2017

XIV Forte de Copacabana Conference
International Security

3/6

COLEÇÃO DE POLICY PAPERS
THE POLICY PAPERS COLLECTION

As Capacidades Sul-Americanas contra Ameaças Cibernéticas: Das Fragilidades Atuais a uma Resposta Comum

The South American Capabilities against Cyber Threats: From the Current Weaknesses towards a Common Response

María Lourdes Puente Olivera
Susana García

Organisers

Konrad Adenauer Stiftung

CEBRI
BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS

Supported by

União Europeia

XIV Forte de Copacabana Conference
International Security

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 14ª edição, a conferência de 2017 tem como tema 'Arquitetura de Segurança: um intercâmbio entre América do Sul e Europa'. A conferência é aberta ao público e os participantes são incentivados a participar ativamente das discussões. Como novidade para este ano, 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 14th edition of the conference is 'Security Architecture: An Exchange between South America and Europe'. The conference is open to the public and the audience is encouraged to actively engage in discussions. As an innovation in 2017, this collection of Policy Papers reflects the major themes of the event and intend 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
Dr. Jan Woischnik

Coordenação editorial Project Coordination
Diogo Winnikes
Reinaldo Themoteo

Colaboração Editorial Support
Diego Andrade de Freitas
Sebastian Breuer

Projeto Gráfico Design
Charles Steiman

Impressão Print
J. Sholna

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
Perspectivas Sul-Americanas para uma Futura Cooperação em Arquitetura de Segurança: Arranjos, Processos e Desafios

South American Perspectives for Future Cooperation on Security Architecture: Arrangements, Processes and Challenges

Antonio Jorge Ramalho
Tradução e revisão Translation and Revision: Leslie Sasson Cohen

2/6
A Ordem de Segurança Global e Europeia na Crise: Poder, Instituições, Princípios

The Global and European Security Order during the Crisis: Power, Institutions, Principles

Markus Kaim
Tradução Translation: Tito Lívio Cruz Romão I Revisão Revision: Leslie Sasson Cohen

3/6
As Capacidades Sul-Americanas contra Ameaças Cibernéticas: Das Fragilidades Atuais a uma Resposta Comum

The South American Capabilities against Cyber Threats: From the Current Weaknesses towards a Common Response

María Lourdes Puente Olivera

Susana García
Tradução e revisão Translation and Revision: Leslie Sasson Cohen

4/6
As Capacidades Europeias contra Ameaças Cibernéticas: Fortalecendo a Segurança de TI na Alemanha

The European Capabilities against Cyber Threats: Strengthening IT Security in Germany

Hagen Colberg
Tradução Translation: Tito Lívio Cruz Romão I Revisão Revision: Leslie Sasson Cohen

5/6
O Nexo Transatlântico do Narcotráfico: a Visão Sul-Americana para uma melhor Colaboração entre a América do Sul e a Europa contra o Tráfico de Drogas

The Transatlantic Narco-Nexus: The South American View for better Collaboration between South America and Europe against Drug Trafficking

Thiago Rodrigues

Carol Viviana Porto
Tradução e revisão Translation and Revision: Leslie Sasson Cohen

6/6
A Perspectiva Europeia para uma melhor Colaboração entre a América Latina e a Europa no Combate ao Narcotráfico

The European View for better Collaboration between Latin America and Europe against Drug Trafficking

Mikael Wigell

Joren Selleslaghs
Tradução e revisão Translation and Revision: Leslie Sasson Cohen

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.

União Europeia

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 quase 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 nearly 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.

María Lourdes Puente Olivera é Especialista em Segurança, Defesa e Serviços de Inteligência e Professora de Relações Internacionais na Universidade Austral e de Estratégia e Segurança Internacional na Pontifícia Universidade Católica da Argentina. Além disso, ela é Diretora na Escola de Política e Governo na Faculdade de Ciências Sociais na Pontifícia Universidade Católica da Argentina. Trabalhou por mais de 20 anos como analista internacional na Marinha argentina e foi Diretora Nacional do Serviço de Inteligência Militar. Ela é cientista política e possui mestrado em Relações Internacionais.

