CEBRI
CENTRO BRASILEIRO DE RELAÇÕES INTERNACIONAIS
BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS

NÚCLEO SEGURANÇA INTERNACIONAL
GRUPO DE ANÁLISE DE SEGURANÇA CIBERNÉTICA (GRUPO CYBER)

INTERNATIONAL SECURITY PROGRAM
CYBERSECURITY ANALYSIS GROUP

A SEGURANÇA CIBERNÉTICA E A TECNOLOGIA 5G NO CENÁRIO BRASILEIRO

CYBERSECURITY AND 5G TECHNOLOGY IN THE BRAZILIAN SCENARIO

PENSAR
DIALOGAR
DISSEMINAR
INFLUENCIAR

#2 *Think tank* da América do Sul e Central

University of Pennsylvania's Think Tanks and Civil Societies Program 2019 Global Go To Think Tank Index Report

THINKING
DIALOGUING
DISSEMINATING
INFLUENCING

#2 Think tank in South and Central America

University of Pennsylvania's Think Tanks and Civil Societies Program 2019 Global Go To Think Tank Index Report

---

O Centro Brasileiro de Relações Internacionais (CEBRI) é um *think tank* independente, que contribui para a construção da agenda internacional do Brasil. Há mais de vinte anos, a instituição se dedica à promoção do debate plural e propositivo sobre o cenário internacional e a política externa brasileira.

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

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

The Brazilian Center for International Relations (CEBRI) is an independent think tank that contributes to building an international agenda for Brazil. For over twenty years, the institution has engaged in promoting a pluralistic and proposal-oriented debate on the international landscape and Brazilian foreign policy.

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

It is a non-profit institution, headquartered in Rio de Janeiro and internationally recognized. Today, its circa 100 associates represent diverse interests and economic sectors and mobilize a worldwide network of professionals and organizations. Moreover, CEBRI has an active Board of Trustees composed of prominent members from Brazilian society.

www.cebri.org

CENTRO BRASILEIRO DE RELAÇÕES INTERNACIONAIS
Rua Marquês de São Vicente, 336 – Gávea – Rio de Janeiro / RJ - CEP: 22451-044
Tel + 55 21 2206-4400 - cebri@cebri.org.br - www.cebri.org

CENTRO BRASILEIRO DE RELAÇÕES INTERNACIONAIS
BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS

NÚCLEO SEGURANÇA INTERNACIONAL
GRUPO DE ANÁLISE DE SEGURANÇA CIBERNÉTICA (GRUPO CYBER)

INTERNATIONAL SECURITY PROGRAM
CYBERSECURITY ANALYSIS GROUP

POLICY PAPER
DEZEMBRO 2020 / *DECEMBER 2020*

A SEGURANÇA CIBERNÉTICA E A TECNOLOGIA 5G NO CENÁRIO BRASILEIRO

CYBERSECURITY AND 5G TECHNOLOGY IN THE BRAZILIAN SCENARIO

PARCERIA/ *PARTNERSHIP*: SIEMENS SIEMENS energy

AUTOR
AUTHOR

Paulo Sergio Melo de Carvalho

Senior Fellow do Núcleo Segurança Internacional do CEBRI e General de Divisão da Reserva do Exército Brasileiro

Senior Fellow of CEBRI's International Security Program and Reserve Major General in the Brazilian Army

COORDENAÇÃO EDITORIAL
EDITORIAL COORDINATION

Julia Dias Leite
Diretora-Presidente do CEBRI
CEBRI CEO

Luciana Gama Muniz
Diretora de Projetos do CEBRI
Project Director at CEBRI

Cintia Hoskinson
Consultora de Projetos do CEBRI
Project Consultant at CEBRI

APOIO EDITORIAL
EDITORIAL SUPPORT

Carlos Arthur Ortenblad Jr.

Gustavo Berlie

Larissa Vejarano

TRADUÇÃO PORTUGUÊS-INGLÊS
PORTUGUESE-ENGLISH TRANSLATION

Leslie Sasson Cohen

DIAGRAMAÇÃO
GRAPHIC DESIGN

Presto Design

NÚCLEO SEGURANÇA INTERNACIONAL

GRUPO DE ANÁLISE DE SEGURANÇA CIBERNÉTICA

O Núcleo Segurança Internacional possui como objetivo principal engajar os setores público e privado, a academia e a sociedade civil em um debate plural sobre temas de segurança internacional e defesa através da produção de publicações e da promoção de debates abertos, *webinars* e debates fechados em formato Chatham House.

