pelo Painel de Alto Nível sobre Ameaças e Desafios da ONU (2004) ou o conceito de segurança humana. A urgência dessa consideração foi impulsionada, entre outras coisas, pela atribuição do Prêmio Nobel da Paz em 2018 a Denis Mukwege e Nadia Murad[2] por suas respectivas lutas no combate à violência contra as mulheres.

A violência contra as mulheres é a manifestação mais dura da discriminação contra as mulheres. A discriminação em todas as suas formas constitui uma violação dos direitos humanos das mulheres e, muitas vezes, prepara o terreno - baixando o limiar e construindo aceitação nas sociedades afetadas - para a agressão violenta contra as mulheres.

Introduction

As international and national security discussions are increasingly taking place against the backdrop of comprehensive security concepts – such as the approach taken by the UN's High-Level Panel on Threats and Challenges (2004) or the human security concept - gender issues increase in importance. The urgency of this consideration was driven home inter alia by the award of the Nobel Peace Prize in 2018 to Denis Mukwege and Nadia Murad[2] for their respective fights against violence against women.

Violence against women is the starkest manifestation of discrimination against women. Discrimination in all its forms constitutes a violation of the human rights of women and often prepares the ground – by lowering the threshold and building acceptance in affected societies - for violent aggression of women.

At the same time, the realization grows that internal and external security are ever more intertwined: "Our security at home entails a parallel interest in peace in our neighbouring and surrounding regions. It implies a broader interest in preventing conflict, promoting human security, addressing the root causes of instability and working towards a safer world", the EU's Global Strategy (June 2016)[3] states.

This paper will briefly recall some key points in the international discussion of and action on the issue (Part I) and sketch where European countries – the EU as well as some individual countries - stand in their reflection and action, taking as point of departure the ground-breaking UN SC Res. 1325 of the year 2000 (Part II). It will also scratch the surface of examining the relevance of gender approaches with regard to some of the more acute present-day threats, including those that are directly linked to the technological changes evoked by slogans such as Industry 4.0 or big data (Part III).

Part I. How we got to where we are today

In this part of the paper I seek to (a) anchor our discussions in a human rights perspective, (b) show-case how the gender dimension has been incorporated into decisions of the Security Council, (c) recall how the concept of security has broadened to include economic, social, environmental and other dimensions; and (d) give a few examples from the literature of recognition given to the key role of equality of women and men with a view to producing desired outcomes in the mutually re-enforcing domains of peace and security and of development.

a) The Vienna World Conference on Human Rights in 1993, with more than 7000 participants, including many human rights activists, one of the major UN conferences of the 1990s, adopted the Vienna Declaration and Action Program and led to the creation of the Office of the UN High Commissioner for Human Rights (UNHCHR). To this day the UNHCHR is one of the most important and visible pillars of the international community's safeguards for the respect of universal human rights and fundamental freedoms. Para. 18 of the Vienna Declaration states[4]:

18. The human rights of women and of the girl-child are an inalienable, integral and indivisible part of universal human rights. The full and equal participation of women in political, civil, economic, social and cultural life, at the national, regional and international levels, and the eradication of all forms of discrimination on grounds of sex are priority objectives of the international community.

The Beijing Declaration and Platform for Action[5], adopted at the Fourth International Women's Conference in Beijing 1995, lists among its 12 critical areas of concern "Violence against Women" and "Women and Conflict".

b) Five years later, in 2000 the UN Security Council adopted the groundbreaking resolution 1325[6] which owes a lot to the initiative of an enlightened man, the Bangladeshi Diplomat Anwarul Chowdhury. The resolution has two main objectives: protection and participation; that is to protect women and girls from violence and to enable them to participate fully in decision-making at all levels. The resolution is grounded in the understanding that peace building /society building will only be successful if the concerns of the entire population are met and if the resources of the entire population can be drawn upon.

During Austria's membership in the Security Council 24 indicators were adopted in 2009 to allow for better monitoring of the implementation of SC Res. 1325. Other important SC Council resolutions are SC Res. 2242(2015) which inter alia created an Informal Group of Experts on Women, Peace and Security which has done work on the country situations of Mali, Iraq, Central African Republic, Afghanistan and Yemen.

The SC Council Resolutions had important reverberations in other fora; here are a few examples:

- **OSCE** is nowadays giving greater weight to including women in their field missions;
- **NATO**, upon the instigation of Austria, Finland, Sweden and Norway, created the post of the NATO Secretary General's Special Representative for Women, Peace and Security (currently Clare Hutchinson). The content of SC Res. 1325 is routinely incorporated into policy, operations, training and military exercises.

Ao mesmo tempo, cresce a percepção de que a segurança interna e externa estão cada vez mais interligadas: "Nossa segurança em casa implica um interesse paralelo pela paz em nossos vizinhos e regiões vizinhas. Implica um interesse mais amplo em prevenir conflitos, promover a segurança humana, atacar as causas profundas da instabilidade e trabalhar em prol de um mundo mais seguro ", afirma a Estratégia Global da UE (junho de 2016)[3].

Este artigo irá recapitular brevemente alguns pontos-chave na discussão e na ação internacional sobre a questão (Parte I) e esboçar sobre a situação dos países europeus - a UE e alguns países individuais - em sua reflexão e ação, tomando como ponto de partida, a inovadora Resolução 1325 do Conselho de Segurança das Nações Unidas, do ano 2000 (Parte II). O artigo irá também examinar superficialmente a relevância das abordagens de gênero em relação a algumas das ameaças atuais mais agudas, incluindo aquelas que estão diretamente ligadas às mudanças tecnológicas evocadas por slogans como Indústria 4.0 ou Big Data (Parte III).

Parte I. Como chegamos onde estamos hoje

Nesta parte do artigo, eu busco (a) ancorar nossas discussões em uma **perspectiva dos direitos humanos**, (b) mostrar como a dimensão de gênero foi incorporada nas **decisões do Conselho de Segurança**, (c) lembrar como o **conceito de segurança foi ampliado** para incluir as dimensões econômica, social, ambiental e outras; e (d) dar alguns exemplos, encontrados na literatura, do reconhecimento dado ao papel chave da igualdade entre mulheres e homens, com vistas a produzir os resultados desejados nos domínios de paz e segurança e de desenvolvimento que se reforçam mutuamente.

a) A **Conferência Mundial de Viena sobre Direitos Humanos**, em 1993, com mais de 7.000 participantes, incluindo muitos ativistas de direitos humanos, reconhecida como uma das principais conferências da ONU dos anos 1990, adotou a Declaração e o Programa de Ação de Viena e levou à criação do Escritório do Alto Comissariado das Nações Unidas para os Direitos Humanos (ACNUDH). Até hoje, o ACNUDH é um dos pilares mais importantes e visíveis das salvaguardas da comunidade internacional para o respeito aos direitos humanos universais e liberdades fundamentais. Par. 18 da Declaração de Viena declara[4]:

> 18. Os direitos humanos das mulheres e das meninas são parte inalienável, integral e indivisível dos direitos humanos universais. A participação plena e igualitária das mulheres na vida política, civil, econômica, social e cultural, a nível nacional, regional e internacional, e a erradicação de todas as formas de discriminação em razão de sexo são objetivos prioritários da comunidade internacional.