María Lourdes Puente Olivera is a Specialist in Security, Defence and Intelligence and Professor in International Relations at the Austral University and in Strategy and International Security at the Pontifical Catholic University of Argentina. Furthermore, she is currently Director of the School of Politics and Government of the Faculty of Social Sciences at the Pontifical Catholic University of Argentina. She worked for more than 20 years as an international analyst in the Navy and was National Director of Military Intelligence. She is a politologist and has a Master in International Relations.

Susana García de Santangelo é conselheira de Ciência e Tecnologia na Marinha argentina e especialista em Segurança Internacional. Além disso, ela é docente na Pontifícia Universidade Católica da Argentina.

Susana García de Santangelo is an adviser in Science and Technology in the Argentine Navy and a specialist in International Security. Besides, she is a lecturer at the Pontifical Catholic University of Argentina.

As Capacidades Sul-Americanas contra Ameaças Cibernéticas: Das Fragilidades Atuais a uma Resposta Comum

María Lourdes Puente Olivera
Susana García

The South American Capabilities against Cyber Threats: From the Current Weaknesses towards a Common Response

The Regional Security Architectures are challenged by the emergence of this new and enlarging space, whereas relationship, communication and operation are also new. In the cyberspace, the States' empowerment is a complex matter and even if they succeed in doing so, they must resort to advanced technology. If we try to answer if South America has enough capacities against cyber threats, we necessarily must know what steps were given in each country. Integration is a pending debt in the sub region and it does not differ from a superior reality.

Deep inside every Latin American country, we can affirm that with different timing and priority, they are trying to incorporate the cyber issue into their own domestic agenda. This purpose, also fueled by the fear to be left out of major regional and global agreements, favors the internal and external tendency of responding adequately to international commitments and good practices. For the last decade or so, the need to design public policies, elaborate planning consistent with public investment efforts and consolidate a comprehensive framework including all the components involved, has been continuously pursued without consolidating that intention into actions at the National level. This reality undoubtedly hinders and slows down any initiative at the regional level.

The last report prepared by the Inter-American Development Bank (IDB) and the Organization of American States (OAS)[1], with support from various institutions, presents a clear description of each Latin American country. It shows how the reality of cybersecurity is in these latitudes and the vulnerability in which they are immersed. We are interested in highlighting three items that the report's data reveal crudely: very few countries have succeeded in adopting a national cybersecurity strategy; the lack of progress in their ability to generate a response to incidents, and the lack of solid, and still less common, regulatory frameworks[2].

Lacking a national strategy document is the most critical of the above mentioned. The cybersecurity strategy is the first step in order to coordinate actions in the region. It should define the structure of responsibilities at the national level, legal framework and technical implementation standards, national and sectoral awareness policy, technical skills and capacities to provide adequate security to critical infrastructure and international and domestic cooperation mechanisms.

Regarding Incident Response Capacity, the IDB Report also points out their weaknesses[3]. These Response Centers are a valuable element in strengthening the resilience of a public or private entity in the event of an attack that could affect the normal operation of a particular critical infrastructure. The lack of national cyber strategies including these capacities has caused that in Latin America the private sector has advanced well above the public sector in terms of operational, cooperation and interconnectivity of its CSIRTs, favored by a greater availability of technical and financial resources, a high risk exposure linked to international trade operations and more specific operating environments.

As for the Normative Framework, even though there is a very weak adherence to the Convention on Cybercrime (Budapest Convention), almost all OAS Member States have increased their law enforcement efforts at the national level. They are in process of updating their legal frameworks to fight against cybercrime and strengthen data protection and privacy laws. Adherence to this type of international agreement does not escape the dislike and lack of confidence that they should subject the norms in whose design they have not taken part and whose accomplishment control is exercised by others, the ones whose interests seem better covered. The resistance is also due to the vulnerability to which the countries are exposed in this type of exchanges.

1 The Inter-American Development Bank (IDB) and the Organization of American States (OAS) presented a study prepared by the two institutions with the support of the University of Oxford - Report on Cyber-security 2016 - showing that the region is highly vulnerable to cyberattacks. The report also had the collaboration of the Center for Strategic International Studies, the Getulio Vargas Foundation, the FIRST organization, the Council of Europe, the Potomac Institute and the World Economic Forum.