O Grupo de Análise de Segurança Cibernética (Grupo Cyber) é desenvolvido no âmbito do Núcleo Segurança Internacional e tem como foco discutir e aprofundar o conhecimento sobre temas estratégicos e contemporâneos relacionados às questões de cibersegurança, tais como: o alinhamento de diferentes abordagens de governança cibernética e resiliência cibernética; regulação e prevenção de conflitos no espaço cibernético; a importância da rede 5G e os riscos relacionados à tecnologia; o impacto do 5G na economia brasileira e na competitividade das indústrias no Brasil; 5G como elemento propulsor da inserção internacional do Brasil no cenário digital global; a crescente migração do multilateralismo para o espaço cibernético e oportunidade para atuação da ONU nesse âmbito.

CONSELHEIRO

André Clark

André Clark é General Manager da Siemens Energy Brasil, tendo sido anteriormente Presidente e CEO da Siemens no Brasil e também CEO da ACCIONA para o Brasil, Bolívia, Uruguai e Paraguai. É formado em Engenharia Química pela Universidade de São Paulo (USP) e possui MBA em Finanças e Gestão de Operações pela Stern School of Business, da Universidade de Nova Iorque. Além disso, hoje também é: Vice-presidente do Conselho Administrativo e Coordenador do Comitê da Indústria da Associação Brasileira de Infraestrutura e Indústrias de Base (ABDIB); Vice-presidente da Diretoria Plenária da Associação Brasileira de Máquinas e Equipamentos (ABIMAQ); Membro do Conselho Empresarial do grupo formado por Brasil, Rússia, Índia, China e África do Sul (BRICS); Membro do Comitê de Líderes da Confederação Nacional da Indústria e do Comitê de Líderes da Mobilização Empresarial pela Inovação (CNI/MEI); Membro do Conselho Curador e coordenador do Núcleo Infraestrutura e do Núcleo Segurança Internacional (CEBRI); Membro do Conselho Consultivo do GRI Club Brasil; Membro do Conselho Superior da Câmara Internacional do Comércio (ICC); Membro da Diretoria e Presidente do Conselho de Transformação Digital do Instituto Brasileiro de Petróleo, Gás e Biocombustíveis (IBP); e Diretor do Conselho Empresarial Brasil-China (CEBC).

SENIOR FELLOW

Paulo Sergio Melo de Carvalho

General de Divisão da Reserva do Exército Brasileiro, especialista em Tecnologia da Informação e Comunicações, com atuação na área de Cibernética nos níveis político-estratégico e operacional-técnico, tendo chefiado o Centro de Defesa Cibernética, de 2014 a 2016, e sendo o primeiro comandante do Comando de Defesa Cibernética, criado em 2016. Atualmente, presta consultoria no setor cibernético e participa na capacitação de recursos humanos, no Brasil e no exterior.

DIRETORA-PRESIDENTE

Julia Dias Leite

Diretora-Presidente do CEBRI. Atua há 20 anos na área de Relações Internacionais. Ocupou cargos de direção nas principais instituições independentes do setor no Brasil e desenvolveu relacionamento com representantes da iniciativa privada, governos e entidades oficiais nacionais e no exterior, em especial da América do Sul, Estados Unidos e Ásia. Dentre elas, foi Secretária Executiva do Conselho Empresarial Brasil-China (CEBC). Formada em Direito pela Universidade Cândido Mendes e com MBA em Gestão de Negócios pela FGV, colaborou na área de pesquisas com o Council of the Americas, em Nova York. É *Fellow* do Inter-American Dialogue e, em 2017, foi a representante brasileira no International Visitor Leadership Program, do Departamento de Estado americano. É Presidente do Conselho de Administração da Piemonte Holding.

INTERNATIONAL SECURITY PROGRAM

CYBERSECURITY ANALYSIS GROUP

The International Security Program's main objective is to engage the public and private sectors, the academia and civil society in a plural debate on international security and defense issues through the production of publications and the promotion of open debates, webinars and closed meetings in the Chatham House format.

The Cybersecurity Analysis Group (Cyber Group) is developed within the scope of the International Security Program and focuses on discussing and deepening knowledge on strategic and contemporary topics related to cybersecurity issues, such as: the alignment of different cyber governance approaches and cyber resilience; regulation and prevention of conflicts in cyberspace; the importance of the 5G network and the risks related to this technology; the impact of 5G on the Brazilian economy and on the competitiveness of companies in Brazil; 5G as a driving force for Brazil's international insertion in the global digital scene; multilateralism's increasing migration to cyber space and an opportunity for the UN to act in this area.