A **Declaração e Plataforma de Ação de Pequim**[5], adotada na Quarta Conferência Mundial sobre a Mulher, em Pequim, em 1995, estabelece entre suas 12 áreas críticas de preocupação, "Violência contra as Mulheres" e "Mulheres em Conflito".

b) Cinco anos depois, em 2000, o Conselho de Segurança da ONU adotou a arrojada resolução **1325**[6], que deve muito à iniciativa de um homem esclarecido, o Diplomata de Bangladesh Anwarul Chowdhury. A resolução tem dois objetivos principais: proteção e participação, isto é, proteger as mulheres e meninas da violência e permitir-lhes participar plenamente na tomada de decisões em todos os níveis. A resolução baseia-se no entendimento de que a construção da paz / construção da sociedade só será bem sucedida se as preocupações de toda a população forem satisfeitas e se os recursos de toda a população puderem ser utilizados.

Durante a adesão da Áustria ao Conselho de Segurança, **24 indicadores** foram adotados em 2009 para permitir um melhor monitoramento da implementação da Resolução 1325 do Conselho de Segurança da ONU. Outras resoluções importantes do Conselho de Segurança são SC Res. 2242 (2015) que, entre outras coisas, criou um Grupo Informal de Especialistas sobre Mulheres, Paz e Segurança, que realizou trabalhos sobre a situação de países como Mali, Iraque, República Centro-Africana, Afeganistão e Iêmen.

As Resoluções do Conselho de Segurança tiveram importante repercussão em outros fóruns. Seguem alguns exemplos:

- **OSCE** (Organização para segurança e cooperação na Europa) está, atualmente, dando mais importância à inclusão de mulheres em suas missões a campo;

- **OTAN,** após provocação da Áustria, Finlândia, Suécia e Noruega, criou o cargo de Representante Especial do Secretário Geral

- Gender balance among the UN Secretary General's Special Representatives – in 2007 none of the 54 UN SG-SRs were women – has in the meantime improved significantly, even though there is still need for more women.

c) 2005 Panel on Threats and Challenges
In his speech to the General Assembly in September 2003, UN Secretary General Kofi Annan drew attention to deep divisions among the Member States on the nature of the threats faced by humanity and the appropriateness of the use of force to address these threats. He asked an international High-Level Panel, chaired by former Prime Minister of Thailand Anand Panyarachun and representing a wide range of experience and expertise, to assess current threats to international peace and security; to evaluate how existing policies and institutions have done in addressing those threats; and to make recommendations for strengthening the UN as a provider for collective security for all.

In his letter to the General Assembly forwarding the recommendations of the Panel[7], the Secretary General endorsed the Panel's core arguments for a "broader, more comprehensive concept of collective security", a concept which sees the interconnectedness of contemporary threats to our security: "We cannot treat issues such as terrorism or civil wars or extreme poverty in isolation". The Panel urged for more emphasis on prevention, and for an improvement of the international communities' toolkit regarding sanctions and mediation. As a result of the Report, at the UN Summit in 2005 the Peacebuilding Commission was created and the Human Rights Council replaced the somewhat discredited Human Rights Commission.

These are the challenges that the Panel discussed in particular: poverty, infectious disease and environmental degradation; conflict between and within States; nuclear, radiological, chemical and biological weapons; terrorism; transnational organized crime.

Were the Panel to submit a list of threats today, it would probably have added non-properly- managed migration, cyber-crime and extremism.

The Outcome Document of the World Summit also contains a paragraph devoted to the concept of Human Security[8] and a commitment to further explore this concept. A formal debate led by the President of the General Assembly was held in June 2012 and a resolution adopted on 25 October 2012[9].

d) Once the economic, social and environmental dimensions of security are explicitly acknowledged, the gender dimension of preventive and remedial action becomes even more obvious. A broad range of institutions, including the World Bank and the World Economic Forum – not usually suspected of feminism –, have drawn attention to the important role of gender equality in promoting economic development. The World Development Report 2012[10] states squarely that "Gender equality matters for development" and that "it is smart economics" because

- fuller access of women to training and employment outside the home improves the productivity of an economy;

- improved status of women produces desirable development outcomes in other fields (such in the areas of health and education);

- leveling the playing field to women's social and political participation is likely to lead to more inclusive institutions and hence to better policy choices.

The World Economic Forum of Davos produces a yearly "Gender Gap Report"[11] which ranks countries accordingly. This is the rationale: " Gender parity is fundamental to whether and how economies and societies thrive. Ensuring the full development and appropriate deployment of half of the world's total talent pool has a vast bearing on the growth, competitiveness and future-readiness of economies and businesses worldwide. The Global Gender Gap Report benchmarks 149 countries on their progress towards gender parity across four thematic dimensions: Economic Participation and Opportunity, Educational Attainment, Health and Survival, and Political Empowerment." The 2018 edition took a particular close look at skills gender gaps related to artificial intelligence, a topic of special relevance to this year's Forte de Copacabana Forum focus.

The Arab Human Development Report 2005[12] deplores that "at a time when the Arab world needs to build and tap the capabilities of all its peoples fully, half of its human potential is often stifled or neglected" and argues that

da OTAN para Mulheres, Paz e Segurança (atualmente ocupado por Clare Hutchinson). O conteúdo da Resolução 1325 é incorporado rotineiramente em políticas, operações, treinamento e exercícios militares.