2 In 2016 only six, three from South America (Brazil, Colombia and Uruguay) and three from Central America (Jamaica, Panama and Trinidad and Tobago) from the 32 Member States of The OAS had adopted cybersecurity strategies. Another 11 countries (only four South American countries: Argentina, Paraguay, Peru and Suriname) would be in an articulation phase.

3 The IDB Report finds that in 16 countries, Computer Security Incident Response Teams (CSIRTs) have been established and operationalized, of which only seven of them have reached intermediate maturity levels , if we consider the Latin American scenario. All of them would be very lagging behind the leading countries in this area like the United States, Israel, Estonia and South Korea.

As Arquiteturas de Segurança Regionais enfrentam o desafio representado pela emergência desse novo e amplo espaço em que relacionamentos, comunicação e a própria operação são também novos. No ciberespaço, o empoderamento do Estado é uma questão complexa e mesmo quando bem sucedido, requer recorrer a tecnologia avançada. Ao tentar responder à questão se a América do Sul tem as capacidades necessárias para se defender contra as ameaças cibernéticas, é necessário saber quais passos foram dados em cada país. A integração é uma dívida pendente na sub-região e não difere de uma realidade superior.

Podemos afirmar que cada país latino-americano está tentando incorporar a questão cibernética em sua agenda doméstica com diferentes ritmos e graus de prioridade. Esse propósito, que também é alimentado pelo temor de ficar de fora de importantes acordos globais e regionais, favorece a tendência interna e externa de responder adequadamente a compromissos e boas práticas internacionais. Durante a última década, a necessidade de elaborar políticas públicas, fazer um planejamento consistente com os esforços de investimento público e de consolidar um quadro abrangente que inclua todos os componentes envolvidos, foi continuamente buscada sem, contudo, consolidar essa intenção em ações em nível nacional. Essa realidade, sem dúvida, dificulta e retarda qualquer iniciativa em nível regional.

O último relatório preparado pelo Banco Interamericano de Desenvolvimento (BID) e pela Organização de Estados Americanos (OEA) [1], com o apoio de diversas instituições, apresenta uma descrição clara de cada país latino-americano. Demonstra a realidade da segurança cibernética nessas latitudes e a vulnerabilidade em que estão imersos. Nosso interesse é ressaltar três itens revelados pelas informações do relatório: poucos países conseguiram adotar uma estratégia nacional de segurança cibernética, a falta de avanços em sua capacidade de gerar respostas a incidentes e a falta de marcos regulatórios sólidos[2].

A falta de um documento estratégico nacional é a questão mais critica dentre as acima listadas. A estratégia de segurança cibernética é o primeiro passo para uma coordenação de ações na região. Ela deve definir a estrutura de responsabilidades em nível nacional, o marco legal e os padrões técnicos de implementação, a política de conscientização nacional e setorial, as habilidades técnicas e capacidades para proporcionar segurança adequada a infraestruturas críticas e os mecanismos de cooperação nacional e internacional.

Com relação à Capacidade de Resposta a Incidentes, o Relatório do BID também destaca suas fragilidades[3]. Esses Centros de Resposta são um elemento valioso para o fortalecimento da resiliência de entidades públicas e privadas no caso de um ataque que pudesse afetar a operação normal de uma infraestrutura crítica em particular. A falta de estratégias cibernéticas nacionais, incluindo essas capacidades, tem resultado em que, na América Latina, o setor privado tenha avançado muito além do setor público em termos de operação, cooperação e interconectividade de seus CSIRTs (Computer Security Incident Response Teams - Equipes de Resposta a Incidentes de Segurança Cibernética), favorecidos por uma maior disponibilidade de recursos técnicos e financeiros, uma maior exposição a riscos relacionada a operações de comércio internacional e ambientes operacionais mais específicos.

Com relação ao Marco Normativo, embora haja pouca adesão à Convenção sobre o Cibercrime (Convenção de Budapeste), quase todos os Estados membros da OEA aumentaram seus esforços para aplicar Leis em nível nacional. Estão em processo de atualização de seus marcos legais para combater os crimes cibernéticos e fortalecer as leis de

1 O Banco Interamericano de Desenvolvimento (BID) e a Organização dos Estados Americanos (OEA) apresentaram um estudo preparado pelas duas instituições com o apoio da Universidade de Oxford - Relatório sobre Segurança Cibernética 2016 - mostrando que a região é altamente vulnerável a ataques cibernéticos. O relatório também contou com a colaboração do Centro de Estudos Estratégicos Internacionais, da Fundação Getúlio Vargas, da Organização FIRST, do Conselho da Europa, do Instituto Potomac e do Fórum Econômico Mundial.