TRUSTEE

André Clark

André Clark is General Manager at Siemens Energy Brazil. Previously he was President and CEO of Siemens in Brazil, and CEO of ACCIONA to Brazil, Bolivia, Uruguay and Paraguay. He holds a degree in Chemical Engineering from the University of São Paulo (USP) and an MBA in Finance and Operations Management from the Stern School of Business, New York University. Currently, he is also: Vice-President of the Administrative Council and Coordinator of the Industry Committee of the Brazilian Association of Infrastructure and Basic Industries (ABDIB); Vice-president of the Plenary Board of the Brazilian Association of Machinery and Equipment (ABIMAQ); Member of the Business Council of the group formed by Brazil, Russia, India, China, and South Africa (BRICS); Member of the Leaders Committee of the Brazilian National Confederation of Industry and the Leaders Committee of the Business Mobilization for Innovation (CNI/MEI); Member of the Board of Trustees and coordinator of the Infrastructure Program and the International Security Program at CEBRI; Member of the Advisory Board of GRI Club Brazil; Member of the Superior Council of the International Chamber of Commerce (ICC); Member of the Board and President of the Digital Transformation Council of the Brazilian Petroleum, Gas and Biofuels Institute (IBP); and Director of the Brazil-China Business Council (CEBC).

SENIOR FELLOW

Paulo Sergio Melo de Carvalho

Reserve Major General in the Brazilian Army, he is a specialist in Information and Communications Technology who works in the area of Cybernetics at the political-strategic and operational-technical levels. From 2014 to 2016, he was head of the Cyber Defense Center, and was the first commander of the Brazilian Army's Cyber Defense Command, created in 2016. Currently, he is a consultant in the cyber sector and participates in capacity building and training activities, in Brazil and abroad.

CEO

Julia Dias Leite

Julia Dias Leite is CEBRI CEO. She has been working in the field of International Relations for twenty years. She held management positions in the sector's main independent institutions in Brazil and developed a relationship with representatives of the private sector, governments, and official bodies in Brazil and abroad, especially in South America, the United States and Asia. She was also Executive Secretary of the Brazil-China Business Council (CEBC). She holds a law degree from Cândido Mendes University and an MBA in Business Management from FGV. She collaborated in the research area with the Council of the Americas, in New York. She is a Fellow of the Inter-American Dialogue and, in 2017, she was the Brazilian representative in the US State Department's International Visitor Leadership Program. She is the Chairperson of the Board of Directors of Piemonte Holding.

PORTUGUÊS

A SEGURANÇA CIBERNÉTICA E A TECNOLOGIA 5G NO CENÁRIO BRASILEIRO

ENGLISH

CYBERSECURITY AND 5G TECHNOLOGY IN THE BRAZILIAN SCENARIO

1 A importância da Tecnologia 5G

A atualidade se mostra cada vez mais dependente do mundo digital. A grande maioria dos indivíduos utiliza-se de tecnologias digitais para desempenhar diversas atividades diariamente. O uso destas aumentou significativamente no mundo todo desde a eclosão da COVID-19, em decorrência da disseminação do trabalho remoto e dos serviços digitais que se intensificam para minimizar as limitações impostas pela pandemia.

Embora o aumento do uso de tais tecnologias e serviços tenha gerado grande aproximação interpessoal no mundo virtual, também facilitou a dinamização de ataques cibernéticos. Portanto, todos os Estados-Nação precisam dedicar especial atenção à proteção de seus ativos de informação, sejam públicos ou privados. As empresas, buscando garantir uma ampliação digital segura para seus negócios e seus consumidores, também consideram os investimentos em tecnologia da informação e comunicações como estratégicos para atuar no mundo de hoje.

No Brasil, onde a população no geral tem utilizado cada vez mais a Internet e as redes sociais, os órgãos governamentais e as empresas públicas têm buscado soluções de proteção das redes de dados, particularmente no que tange ao trânsito da informação entre o mundo corporativo e os consumidores.

Atualmente, o mundo vive uma revolução sem precedentes, com a chegada da tecnologia 5G na área de telecomunicações, a qual deverá mudar todo o modo como trabalhamos e vivemos: de um ambiente onde o uso da tecnologia celu-

lar é utilizada, quase que exclusivamente, para trocar mensagens entre humanos, chegaremos a uma nova realidade, com a interação de bilhões de artefatos conversando entre si e formando uma malha digital para um mundo plenamente conectado.

A disrupção tecnológica com a chegada da tecnologia 5G ocorrerá em três aspectos principais:

a) aumento do potencial de banda para aplicações, chegando de uma a duas ordens de magnitude maior que a tecnologia 4G do Brasil, onde câmeras de segurança pública de alta definição poderão ser usadas para capturar detalhes do rosto de pessoas ou vídeos de realidade virtual e aumentada, bem como poderão ser sobrepostas em tempo real para auxiliar em operações nas fábricas, por exemplo;

b) queda da latência em uma ordem de grandeza, permitindo tempo de resposta instantâneo, exemplificando: pode-se solicitar a um carro autônomo que pare em nanosegundos; e

c) incremento em duas ordens de magnitude do número de dispositivos conectados simultaneamente, possibilitando, entre outros casos, que milhares de sistemas de controle industrial possam trabalhar em completa coordenação por meio sem fio.

O impacto da tecnologia 5G para a sociedade, em um período de 10 a 25 anos, será muito amplo, porque os modelos de negócios serão readaptados para um padrão de otimização e engenharia, e poderão ser imensamente automatizados.