- Equilíbrio de gênero entre os **Representantes Especiais do Secretário Geral da ONU** - em 2007, nenhum dos 54 RE-SG da ONU eram mulheres – entretanto isso melhorou significativamente desde então, embora ainda haja necessidade de mais mulheres.

c) Painel de 2005 sobre Ameaças e Desafios
Em seu discurso à Assembleia Geral em setembro de 2003, o secretário-geral da ONU, Kofi Annan, chamou a atenção para as profundas divisões entre os Estados membros sobre a natureza das ameaças enfrentadas pela humanidade e a conveniência do uso da força para lidar com elas. Ele pediu a um Painel Internacional de Alto Nível, presidido pelo ex-Primeiro Ministro da Tailândia Anand Panyarachun, representando uma ampla gama de experiências e conhecimentos, para avaliar as ameaças atuais à paz e à segurança internacionais; avaliar os resultados das políticas e instituições existentes ao lidar com essas ameaças; e fazer recomendações para fortalecer a ONU como provedor de segurança coletiva para todos.

Em sua carta à Assembleia Geral encaminhando as recomendações do Painel[7], o Secretário-Geral endossou os principais argumentos para um "conceito mais amplo e abrangente de segurança coletiva", que considere a interconectividade das ameaças contemporâneas à nossa segurança: "Nós não podemos tratar questões como terrorismo ou guerras civis ou pobreza extrema isoladamente ". O Painel pediu mais ênfase na prevenção e na melhoria dos instrumentos das comunidades internacionais com relação a sanções e mediação. Como resultado do Relatório, na Cúpula das Nações Unidas de 2005, foi criada a **Comissão de Consolidação da Paz** e a desacreditada Comissão de Direitos Humanos foi substituída pelo **Conselho de Direitos Humanos**.

Estes são os **desafios** que o Painel discutiu com profundidade: pobreza, doenças infecciosas e degradação ambiental; conflito entre Estados e dentro dos Estados; armas nucleares, radiológicas, químicas e biológicas; terrorismo; crime organizado transnacional.

Se o Painel enviasse uma lista de ameaças hoje, provavelmente acrescentaria migração sem gestão adequada, crime cibernético e extremismo.

O Documento Final da Cúpula Mundial também contém um parágrafo dedicado ao conceito de **Segurança Humana**[8] e o compromisso de explorar ainda mais esse conceito. Um debate formal conduzido pelo Presidente da Assembleia Geral foi realizado em junho de 2012 e uma **resolução** foi adotada em 25 de outubro de 2012[9].

d) Uma vez que as dimensões econômica, social e ambiental da segurança são explicitamente reconhecidas, a dimensão de gênero das ações preventivas e corretivas torna-se ainda mais óbvia. Uma ampla gama de instituições, incluindo o Banco Mundial e o Fórum Econômico Mundial - geralmente não suspeitos de feminismo - chamaram a atenção para o importante papel da igualdade de gênero na promoção do desenvolvimento econômico. O **Relatório sobre o Desenvolvimento Mundial de 2012**[10] afirma de maneira clara que "a igualdade de gênero é importante para o desenvolvimento" e que "é uma economia inteligente" porque

- O acesso mais pleno das mulheres à formação e ao emprego fora de casa melhora a produtividade da economia;

- A melhoria da situação das mulheres produz resultados desejáveis em outros setores (como nas áreas de saúde e educação);

- Estabelecer condições igualitárias para a participação social e política das mulheres pode levar a instituições mais inclusivas e, consequentemente, a melhores escolhas políticas.

O **Fórum Econômico Mundial de Davos** produz anualmente o relatório "**Gender Gap Report**"[11] (relatório sobre a paridade de gênero), que classifica os países de acordo com o grau de desigualdade de gênero. O raciocínio por trás disso é: "A paridade entre os gêneros é fundamental como condição para as economias e as sociedades prosperarem e para a maneira como o farão. Garantir o pleno desenvolvimento e a utilização apropriada de metade dos talentos do mundo tem uma grande influência no crescimento, na competitividade e no preparo para o futuro das economias e das empresas em todo o mundo. O Global Gender Gap Report faz uma avaliação de 149 países sobre seu progresso em relação à igualdade de gênero em quatro dimensões temáticas: participação econômica e oportunidade, realização educacional, saúde e sobrevivência e empoderamento político. "A edição de 2018 examinou de perto as lacunas de gênero relacionadas à inteligência artificial, um

the rise of women is in fact a prerequisite for an Arab renaissance, inseparably and causally linked to the fate of the Arab world and its achievement of human development".

Part II. The EU's approach to Gender and Security

This part of the paper will give a short summary of the content of currently relevant EU policy documents. It will also provide a few examples of relevant EU member States engagement in the area of WPS.

The EU's commitment to gender equality in its internal and external policies is of long standing. At the Beijing World Conference in 1995, the EU successfully promoted the concept of "mainstreaming" a gender perspective into all policies, programs and projects which opened the door for bringing the topic out of secluded discussions in dedicated "Women's issues fora" and obliged all decision-makers to take cognizance – if nothing else - of the issues at hand.

In June 2016 the EU adopted, for the first time, a comprehensive Global Strategy for its engagement with the world in foreign and security policy: "Shared Vision: Common Action. A Stronger Europe". In this strategy, the EU commits, under the heading of "Conflict settlement" inter alia to fostering inclusive governance at all levels. It pledges to develop more creative approaches to diplomacy. "This also means", the Strategy states, "promoting the role of women in peace efforts – from implementing the UNSC Resolution on Women, Peace and Security to improving the EU's international gender balance".[13]

In 2016 as well, with the appointment of Ambassador Mara Marinaki as EEAS Advisor for gender and for the implementation of SC Res. 1325 (Principal Gender Adviser), the EEAS (External Action Service of the EU) gave visible expression to the importance of equality between women and men and of the Women Peace Security (WPS) Agenda as a cross-cutting issue in all EU institutions and in all policies of EU member States.

There are currently four workstreams:

- mainstreaming of Gender/WPS topics within the EEAS at all levels (Headquarter, EU delegations, CSDP missions and operations);
- promoting relevant EU engagement with third parties (equality between women and men, (primarily) economic empowerment of women; prevention of violence against women, including sexual violence in conflicts; participation of women on an equal footing with men in conflict prevention and in peace processes; role of women in combatting terrorism and extremism;
- conscience raising within EU delegations and EU member States regarding the implementation of strategic documents, in particular the Gender Action Plan II (2016 – 2020) and the Strategic Document on Gender Equality 2016-2019;
- improved implementation of the SC Res. 1325 on Women, Peace and Securite, including in civilian and military crisis deployments and through the promotion of national action plans in follow-up of SC Res. 1325.