2 Em 2016, apenas seis países, três da América do Sul (Brasil, Colômbia e Uruguai) e três da América Central (Jamaica, Panamá e Trinidad e Tobago) dos 32 Estados membros da OEA adotaram estratégias de segurança cibernética. Outros 11 países (apenas quatro países sul-americanos: Argentina, Paraguai, Peru e Suriname) estariam em fase de articulação.

3 O Relatório do BID descobriu que dos 16 países em que as equipes de resposta a incidentes de segurança cibernética (CSIRTs) foram estabelecidas e operacionalizadas, em apenas 7 atingiram nível intermediário de maturidade, se considerarmos o cenário latino-americano. Todos estariam em nível muito inferior ao de países líderes na área como Estados Unidos, Israel, Estônia e Coréia do Sul.

Considering the region as a whole, we observe that the cybersecurity policy in terms of integration is a matter more hemispheric than Latin American, taking into account that the organization that has shown progress in integrating common will into declarations and directives is the Organization of American States (OAS)[4]. The activity of the OAS, through its diverse and specific organisms, shows common intentions, but achievements rely only in discursive terms, even though an asymmetric and confusing operational capacity can be observed in terms of integration, cooperation and efficiency on the part of the governments of the countries that make up the American region as a whole. The most outstanding cooperation is the assistance provided by OAS to Latin American countries in the design process of their respective cyber security strategies and the corresponding settlement of CSIRTs. We also recognize advances in generating mutual confidence measures.

Inside the sub-region arena, South America still argues about the strengths of a viable Regional mechanism capable of integrating the different needs and aspirations of its diverse members. Therefore it should not be surprising that they have not been able to design an integral cybersecurity policy for the region, since this is only one side among many other slopes that make up the Latin American polyhedron[5].

Regarding training and cyber exercises, most of them are bilateral and their frequency is extremely low. Although we should admit the existence of some international experiences, like those organized by specific agencies from Spain with Latin America[6], they involve the particular complexity of including the participation of different domestic actors. The lack of solid national strategies causes this participation to be inorganic and increases domestic and international asymmetries. Therefore, what constitutes an advance is not so clear in terms of overall results.

Present asymmetries in Latin America and those inside each country (beside intra-national agencies) make the region vulnerable to the actions of third parties and cooperation may be reduced to a mere transmission of best practices, restricting the participation of Latin American countries to the provision of information about their own vulnerabilities. Latin America still, in a framework of inequality, continues to crave technological independence, also in the cybernetic arena.

Challenges and Proposals

South American countries need to advance first in the formulation and strengthening of national strategies of cyber security.

In this way, the first objective of such strategies will be to advance national determinations of critical infrastructure, in the detection of incidents and in the definition of levels of security. That is, to achieve the diagnosis of their own situations and the strategic planning that includes which assets they are going to protect and how they are turning this into a national matter. We need to solve these questions before taking part in international and regional levels.

At the same time, investment in technology is urgently needed to reduce the dependency gap of Latin American countries. It is investment in knowledge, in human resources, but also in communications infrastructure, mainly in connectivity.

It is also important to continue the trend towards shaping a harmonized legal basis to address cybercrime. The best channel for such cooperation is the Budapest Convention on Cybercrime. However, the construction of a regional approach to it would contribute to the generation of confidence in this sense.

International and/or European cooperation should differentiate three specific levels. First the fight against cybercrime, for if there is a common enemy identified, it should be the level

4 Extensive work done in OAS by the Secretariat of the Inter-American Committee against Terrorism (CICTE) and the Cybercrime Task Force of the Meeting of Ministers of Justice or Attorneys General of the Americas (REMJA / OAS) and the Inter-American Telecommunication Committee (CITEL).