Portanto, processos de gerência de produção, transporte e logística serão coordenados por Inteligência Artificial e teremos robôs industriais trabalhando como orquestras, grades inteligentes de energia, medicina personalizada e doméstica, e mineração por controle remoto.

As cidades inteligentes poderão fornecer serviços de controle de espaço terrestre e aéreo para veículos autônomos para entregas, bem como a segurança pública terá melhor capacidade de investigação e controle. Entretanto, tudo isso envolve riscos devido ao fato de a arquitetura das redes ser centralizada nas operadoras, ao aumento do poder de processamento na borda da rede e, principalmente, ao aumento do número de antenas e uso de redes definidas por *software* em 5G, o que aumentará exponencialmente a superfície de atacantes.

Em um tempo recente, no Brasil, quando a segurança cibernética foi necessária no contexto dos chamados grandes eventos (Copa do Mundo e Olimpíadas), o

ambiente nacional cibernético ainda era precário e com pouco compartilhamento mútuo entre as agências governamentais e reduzido espaço de atuação das empresas privadas, mas o ambiente hoje já é bem mais conectado.

Por exemplo, em tempos de pandemia de COVID-19, multiplicam-se os ataques de *ransomware*[1], onde o sequestro dos dados pode afetar o desempenho das empresas e instituições [1]. No cenário da tecnologia 5G, essas ameaças são potencializadas pela quantidade maior de dispositivos e pela automatização de fluxos e processos entre sistemas ciberfísicos.

É muito mais impactante um ataque de *ransomware* a uma estação de energia elétrica, o qual pode deixar os cidadãos sem energia durante dias, do que um ataque visando apagar ou destruir informações de um banco de dados de uma empresa no mercado, por exemplo.

Uma vantagem do ponto de vista da tecnologia 5G é que ela foi projetada e padronizada com a mentalidade de "segurança na concepção". Ou seja, os protocolos, a camada física e a camada de enlace[2] já pressupõem modelos de ameaças mais avançados do que aquele simples, sem formalismos, quando do começo da arquitetura da Internet. Então, muitos mecanismos estão presentes para garantir uma comunicação em nível de enlace e aplicação com a rede móvel, de maneira adequada e com autenticação e criptografia forte. Mas, ainda assim, é preciso supervisionar a implantação de projetos de tecnologia 5G para assegurar que todos esses recursos serão habilitados.

No Brasil, as normas regulatórias de segurança cibernética, até o momento, não são impositivas, mas, com o advento da tecnologia 5G e de uma sociedade mais avançada, conectada em maior banda e baixa latência[3] e com milhares de dispositivos de controles industriais e veículos autônomos, é estratégico preservar a soberania nacional, do ponto de vista de entendimento das tecnologias e seus riscos.

De fato, o ambiente cibernético internacional tem se tornado mais militarizado, com a crescente presença de ameaças avançadas persistentes (em inglês, APT) que podem ser desenvolvidas por Estados-Nação. Esse cenário muda para uma

---

1. O *ransomware* é uma forma de *malware* (*software* concebido para causar danos a um único computador, servidor, ou rede informática) que codifica os arquivos da vítima. O invasor exige, então, um pedido de resgate, "*ransom*", para restabelecer o acesso aos dados mediante pagamento que, geralmente, é feito em Bitcoins. (CSO - United States).

2. Trata-se de uma das sete camadas do modelo OSI (modelo de rede de computador referência da ISO, que é dividido em camadas de funções). Seu objetivo básico é assegurar a transferência confiável de dados entre sistemas conectados diretamente por um meio físico.

3. Latência se refere ao tempo que um pacote de dados leva para ir de um ponto designado para o outro. Baixa latência é sinônimo de atraso.

maior interação entre os entes público (civil e militar) com um pacto profundo de compartilhamento de informações e a consequente responsabilização dos entes envolvidos em ações maliciosas.

É sabido, ainda, que o atual cenário imposto pela pandemia da COVID-19 provocou uma alteração na forma de trabalho em todo o mundo. Esta nova realidade traz novos desafios para os órgãos e empresas, sejam públicos ou privados. No setor de Tecnologia da Informação (TI), dentre os desafios, está a definição de políticas e meios para manter os equipamentos seguros e para proteger o acesso às redes corporativas, considerando-se o número crescente de dispositivos que estão fora do perímetro de segurança da rede e que precisam acessá-la.

Nesse contexto, reveste-se de maior relevância a implementação de políticas efetivas para a segurança cibernética, uma vez que, para a manutenção dos serviços públicos e privados, os colaboradores, em muitos casos, acessam as redes corporativas de forma remota. Sendo assim, devem ser estabelecidas políticas de acesso seguro e implementadas soluções para garantir a segurança das redes, onde estarão inseridas as de tecnologia 5G, sejam públicas ou privadas.