Under the Austrian presidency of the Council, the EU replaced an older version from 2008 through the "Strategic Approach to Women, Peace and Security" which is annexed to the Council Conclusions adopted on 10 December 2018[14].

An EU Action Plan is oriented along the six objectives of the EU Strategy and contains measures to be completed short-term (by the end of the year) , mid-term (synchronized with the remaining duration of the general Gender Action Plan, 2019-2020) and long-term (for the duration of the Commission's mandate 2019-2024).

The six objectives are:

Participation:

- higher percentage of women within EU-institutions and within EU member States' institutions;
- Active promotion of the participation of women in all political decision making processes, including conflict prevention, conflict solution, mediation, post-conflict recovery and consolidation of peace;

Gender Mainstreaming

- Incorporating a gender perspective as an integrative component of all policy areas

tópico de especial relevância para o foco do Fórum do Forte de Copacabana deste ano.

O **Relatório do Desenvolvimento Humano Árabe 2005**[12] lamenta que "em um momento em que o mundo árabe precisa construir e explorar as capacidades de todos os seus povos, metade do seu potencial humano é muitas vezes sufocado ou negligenciado" e argumenta que a ascensão das mulheres é de fato pré-requisito para um renascimento árabe, inseparável e causalmente ligado ao destino do mundo árabe e à sua conquista do desenvolvimento humano ".

Part II. A abordagem da UE em matéria de Gênero e Segurança

Esta parte do documento apresentará um breve resumo do conteúdo dos documentos de política da UE atualmente relevantes. Fornecerá também alguns exemplos de envolvimento relevante dos Estados membros da UE no tópico Mulheres, Paz e Segurança (WPS – Women, Peace and Security, em inglês).

O compromisso da UE com a igualdade de gênero nas suas políticas interna e externa não é algo recente. Na Conferência Mundial de Beijing em 1995, a UE promoveu com sucesso o conceito de "***mainstreaming***" ou **incorporação** de uma perspectiva de gênero em todas as políticas, programas e projetos, o que abriu caminho para desenterrar o tópico de discussões isoladas em "fóruns de questões femininas" e obrigou todos os tomadores de decisão a tomar conhecimento – ao menos isso - dos problemas em questão.

Em junho de 2016, a UE adotou, pela primeira vez, uma **estratégia global** abrangente para o seu envolvimento mundial em matéria de política externa e segurança: "**Visão compartilhada: Ação Comum. Uma Europa Mais Forte**". Nesta estratégia, a UE compromete-se, sob o item "Resolução de Conflitos", a promover a governança inclusiva em todos os níveis. Compromete-se, também, a desenvolver abordagens mais criativas para a diplomacia. "Isto também significa", afirma a Estratégia, "promover o papel das mulheres nos esforços de paz - desde a implementação da Resolução do Conselho de Segurança das Nações Unidas sobre Mulheres, Paz e Segurança até a melhoria da paridade de gênero europeia"[13].

Também em 2016, com a nomeação da Embaixadora Mara Marinaki como Conselheira do SEAE para questões de gênero e para a implementação da Resolução do Conselho de Segurança 1325 (**conselheiro principal para questões de gênero**), o SEAE (Serviço de Ação Externa da UE) deu visibilidade à importância da igualdade entre mulheres e homens e da Agenda para Mulheres, Paz e Segurança (WPS) como questão transversal em todas as instituições da UE e em todas as políticas dos Estados membros da UE.

Atualmente, existem quatro **fluxos de trabalho**:

- Incorporação dos temas de gênero/WPS no SEAE em todos os níveis (sede, delegações UE, missões e operações da PCSD);

- Promoção do envolvimento da UE com terceiros (igualdade entre mulheres e homens, (em primeiro lugar) empoderamento econômico das mulheres; prevenção da violência contra as mulheres, incluindo a violência sexual em conflitos; participação das mulheres em igualdade de condições com relação aos homens nos processos de paz e de prevenção de conflitos; o papel das mulheres no combate ao terrorismo e ao extremismo;

- Conscientização nas delegações da UE e nos Estados membros com relação à implementação de documentos estratégicos, em particular, o Plano de Ação para as Questões de Gênero II (2016-2020) e do Documento Estratégico sobre Igualdade de Gênero (2016-2019);

- Melhoria na implementação da Resolução 1325 do Conselho de Segurança sobre Mulheres, Paz e Segurança, incluindo a mobilização em casos de crise civil e militar e pela promoção de planos de ação nacionais em seguimento à Resolução 1325.

Sob a presidência austríaca do Conselho, a UE substituiu uma versão mais antiga de 2008 através da "Abordagem Estratégica para as Mulheres, Paz e Segurança", que está anexada às Conclusões do Conselho adotadas em 10 de dezembro de 2018[14].

Um plano de ação da UE orienta-se pelos seis objectivos da estratégia da UE e contém medidas a concluir a curto prazo (até ao final do ano) a médio prazo (sincronizadas com a restante duração do plano geral de acção sobre o género, 2019- 2020) ea longo prazo (durante o mandato da Comissão 2019-2024).

Leading by example
- Stronger political EU engagement and more effective EU measures to implement the WPS-Agenda at local, national, regional and international levels;

Prevention
- EU early warning systems and measures need to be gender-responsive;

- Stronger role of the EU in preventing, monitoring and reporting on human rights violations inflicted on women and girls in conflict situations;

- Implementation of the "zero tolerance policy" and accountability/ending of impunity for perpetrators;

Protection
- EU engagement for the rights of women and girls at local, national, regional and international levels;

- Promoting the creation/activation of institutional mechanisms for the protection of women and girls – as well as men and boys – in fragile contexts/situations of conflict, in order to contribute to the prevention and elimination of all forms of sexual and gender-specific violence;

Relief and Recovery[15]
- Making available of adequate aid to facilitate relief and recovery for women and girls particularly affected by situations of ongoing or past conflict:

Let us also take a glance on some individual EU member States commitments and actions:

Austria
Since 2007 Austria has worked consistently to bring the recommendations of SC Res. 1325 on the ground, through national action plans which focus on Austrian military and civilian staff participation in peace missions, in the context of multilateral and bilateral relations, development cooperation and humanitarian aid.