5 At the subregional level, UNASUR - Union of South American Nations - has addressed the issue from 2012 on in its Action Plans, forming a Working Group, and Mercosur - Common Market of the South -, through the creation in 2014 of Meeting of Authorities on Privacy and Security of Information and Technological Infrastructure of Mercosur (RAPRISIT), as an auxiliary body of the Common Market Council. However, the difficulties that such organizations are facing as integration mechanisms are real obstacles in finding concrete advances in common policies in their decisions.

6 International exercises CyberEx, International competition of cyber security oriented to incident response teams that trains the activities of reaction and technical analysis of the participants before a cyber attack. The particularity of these is that the participants represent five sectors involved in this matter: private, governmental, academic, mixed and military

proteção da informação e da privacidade. A adesão a este tipo de acordo internacional não está imune à aversão e à falta de confiança a que estão sujeitas as normas de cuja elaboração não participaram e cujo controle de desempenho é exercido por terceiros cujos interesses parecem estar mais bem cobertos. A resistência também se deve à vulnerabilidade a que estão expostos os países nesse tipo de intercâmbio.

Considerando a região como um todo, observamos que a política de segurança cibernética em termos de integração é uma questão mais hemisférica do que latino-americana, uma vez que a organização que mais avançou na integração da vontade comum em suas declarações e diretrizes é a Organização dos Estados Americanos (OEA) [4]. A atividade da OEA, por meio de seus organismos diversos e específicos, mostra intenções comuns, mas as realizações dependem apenas de termos discursivos, embora uma capacidade operacional confusa e assimétrica possa ser observada em termos de integração, cooperação e eficiência por parte do governo dos países que compõem a região da América como um todo. A atividade de cooperação com mais destaque é a assistência prestada pela OEA aos países latino-americanos no processo de elaboração de suas estratégias de segurança cibernética e o correspondente processo de estabelecimento de CSIRTs. Também reconhecemos avanços na geração de medidas de confiança mútua.

Na arena sub-regional, a América do Sul ainda debate os pontos fortes de um mecanismo regional viável, capaz de integrar as diferentes necessidades e aspirações de seus diversos membros. Portanto, não é surpresa que ainda não tenham sido capazes de elaborar uma política integrada de segurança cibernética para a região, uma vez que essa é apenas uma das muitas faces que compõem o poliedro americano[5].

No que diz respeito a treinamento e exercícios cibernéticos, a maioria deles é bilateral e sua frequência é extremamente baixa. Embora devamos admitir a existência de algumas experiências internacionais, como aquelas organizadas por agências específicas da Espanha em conjunto com a América Latina6, elas envolvem a complexidade particular de incluir a participação de diferentes atores domésticos. A falta de estratégias nacionais sólidas faz com que essa participação não seja orgânica e aumenta as assimetrias domésticas e internacionais. Portanto, o que deveria constituir um avanço, não é tão claro em termos de resultados globais.

As assimetrias presentes na América Latina e aquelas em cada país (além das agências intranacionais) tornam a região vulnerável às ações de terceiros e, a cooperação pode ser reduzida a uma mera transmissão de melhores práticas, restringindo a participação de países latino-americanos no fornecimento de informações sobre suas próprias vulnerabilidades. Mesmo em um quadro de desigualdade, a América Latina ainda deseja atingir sua independência tecnológica também na arena cibernética.

Desafios e Propostas

Os países sul-americanos precisam avançar, primeiro, na formulação e fortalecimento de suas estratégias nacionais de segurança cibernética.

Deste modo, o primeiro objetivo de tais estratégias deve ser o de avançar as determinações nacionais para infraestruturas críticas, na detecção de incidentes e na definição de níveis de segurança. Ou seja, conseguir diagnosticar sua própria situação e fazer o planejamento estratégico incluindo os ativos a serem protegidos e como isso está sendo tornado uma questão nacional. Precisamos resolver estas questões antes de ter maior participação nos níveis regional e internacional.

Ao mesmo tempo, o investimento em tecnologia é urgente e necessário para reduzir o fosso de dependência dos países latino-americanos. Deve haver investimento em conhecimento, em

4 Trabalho extensivo realizado na OEA pela Secretaria do Comitê Interamericano contra o Terrorismo (CICTE) e pelo Grupo de Trabalho sobre Crimes Cibernéticos da Reunião de Ministros da Justiça ou Procuradores-Gerais das Américas (REMJA / OEA) e do Comitê Interamericano de Telecomunicações (CITEL).