Assim, será abordado o papel do Brasil nesse cenário de segurança cibernética na tecnologia 5G, discorrendo sobre os principais desafios e oportunidades que aparecerão, a posição atual do Brasil em relação a essas questões, e os caminhos que entendemos serem importantes para o país se inserir e planejar uma agenda de tecnologia 5G positiva. Em conclusão, serão recomendadas ações de políticas públicas em nível de Estado, de longo prazo, para termos melhor êxito nessa futura sociedade digital.

2 Oportunidades e Desafios

A rede 5G, do ponto de vista tecnológico, traz surpreendentes avanços em tecnologias de comunicação de rádio com taxas altas, em frequências de espectro de 3.7 GHz por exemplo, que necessitam de células menores e, portanto, possuem maior multiplexação espacial.

Adicionalmente, a rede 5G traz a criação de uma maior capacidade computacional acoplada à rede, com os ambientes de computação em nuvem na sua borda. Tudo isso traz grandes oportunidades de novas aplicações no Brasil.

Inicialmente, serão abordadas as oportunidades e o lado benéfico das tecnologias e, em seguida, os desafios e impeditivos, com foco em segurança.

A. OPORTUNIDADES

Um candidato natural dessas novas aplicações é o agronegócio, que hoje faz uso de comunicação via satélite, de controle refinado para agricultura de precisão e de maquinário agrícola altamente sofisticado. Portanto, naturalmente, aplicações de redes 5G possuem grande potencial de utilização neste ambiente.

As mineradoras brasileiras, como Vale, Petrobras e Votorantim, também possuem essa tendência de eliminar riscos humanos, substituindo suas frotas de grandes caminhões por veículos autônomos e trocando humanos por robôs nas minas e nos trabalhos de perfuração, especialmente se o ambiente apresentar condições inóspitas.

Contudo, existem muitas outras possíveis utilizações. O parque industrial brasileiro é o maior do Hemisfério Sul e tem uma janela grande de oportunidades com o advento da tecnologia 5G no ambiente fabril, chamado Indústria 4.0. A janela de oportunidade para diferencial em tecnologia de 5G será de, no máximo, três anos [2]. Depois, a maioria das empresas já estará empregando a tecnologia em alguma medida, tornando-a comoditizada.

As indústrias poderão ser automatizadas e os dados das máquinas, sensores, controladores e atuadores serão transferidos em alta velocidade e em tempo

real via tecnologia 5G, permitindo a orquestração completa do ciclo de fabricação de produtos.

Nessa área existe oportunidade especial nas chamadas redes privadas 5G, ou redes privativas 5G. Trata-se de redes que são controladas por empresas, com completo isolamento do tráfego dos registros dos sensores do ambiente externo.

Essas redes privativas podem ser criadas e gerenciadas por grandes empresas, como é o caso atual da Vale e da Eletrobras, mas é necessária uma alocação de espectro específica para essa aplicação. Na Alemanha, a faixa espectral alocada é entre 3.7 e 3.8 GHz, com faixas de 100 MHz por projeto, fornecendo alta vazão e conectividade ampla de dispositivos.

No Brasil, já existem decisões da agência reguladora ANATEL para liberar faixa de 30 MHz na frequência de 1.5 GHz, mas o assunto ainda não está completamente regulamentado. Existe também a possibilidade de oportunidades de outros modelos de negócio, onde a operadora aluga suas antenas 5G para as aplicações industriais através de tecnologias de fatiamento de rede. Esse modelo pode ter melhor desempenho e menor necessidade de gasto inicial da empresa, pois os custos de compra das estações rádio base de 5G e, também, a qualificação de pessoal técnico operacional para manter a rede em funcionamento podem ser proibitivos.

O fatiamento de rede [3] pode ser a maneira de lidar com a tecnologia 5G na Indústria 4.0 em regiões de alta conectividade e uma forma das operadoras diminuírem o tempo do retorno de investimento. Entretanto, para áreas remotas e isoladas do Brasil, a necessidade implica ter uma rede 5G própria, onde a janela de oportunidades possa favorecer investimentos por uma grande empresa de maneira solitária, ou de maneira cooperativa por um conjunto de empresas.

Aqui, pode-se somar a oportunidade de regionalização de soluções 5G, pois, não tendo rede elétrica abundante em certas regiões do Brasil, como no estado do Amapá, as estações rádio base regionalizadas precisarão fazer uso de energia solar, conexão por satélite ou mesmo uso de rede de fibra óptica subfluvial em rios amazônicos e na região do Pantanal. Tais regionalizações favorecem a indústria nacional em certos aspectos tecnológicos que empresas brasileiras já dominam no alcance a essas regiões.