Through its **development cooperation** – 15 % of its bilateral aid is pledged to the promotion of peace and prevention of conflict – Austria supports the African Union Program for Gender, Peace and Security. Other geographical priority areas are the Black Sea region (where Austria focuses on policy development and institutions to support women who have suffered sexual violence) and Syria/Iraq where Austria contributes towards the development of a UN Strategy to counter sexual violence in conflicts in the MENA region (e.g. Conference "Fighting Conflict Related Sexual Violence – Grassroots Women as Agents of Change" in Graz, 2016). The **Austrian Army** continues to pursue a 10 % women goal, in particular in positions of leadership and continuously conducts training programs on SC Res. 1325. The Peace University in Stadtschlaining offers **training courses for the protection of civilians** in armed conflict which constitute a concrete contribution to combatting sexual violence in conflicts.

Sweden[16]
Sweden has adopted a national four-year **Action Plan** (from 2016 to 2020) for implementing the country's women's policy as well as SC Res. 1325 (and subsequent WPS resolutions), covering actions and projects worldwide.

Strategic focus of the Action Plan is **Conflict prevention** (participation of more women e.g. in peace talks, mediation, etc.). To this end, Sweden is supporting civil society organizations in conflict or post-conflict countries working on peace processes and peacebuilding. Sweden strives to include a gender perspective in peace agreements and seeks to empower women to engage in mediation.

Leadership and expertise: Relevant State actors and government agencies must ensure operationalization of the Action Plan.

Sweden is forging **international alliances and partnerships** in order to ensure global implementation of Resolution 1325, increasing the exchange of information and experience as well as facilitating joint action. The relevant fora include the Nordic Countries, the EU, the Council of Europe (important normative role), as well as the UN, NATO and OSCE.

Geographic priority countries are in **Africa**: DRC, Liberia, Mali and Somalia; **Asia:** Afghanistan and Myanmar; **Europe**: BiH and Ukraine; **Latin America**: Colombia; **Middle East:** Iraq, Palestine and Syria.

United Kingdom
The UK has visibly championed the cause

Os **seis objetivos** são:

Participação:
- maior percentual de mulheres nas instituições da UE e nas instituições dos Estados membros da UE;

- Promoção ativa da participação das mulheres em todos os processos de tomada de decisão política, incluindo a prevenção de conflitos, a solução de conflitos, a mediação, a recuperação pós-conflito e a consolidação da paz;

Incorporação (*mainstreaming*) de gênero
- Incorporar uma perspectiva de gênero como componente integrativo em todas as políticas

Liderança pelo exemplo
- Maior empenho político da UE e medidas mais eficazes da UE para implementar a Agenda WPS a nível local, nacional, regional e internacional;

Prevenção
- Os sistemas e medidas de alerta prévio da UE devem ser sensíveis às questões de gênero;

- Papel mais preponderante da UE na prevenção, monitoramento e comunicação de informações sobre violações dos direitos humanos infligidas a mulheres e meninas em situações de conflito;

- Implementação da "política de tolerância zero" e responsabilização/fim da impunidade para os perpetradores;

Proteção
- Envolvimento da UE em prol dos direitos das mulheres e das meninas em níveis local, nacional, regional e internacional;

- Promoção da criação/ativação de mecanismos institucionais para a proteção de mulheres e meninas - assim como homens e meninos - em contextos/situações de conflito e vulnerabilidade, a fim de contribuir para a prevenção e eliminação de todas as formas de violência sexual e de gênero;

Alívio e Recuperação[15]
- Disponibilizar ajuda adequada para facilitar o socorro e a recuperação de mulheres e meninas particularmente afetadas por situações de conflito em curso ou passadas.

Vejamos alguns compromissos e ações individuais dos Estados membros da UE:

Áustria
Desde 2007, a Áustria tem trabalhado consistentemente para implementar as recomendações da Resolução 1325 do Conselho de Segurança através de planos de ação nacionais centrados na participação das equipes militar e civil austríacas em missões de paz, no contexto das relações multilaterais e bilaterais, da cooperação para o desenvolvimento e da ajuda humanitária.

Através da sua **cooperação para o desenvolvimento** - 15% da sua ajuda bilateral é destinada à promoção da paz e prevenção de conflitos - a Áustria apoia o Programa da União Africana para o Gênero, a Paz e a Segurança. Outras áreas geográficas prioritárias são a região do Mar Negro (onde a Áustria concentra seus esforços no desenvolvimento de políticas e instituições de apoio às mulheres que sofreram violência sexual) e Síria/Iraque, onde a Áustria contribui para o desenvolvimento de uma estratégia da ONU para combater a violência sexual nos conflitos na região do Oriente Médio e Norte da África (ex. Conferência "Combate à Violência Sexual Relacionada a Conflitos - Mulheres Nativas como Agentes de Mudança" em Graz, 2016). O **Exército austríaco** continua a perseguir uma meta de 10% de mulheres, particularmente, em cargos de liderança, e realiza continuamente programas de treinamento sobre a Resolução 1325. A Universidade da Paz em Stadtschlaining oferece **cursos de treinamento para a proteção de civis** em conflitos armados, que constituem uma contribuição concreta para o combate à violência sexual em conflitos.

Sweden[16]
A Suécia adotou um **plano de ação** nacional de quatro anos (de 2016 a 2020) para implementar a política de mulheres do país, assim como a resolução 1325 do Conselho de Segurança da ONU (e subsequentes resoluções em WPS), cobrindo ações e projetos em todo o mundo.

O **foco estratégico** do Plano de Ação é a **prevenção de conflitos** (participação de mais mulheres, por exemplo, em negociações de paz, mediação, etc.). Para este fim, a Suécia está apoiando organizações da sociedade civil em países em conflito ou pós-conflito, trabalhando em processos de paz e construção da paz. A Suécia se esforça para incluir uma perspectiva de gênero nos acordos de paz e busca capacitar as mulheres para se envolver na mediação.

of Women, Peace and Security for years, including in Brazil.[17] In their joint foreword to the latest report to Parliament[18], the three Secretaries Jeremy Hunt (Foreign and Commonwealth Affairs), Penny Mordaunt (International Development) and Gavin Williamson (Defense), emphasize their commitment:

"(....)We must continue to promote gender equality and women's empowerment, most importantly through women's inclusion in peace processes. We know the positive impact women can have on conflict prevention and peacebuilding: when women meaningfully participate in peace processes the resulting agreement is 35 percent more likely to last at least 15 years."

The UK works at amplifying the voices of women peacebuilders, including through the launch of the Women Mediators across the Commenwealth (WMC) initiative.

Under the UK Presidency of the UN Security Council in August of 2018 a female civil society member was able to brief the Council on Iraq for the very first time.

The DFID supports over 120 programmes in more than 30 countries to eradicate violence against women.