5 No nível sub-regional, a UNASUL - União das Nações Sul-Americanas - abordou a questão a partir de 2012 em seus Planos de Ação, formando um Grupo de Trabalho e o Mercosul - Mercado Comum do Sul -, através da criação em 2014 da Reunião de Autoridades sobre Privacidade e Segurança da Informação e Infraestrutura Tecnológica do Mercosul (RAPRISIT), como órgão auxiliar do Conselho do Mercado Comum. No entanto, as dificuldades que essas organizações enfrentam como mecanismos de integração são obstáculos reais à obtenção de avanços concretos em políticas comuns em suas decisões.

6 Exercícios internacionais CyberEx, competição internacional de segurança cibernética orientada para equipes de resposta a incidentes que treinam as atividades de reação e análise técnica dos participantes antes de um ataque cibernético. A particularidade é que os participantes representam cinco setores envolvidos neste assunto: privado, governamental, acadêmico, mixto e militar.

most easily achievable even though it requires more national agencies involved and internal coordination; secondly, the exchange of transnational information and experience. It requires an explicit care of sensitive matters like privacy and network neutrality. Finally cyber defense, whose complexity is given by the possibility or inability to integrate common defense strategies.

Argentina and Brazil should take the lead in the region in terms of coordination and exchanges, so that a sub-regional alternative is possible in order to strengthen our capabilities and later contribute to their spread inside the region.

Europe, the European countries, through their organizations, would contribute by encouraging, through agreements, exchanges and exercises; such as actions that strengthen the regional perspective in order to better cooperate with them. Although it is difficult to define borders and/or exercise sovereignty in cyberspace, we know that the enemy actors are common, because they appear to be the same: organization and/or criminal and/or terrorist individuals.

Raising awareness and involving the private sector and the civil society are the other side of an effective fight against cyber dangers. This can only be achieved with the involvement of the State, with a strong political will to prioritize the issue, and by solving the problem of hiring, training and retaining trained human resources in the face of private competition that can pay better. Without this tool, there is no capacity to lead the process towards effective integration.

recursos humanos, mas também em infraestrutura de comunicações, e principalmente em conectividade.

Também é importante continuar na direção de moldar uma base jurídica harmonizada para enfrentar o crime cibernético. O melhor canal para essa cooperação é a Convenção de Budapeste sobre o Cibercrime. No entanto, o desenvolvimento de uma abordagem regional sobre a Convenção contribuiria para a geração de confiança nesse sentido.

A cooperação internacional e/ou europeia deve diferenciar três níveis específicos. Primeiro, o combate aos crimes cibernéticos, pois havendo um inimigo comum identificado, é o nível mais facilmente alcançado, embora exija mais agências nacionais envolvidas e coordenação interna; Em segundo lugar, o intercâmbio de informações e experiências transnacionais. Exige um cuidado explícito de assuntos sensíveis, como a privacidade e a neutralidade da rede. Finalmente, a defesa cibernética, cuja complexidade é dada pela possibilidade ou incapacidade de integrar estratégias de defesa comuns.

Brasil e Argentina deveriam assumir a liderança na região em termos de coordenação e intercâmbios, de modo a viabilizar uma alternativa sub-regional e fortalecer nossas capacidades e contribuir, mais adiante, com a sua disseminação na região.

A Europa e os países europeus, por meio de suas organizações, contribuiriam se incentivassem por meio de acordos, intercâmbio e exercícios ações para fortalecer a perspectiva regional e realizar uma melhor cooperação com ela. Embora seja difícil definir fronteiras e/ou exercitar a soberania no ciberespaço, sabemos que os inimigos são comuns por que parecem ser os mesmos: organizações e/ou indivíduos criminosos e/ou terroristas.

A sensibilização e o envolvimento do setor privado e da sociedade civil são o outro lado de uma luta efetiva contra os perigos cibernéticos. Isso só pode ser alcançado com o envolvimento do Estado, com uma forte vontade política que priorize a questão e com a solução do problema de recrutamento, treinamento e retenção de recursos humanos capacitados em face da concorrência do setor privado, que pode pagar mais. Sem essa ferramenta, não há capacidade para liderar o processo em direção à integração efetiva.