Outro panorama de oportunidade é no âmbito das cidades inteligentes. A partir de 2010, houve investimento nacional na criação de redes de fibra óptica metropolitanas em cidades de pequeno e médio porte no Brasil. Esse investimento era parte de um Programa Nacional de Banda Larga (PNBL) [4]. Porém, muitas dessas implantações não atingiram o seu potencial transformador, muitas vezes, em

função de baixa cobertura nas cidades. O problema da última malha envolvia a passagem de fibras ópticas adicionais até o anel metropolitano de fibra, e a integração entre os sistemas das cidades ainda estava em sua infância. Passados 10 anos, temos um ambiente mais propício, com soluções tecnológicas de cidades inteligentes, onde os sistemas de saúde e de segurança pública, e os centros de controle das cidades podem se organizar melhor, e o uso de redes 5G privativas pode ser uma grande oportunidade de alavancar essa transformação.

Redes 5G privativas baseadas em cidades inteligentes podem permitir uma enorme economia em áreas como sincronização de transporte público em tempo real, gerando economia de combustível, com sistemas de controle em laço retroalimentável, bem como na sincronização de serviços de saúde e em novas aplicações, tais como controle de tráfego aéreo e terrestre para drones de entrega de produtos, como, por exemplo, itens médicos de alta importância, como desfibriladores.

B. DESAFIOS

Apesar de todas as oportunidades interessantes que aparecem no uso da tecnologia 5G, existem também muitas incertezas, em especial na área de segurança cibernética. Iniciando-se pelo receio de espionagem internacional, passando pela sabotagem e até à guerra cibernética, um grande desafio em 5G é como manter a segurança nacional, com a exposição cada vez maior de sistemas ciberfísicos, em um contexto de desconfiança em relação a fornecedores.

Esse desafio terá que ser superado por uma série de ações de certificação que garantam uma ampla validação da segurança dos fornecedores e pela sua responsabilização por seus atos.

As implantações dos projetos de rede 5G, sejam eles públicos ou privativos, também irão precisar passar por uma padronização de redes seguras como requisito mínimo de conectividade com outras redes.

Ou seja, o desafio de padronização terá que ser feito por cooptação, por meio de regras de entrada mais rígidas, com padrões mínimos de configuração e recursos de segurança implantados para posterior participação. Um exemplo desse tipo de procedimento acontece nas redes acadêmicas americanas ligadas à Internet, que só recebem suporte financeiro da *National Science Foundation* (NSF) [5] em caso de altas condições de segurança. Outro excelente exemplo desse processo de uniformização de segurança é o projeto *EU Toolbox on 5G Cybersecurity* [6].

A recomendação europeia de segurança cibernética em 5G (*EU Toolbox on 5G Cybersecurity*) tenta criar regras rígidas entre países-membros da União Euro-

peia para minimizar riscos da implantação de redes 5G sem critérios fortes de segurança.

Isto ocorre devido à desconfiança de que essas redes, as quais serão o alicerce da sociedade digital do futuro, possam vir a ser um ponto de ataque por inimigos. Convém lembrar que a principal falha de segurança de uma rede sempre estará em seu elo mais fraco.

Assim sendo, os requisitos europeus passam por processos refinados de inspeção de segurança dos dispositivos, especialmente em relação aos produtos de rede 5G do núcleo, produtos de gerência de rede, produtos de orquestração de serviços e produtos das redes de acesso.

Adicionalmente, são exigidas medidas para aumentar a concorrência e diminuir a possibilidade de monopólio, por meio de regras para operadoras apresentarem, em suas redes, uma certa diversidade de equipamentos interoperáveis, e, finalmente, a recomendação também solicita aos países-membros uma forte regulamentação da parte de responsabilização em caso de vazamentos e espionagem.

Um outro desafio, mais relacionado com o Brasil, é que as operadoras de telecomunicações têm baixa capacidade de investimento em CAPEX, e a necessidade de aquisição de grande número de equipamentos 5G, devido a células menores, pode ser um desafio para uma implantação com sucesso no Brasil.

Além disso, regiões com grande deficiência de cobertura já em 4G, tenderão a ter lacunas também em 5G, e, portanto, o uso da cobertura 5G para a gerência de processos industriais nessas áreas pode ser problemático.

Por outro lado, conforme for executado o mapeamento das oportunidades acima, a popularização de redes privadas 5G pode aumentar essa cobertura, colocando outras empresas, por exemplo, provedores de Internet regionais ou locais, em áreas com baixa cobertura e investimentos privados dessas pequenas e médias empresas.

As fibras ópticas existentes de empresas elétricas, empresas de pedágio de estradas e outras, podem fazer o *backhaul*[4] de redes 5G privativas até as cidades inteligentes e, portanto, preencher a lacuna de cobertura apontada nesse desafio.