The British Defence Academy inaugurated a Military Gender and Protection Advisors Course with training in understanding gender dynamics in military operations.

In November 2019, the UK will host an International Conference on Preventing Sexual Violence in Conflict, an area of long-standing engagement.

Part III Threats connected to Digital Economy and Cyber Space

This part makes the point that the more our societies rely on advanced technologies for wealth generation and security, the more critical the under-representation of women in some fields becomes.

In almost any country some of the more technologically laden sectors are characterized by a particularly low participation of women. In university jargon it is STEM – Science, Technology, Engineering and Mathematics – where women are notoriously underrepresented.

This is true also for such a key field as energy – fossil, nuclear as well as renewables even though there is a slightly better representation of women in renewable energy as was pointed out by a recent report by the International Renewable Energy Agency (IRENA): globally renewable energy employs about 32 % women, compared to 22 % in the energy sector overall[19]

It has been long argued that the under-representation of women in crucial areas such as energy or more broadly STEM deprives the economy and society at large of a large pool of talent badly needed to promote the energy transition to climate-compatible energy scenarios and address other major present day challenges.[20]

The World Economic Forum Gender Gap Report spells this out very explicitly in its 2018 edition with regard to AI (Artificial Intelligence):[21]

"This report finds that, globally, although many countries have achieved important milestones towards gender parity across education, health, economic and political systems, there remains much to be done. On the one hand, countries where the next generation of women are becoming leaders in their domains are poised for further success. On the other hand, this year's analysis also warns about the possible emergence of new gender gaps in advanced technologies, such as the risks associated with emerging gender gaps in Artificial Intelligence-related skills. In an era when human skills are increasingly important and complementary to technology, the world cannot afford to deprive itself of women's talent in sectors in which talent is already scarce."

The same holds true for the field of cybersecurity, where – according to a recent FORBES article[22] – only 20 % of the staff dealing with cybersecurity are women. It is argued that diversifying the cybersecurity staff by increasing the number of women working on cybersecurity would entail significant advantages, such as matching a broad range of perpetrator profiles with a broad range of protector profiles. The sector will create many vacancies in the next few years, which would allow interested women to "catch up", especially since supply of female candidates for these vacancies seems to be quite limited.

Liderança e experiência: Atores relevantes do Estado e agências governamentais devem garantir a operacionalização do Plano de Ação.

A Suécia está forjando **alianças e parcerias internacionais** para garantir a implementação global da Resolução 1325, aumentando o intercâmbio de informações e experiências, bem como facilitando a ação conjunta. Os fóruns relevantes incluem os países nórdicos, a UE, o Conselho da Europa (importante papel normativo), bem como as Nações Unidas, a OTAN e a OSCE.

Países geograficamente prioritários estão na África: RDC, Libéria, Mali e Somália; Ásia: Afeganistão e Mianmar; **Europa**: Bósnia e Herzegovina; **América Latina**: Colômbia; **Oriente Médio**: Iraque, Palestina e Síria.

Reino Unido
O Reino Unido tem defendido visivelmente a causa da Mulher, Paz e Segurança por anos, inclusive no Brasil[17]. No prefácio conjunto ao mais recente relatório ao Parlamento[18], os três secretários, Jeremy Hunt (Assuntos Internacionais e da Comunidade - *Commonwealth*), Penny Mordaunt (Desenvolvimento Internacional) e Gavin Williamson (Defesa), enfatizam seu compromisso:

"(....)Devemos continuar a promover a igualdade de gênero e o empoderamento das mulheres, principalmente por meio da inclusão das mulheres nos processos de paz. Conhecemos o impacto positivo que as mulheres podem ter na prevenção de conflitos e na construção da paz: quando as mulheres participam de forma significativa nos processos de paz, o acordo resultante tem 35% mais chances de durar pelo menos 15 anos."

O Reino Unido trabalha para ampliar as vozes femininas que constroem a paz, inclusive por meio do lançamento da iniciativa Mulheres Mediadoras na Comunidade (Women Mediators across the Commenwealth - WMC).

Sob a presidência britânica do Conselho de Segurança da ONU, em agosto de 2018, um membro da sociedade civil do sexo feminino foi capaz de, pela primeira vez, falar ao Conselho sobre o Iraque.

O DFID (Departamento para o Desenvolvimento Internacional) apoia mais de 120 programas em mais de 30 países para erradicar a violência contra as mulheres.

A Academia Britânica de Defesa inaugurou um Curso de Assessoria Militar sobre Gênero e Proteção com treinamento para entender a dinâmica de gênero nas operações militares.

Em novembro de 2019, o Reino Unido sediará uma Conferência Internacional sobre Prevenção da Violência Sexual em Conflitos, uma área em que está envolvido há muito tempo.

Parte III Ameaças relacionadas à Economia Digital e ao Ciberespaço

Esta parte do artigo enfatiza que, quanto mais nossas sociedades dependem de tecnologias avançadas para a geração de riqueza e segurança, mais crítica se torna a sub-representação das mulheres em alguns campos.

Em quase todos os países, alguns dos setores mais tecnologicamente intensivos são caracterizados por uma participação particularmente baixa de mulheres. No jargão da universidade, são as áreas **STEM** - Ciência, Tecnologia, Engenharia e Matemática - onde as mulheres são notoriamente sub-representadas.

Isto também vale para um setor tão importante como o **energético** – energias fóssil, nuclear e também as renováveis, embora exista uma representação ligeiramente maior das mulheres nas energias renováveis, como foi apontado por um relatório recente da Agência Internacional de Energia Renovável (IRENA): globalmente a energia renovável emprega cerca de 32% de mulheres, em comparação com 22% no setor de energia em geral[19].

Há muito argumenta-se que a sub-representação de mulheres em áreas cruciais como energia ou de modo geral, as áreas STEM priva a economia e a sociedade em geral de um grande conjunto de talentos necessários para promover a transição energética para cenários energéticos compatíveis com a mudança do clima e outros grandes desafios atuais[20].