Do ponto de vista mais técnico, da tecnologia em si, existe desafio no tocante a monitorar esse novo tipo de rede. Tecnologias de fatiamento separam o tráfego e o es-

4. São infraestruturas das redes de telecomunicações de alta capacidade utilizadas na prestação de serviços de telecomunicações. Um *backhaul* é composto por equipamentos que se conectam aos *backbones* (as redes centrais da internet), localizados nas estações centrais das operadoras, por um equipamento instalado na área atendida e pela conexão entre eles. Essa conexão pode se dar por cabo de fibra ótica, rádio, satélite ou outras tecnologias.

pectro por cliente e, assim, muita informação fica perdida, pois a monitoração horizontal possível é realizada apenas no nível da fatia da rede definida por *software*.

Então, será necessário o desenvolvimento de tecnologias que permitam realizar uma monitoração mais vertical, indo mais fundo nas camadas de virtualização da rede, até o nível de bilhetagem e conectividade (sinais de rádio). Existem algumas iniciativas para lidar com esse desafio, como o *Network Data Analytics Functions* (NMDAF) [7], mas muito mais precisa ser feito.

Finalmente, a área de privacidade dos dados é um importante desafio em 5G: com o grande volume de dados à disposição e a necessidade de armazenar os dados por longo prazo, ela torna-se um alvo para sequestradores de dados. Mesmo com a nova legislação brasileira da Lei Geral de Proteção de Dados Pessoais (LGPD), é preciso acoplar a segurança do sistema 5G também à proteção dos dados dos usuários, via responsabilização.

A gestão de segurança do 5G tem que ser bem realizada e o nível de conscientização da segurança cibernética, nesse contexto, tem que aumentar, para evitar ataques nesses sistemas de operadoras considerados críticos. Existem algumas iniciativas que elencam princípios para evitar ataques em infraestrutura crítica, como as discutidas no âmbito do *Paris Call* [8].

3 O Brasil na discussão da Tecnologia 5G e sua segurança

Infelizmente, o Brasil se encontra em situação de atraso no desenvolvimento da tecnologia 5G e também na representatividade de sua padronização. No âmbito da academia, temos poucas pesquisas relevantes e patentes nas áreas de ondas milimétricas ou rádios com maciça quantidade de antenas (MIMOs) para esse tipo de aplicação, destacando-se, neste quesito, apenas poucos institutos de pesquisa.

Alguns desenvolvimentos relevantes em pesquisa e inovação se sobressaem, em especial na área de fatiamento de redes (*slicing*), como o Projeto EU-Brasil NECOS (*Novel Enablers for Cloud Slicing*) [9]. Mesmo essas pesquisas não geram muitos resultados práticos, por falta de um incentivo à geração de empresas de ponta, nessa área altamente competitiva.

Nossa atuante indústria nacional de equipamentos de redes é mais forte em redes ópticas e redes cabeadas, merecendo destaque as empresas Padtec e Datacom, respectivamente. Existem algumas iniciativas isoladas, porém a maioria dos produtos de redes móveis, utilizados nas operadoras e outras empresas brasileiras, são estrangeiros. O Brasil acabou mais como receptor da tecnologia 5G do exterior, a saber, de empresas de outros países como a Suécia (Ericsson), Finlândia (Nokia), China (Huawei) ou Coreia do Sul (Samsung).

Com essa perspectiva tecnológica, restou ao Brasil trabalhar para entender a tecnologia a partir de parcerias com essas empresas estrangeiras que já atuam no país e realizar provas de conceito em redes 5G privadas e testes em laboratório, bem como trabalhar para melhorar a maturidade de validação das tecnologias.

Por outro lado, no espectro de segurança cibernética na tecnologia 5G, a preocupação da alta gestão nacional está em nível elevado. Como já foi mencionado, trata-se da tecnologia para viabilizar a sociedade digital do futuro, então é preciso se precaver apropriadamente. Além disso, há a discussão geopolítica de alinhamento entre países. Enfim, nesse sentido, vários decretos e normatizações têm sido apresentados, ao longo do último ano, com o objetivo de conferir segurança a essa transição para a tecnologia 5G.

Do ponto de vista da normatização de segurança, o governo federal emitiu o Decreto N. 10.222, em 5 de fevereiro de 2020, da Estratégia Nacional de Segurança Cibernética [10], que traz diretrizes para todo o sistema de gestão administrativo federal sobre como lidar com segurança cibernética, e qual é a nossa estratégia para ficarmos mais fortes nessa área, como país.

Esta estratégia orienta os órgãos, públicos e privados, para um acompanhamento técnico permanente, pela relevância do tema, e constantes evoluções tecnológicas na área de segurança cibernética. Trata-se de um arcabouço legal que não existia e que permite mostrar o aumento da conscientização do problema de segurança cibernética e incrementar mecanismos de acompanhamento e responsabilização por delitos.

No âmbito específico da tecnologia 5G, destaca-se também um documento publicado pelo Gabinete de Segurança Institucional ligado à Presidência da República, a Instrução Normativa N° 4, que dispõe sobre os requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G [11].