O Relatório do Gênero do Fórum Econômico Mundial explica isto muito explicitamente na sua edição de 2018 no que diz respeito à IA (Inteligência Artificial)[21]:

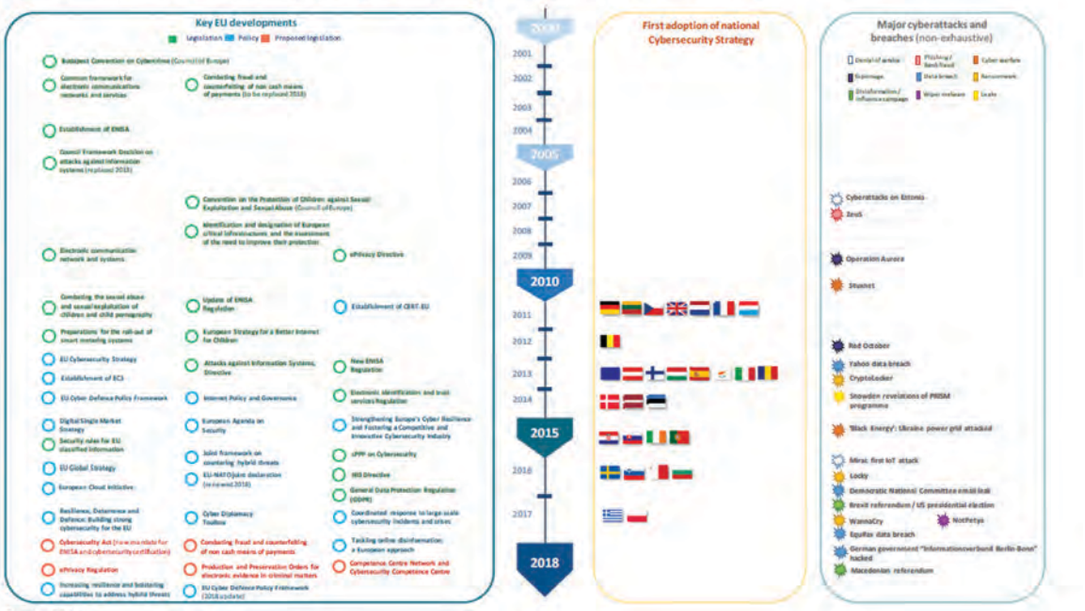
"Este relatório conclui que, globalmente, embora muitos países tenham alcançado marcos importantes para a paridade de gênero nos sistemas de educação, saúde, economia e política, ainda há muito a ser feito. Por um lado, os

An EU Policy Brief[23] provides an overview of the amount of activity in the area and the multitude of EU actors involved in it; the diagram on the following page gives a flavor of the flurry of activities and multitude of approaches and legal documents; the gender dimension is not explicitly addressed as it seems.

A study by KPMG[24] on the cybersecurity situation in Austria finds that the sectors industry, energy, infrastructure/transport/logistics are most often subject to cyberattacks; it did not reflect on the gender dimension explicitly either.

At the Vienna Cyber Security Week 2019 the gender dimension was acknowledged explicitly through the inclusion of a Women's Cyber Forum. The following video links allow for a glimpse into the discussions: Women's Cyber Forum @ VCSW19 - Stakeholder Voices (Part 1/2) https://youtu.be/Lb3iC8vWVPo ; Women's Cyber Forum @ VCSW19 -Stakeholder Voices (Part 2/2) https://youtu.be/1sQwBUGkyuQ .

Figure 2 – An acceleration in policy development and legislation (as at 31 December 2018)



Source: ECA.

*I am grateful to Amadeus Faltheiner, Attaché at the Austrian Embassy in Brasilia from February to August 2019, for his preparatory research for and assistance with the redaction of this Policy Brief.

países onde a próxima geração de mulheres está se tornando líder em seus domínios estão prestes a ter êxito. Por outro lado, a análise deste ano também adverte sobre o possível surgimento de novas disparidades de gênero em tecnologias avançadas, como os riscos associados a disparidades de gênero emergentes em habilidades relacionadas à Inteligência Artificial. Em uma era em que as habilidades humanas são cada vez mais importantes e complementares à tecnologia, o mundo não pode se dar ao luxo de se privar do talento das mulheres em setores nos quais o talento já é escasso."

O mesmo vale para o campo da **segurança cibernética**, onde - de acordo com um artigo recente da FORBES[22] - apenas 20% dos funcionários que lidam com segurança cibernética são mulheres. Argumenta-se que a diversificação da equipe de cibersegurança, aumentando o número de mulheres que trabalham na área, traria vantagens significativas, como, por exemplo, poder combinar uma ampla gama de perfis de perpetradores com uma ampla gama de perfis de proteção. O setor criará muitas vagas nos próximos anos, o que permitiria que as mulheres interessadas se atualizassem, especialmente porque a oferta de candidatas para essas vagas parece ser bastante limitada.

Um *Policy Brief* da UE[23] fornece uma visão geral do volume de atividade na área e da multiplicidade de intervenientes da UE envolvidos na mesma; o diagrama na página seguinte dá uma ideia da enxurrada de atividades e múltiplas abordagens e documentos legais; a dimensão de gênero não é explicitamente abordada como parece.

Um estudo da KPMG[24] sobre a situação de cibersegurança na Áustria constata que os setores industrial, de energia, infraestrutura/transportes/logística estão mais sujeitos a ataques cibernéticos; também não refletiu sobre a dimensão de gênero explicitamente.

Na Semana de Segurança Cibernética de Viena, em 2019, a dimensão de gênero foi reconhecida explicitamente por meio da inclusão de um Fórum Cibernético Feminino. Os links de vídeo a seguir permitem vislumbrar as discussões: Women's Cyber Forum - VCSW19 - Stakeholder Voices (Parte 1/2) https://youtu.be/Lb3iC8vWVPo; Fórum Cibernético Feminino @ VCSW19 - Vozes de Entusiasta (Parte 2/2) https://youtu.be/1sQwBUGkyuQ.

* Sou grata a Amadeus Faltheiner, adido na Embaixada da Áustria em Brasília, de fevereiro a agosto de 2019, por sua pesquisa preparatória e assistência na redação deste Resumo de Política (Policy Brief).

1 Gender and Humanitarian Action.

2 https://www.nobelprize.org/prizes/peace/2018/press-release/

3 EU Global Strategy, 2016, p. 14

4 https://www.ohchr.org/EN/ProfessionalInterest/Pages/Vienna.aspx

5 http://beijing20.unwomen.org/en/about

6 https://www.peacewomen.org/SCR-1325

7 Note by the Secretary-General on the Follow-Up to the Outcome of the Millennium Summit, A/59/565 of 2 December 2004.

8 A Res 60/1 2005 World Summit Outcome, para. 143 reads: We stress the right of people to live in freedom and dignity, free from poverty and despair. We recognize that all individuals, in particular vulnerable people, are entitled to freedom from fear and freedom from want, with an equal opportunity to enjoy all their rights and fully develop their human potential. To this end, we commit ourselves to discussing and defining the notion of human security in the General Assembly.

9 A/RES/66/290

10 https://openknowledge.worldbank.org/bitstream/handle/10986/4391/9780821388105_overview.pdf?sequence=6&isAllowed=y

11 https://www.weforum.org/reports/the-global-gender-gap-report-2018

12 http://www.arab-hdr.org/reports/2005/english/execsummary-e2005.pdf?download

13 http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf ; p.31.

14 Women, Peace and Security, Council conclusions (10 December 2018), 15086/18; https://www.consilium.europa.eu/de/press/press-releases/2018/12/10/women-peace-and-security-council-adopts-conclusions/

15 The EU is the biggest contributor to the UN Women's WPHF solely dedicated to enhancing the participation of women in relevant peace processes, currently accounting for 61 % of total WPHF contributions. For the latest report go to http://www.unwomen.org/en/digital-library/publications/2019/06/empowerment-and-accountability-for-gender-equality-in-humanitarian-action-and-crisis-response-2018

16 https://www.government.se/contentassets/8ae23198463f49269e25a14d4d14b9bc/women-peace-and-security-eng.pdf

17 Since 2014, the British Embassy in Brasília has been funding bilateral projects to advance the UN WPS agenda in Brazil, including Raising the profile of the Preventing Sexual Violence in Conflict Initiative (PSVI) in cooperation with universities; Enhancing Brazil's engagement with the UN Women, Peace and Security Agenda: mainstreaming gender and addressing sexual violence in conflict, including by analyzing the challenges and lessons learned from the first Brazilian women incorporated in the forces, and by developing training modules on sexual violence for CCOPAB (Brazilian Peacekeeping Training Centre), for officers and civilian experts; by working with the Global South Unit for Mediation (PUC-RJ) on gender and violence.

18 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/765743/UK_National_Action_Plan_on_Women_Peace_and_Security_2018_-2022_annual_report_to_Parliament_2018.pdf

19 https://www.irena.org/publications/2019/Jan/Renewable-Energy-A-Gender-Perspective

20 The Global Women's Network for the Energy Transition, www.globalwomennet.org , e.g. advocates for greater inclusion of women in all fields of the energy sector and offers networking and mentoring opportunities for women in energy;

21 http://www3.weforum.org/docs/WEF_GGGR_2018.pdf , p.v

22 https://www.forbes.com/sites/laurencebradford/2018/10/18/cybersecurity-needs-women-heres-why/#157982c547e8

23 https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf

24 KPMG, Cyber Security in Österreich. September 2017, kpmg.at/cyber

1 Gender and Humanitarian Action, https://gsdrc.org/document-library/gender-conflict-and-peace/

2 https://www.nobelprize.org/prizes/peace/2018/press-release/

3 EU Global Strategy, 2016, p. 14

4 https://www.ohchr.org/EN/ProfessionalInterest/Pages/Vienna.aspx

5 http://beijing20.unwomen.org/en/about

6 https://www.peacewomen.org/SCR-1325

7 Nota do Secretário-Geral sobre o Seguimento do Resultado da Cúpula do Milênio, A/59/565 of 2 December 2004.

8 A Res 60/1 2005 Resultado da Cúpula Mundial, par. 143: Ressaltamos o direito das pessoas de viver em liberdade e dignidade, livres da pobreza e do desespero. Reconhecemos que todos os indivíduos, em particular as pessoas vulneráveis, têm o direito de se libertar do medo e da necessidade, com oportunidades iguais de desfrutar de todos os seus direitos e desenvolver plenamente o seu potencial humano. Para tanto, nos comprometemos a discutir e definir a noção de segurança humana na Assembléia Geral.

9 A/RES/66/290

10 https://openknowledge.worldbank.org/bitstream/handle/10986/4391/9780821388105_overview.pdf?sequence=6&isAllowed=y

11 https://www.weforum.org/reports/the-global-gender-gap-report-2018

12 http://www.arab-hdr.org/reports/2005/english/ecsummary-e2005.pdf?download

13 http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf ; p.31.

14 Mulheres, paz e segurança, conclusões do Conselho (10 Dezembro 2018), 15086/18; https://www.consilium.europa.eu/de/press/press-releases/2018/12/10/women-peace-and-security-council-adopts-conclusions/

15 A UE é o maior contribuinte para o WPHF da ONU Mulheres dedicado exclusivamente a aumentar a participação das mulheres em processos de paz relevantes, representando atualmente 61% do total das contribuições do WPHF. Para ter acesso ao último relatório, veja http://www.unwomen.org/en/digital-library/publications/2019/06/empowerment-and-accountability-for-gender-equality-in-humanitarian-action-and-crisis-response-2018

16 https://www.government.se/contentassets/8ae23198463f49269e25a14d4d14b9bc/women-peace-and-security-eng.pdf

17 Desde 2014, a Embaixada Britânica em Brasília vem financiando projetos bilaterais para avançar a agenda da ONU em material de WPS no Brasil, incluindo o aumento do perfil da Iniciativa de Prevenção da Violência Sexual em Conflito (PSVI) em cooperação com universidades; Reforçando o engajamento do Brasil com a Agenda ONU Mulheres, Paz e Segurança: incorporando gênero e abordando a violência sexual em conflitos, inclusive analisando os desafios e lições aprendidas com as primeiras mulheres brasileiras incorporadas às forças e desenvolvendo módulos de treinamento sobre violência sexual para o CCOPAB (Centro Conjunto de Operações de Paz do Brasil), para oficiais e especialistas civis; trabalhando com a Unidade do Sul Global para Mediação (PUC-RJ) sobre gênero e violência.

18 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/765743/UK_National_Action_Plan_on_Women_Peace_and_Security_2018_-2022_annual_report_to_Parliament_2018.pdf

19 https://www.irena.org/publications/2019/Jan/Renewable-Energy-A-Gender-Perspective

20 A Rede Global de Mulheres para a Transição Energética, www.globalwomennet.org , por exemplo, defende uma maior inclusão das mulheres em todas as áreas do setor energético e oferece oportunidades de networking/contatos e de mentoria para mulheres sobre o setor energético;

21 http://www3.weforum.org/docs/WEF_GGGR_2018.pdf , p.v

22 https://www.forbes.com/sites/laurencebradford/2018/10/18/cybersecurity-needs-women-heres-why/#157982c547e8

23 https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf

24 KPMG, Cyber Security in Österreich. September 2017, kpmg.at/cyber

XVIFORTE