Tem especial atenção a questão de possíveis vulnerabilidades e *backdoors* existentes em equipamentos, que, se implementados tanto de maneira intencional quanto involuntária, podem comprometer a segurança dos sistemas de comunicações nacionais.

É importante destacar o mecanismo de auditoria citado no documento que deve ser executado mensalmente pelas operadoras, as quais devem informar a versão de equipamento de *hardware* e as versões de *software*, com o intuito de que auditorias de segurança possam constantemente monitorar essa superfície de ataque.

Finalmente, alinhada a essas normatizações de Estado, a ANATEL, agência reguladora de telecomunicações, realizou as consultas públicas 6/2020, 11/2020 e 12/2020 em aspectos que abordam o 5G do ponto de vista de certificação de equipamentos e uma, em especial, sobre cibersegurança, a 13/2020 [12].

Essa consulta trata dos requisitos mínimos de segurança, de modo a diminuir a possibilidade de vulnerabilidades, por meio de atualizações de *software/firmware* e também por recomendações sobre melhores práticas em configurações e na gerência remota.

Outros aspectos relevantes da regulamentação da ANATEL consistem em sugerir quais os métodos criptográficos mais adequados para transmissão de dados e em repouso, bem como estabelecer, para fornecedores de equipamentos, uma política clara de suporte ao produto, de responsabilização nas atualizações e correções

de vulnerabilidades assim que surgirem, e, ainda, de prover atualizações de segurança em tempo real por, no mínimo, dois anos.

No ambiente de outra infraestrutura crítica, o setor elétrico, a ANEEL, agência reguladora de energia, tem trabalhado com discussões em *workshops* e *white papers*, para advogar arquiteturas de redes mais seguras com defesa em profundidade, até os elementos ciberfísicos como transformadores e outros controles. Nesse sentido, o movimento do Brasil foi na criação de um centro de troca de informações de incidentes específico em relação a sistemas de controle industriais, o ICS-CERT.

A ANATEL e a ANEEL têm realizado colaborações para que seja flexibilizado o uso de postes elétricos para posicionamento de fibras ópticas, devido ao aumento exponencial de tráfego de redes que a rede 5G propiciará, bem como permitirão que as redes privadas 5G possam utilizar esses recursos de postes já instalados, ao invés de terem que implantar novas fibras ópticas subterrâneas.

4 Caminhos para o Brasil se inserir no contexto da Tecnologia 5G

Considerando-se o fato de o Brasil ter se iniciado lentamente na implantação da geração 5G, por exemplo, já existem países com a tecnologia em produção. Além disso, não tivemos os desenvolvimentos tecnológicos *in-house* como alguns países europeus. Dessa forma, precisamos, para nos inserir nesse contexto do 5G, aumentar, de maneira rápida, a quantidade de técnicos e engenheiros capacitados na nova tecnologia.

Existem algumas iniciativas do setor industrial CNI, via SENAI, em cursos de capacitação, impulsionados pela transformação da Indústria 4.0. Existem também empreendimentos de cursos de formação em nível de pós-graduação em várias universidades brasileiras, como a Escola Politécnica da Universidade de São Paulo (Poli-USP) e o Instituto Nacional de Telecomunicações (Inatel). Entretanto, a demanda tenderá a aumentar ainda mais.

Como a rede 5G, do lado da segurança cibernética, é essencialmente um problema tecnológico equivalente à segurança computacional convencional, convém reforçar um caminho de formação de profissionais de segurança cibernética com melhor qualidade no Brasil.

Embora no Brasil existam muitos cursos em formação de segurança cibernética, em geral, a experiência tem demonstrado, quando são apresentados problemas críticos de segurança, que a formação que eles oferecem ainda precisa ser aprimorada. A pandemia da COVID-19 e a popularização de cursos on-line pelas universidades brasileiras podem trazer um benefício de maior oferta de cursos de melhor qualidade e menor custo para os brasileiros.

Outro aspecto importante para o Brasil se inserir e ficar melhor protegido utilizando as tecnologias 5G, do ponto de vista da segurança cibernética, é aumentar fortemente o compartilhamento de informações entre empresas, instituições públicas e centros de pesquisa. O compartilhamento pode ser automatizado por uma infraestrutura de indicadores de comprometimento (os chamados IoCs), que poderão ser feitos mais setorialmente, no futuro.

No momento, existe no Brasil uma tradição de compartilhamento de informações, devido ao fato de a Internet brasileira ter sido influenciada pelo Comitê Gestor da Internet no Brasil, em que o *CERT.br* atua como ponto central em tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet no Brasil, provendo coordenação e apoio, fazendo os contatos para escalonar incidentes.

Porém, as organizações de grupos maliciosos estrangeiros se encontram na Internet para trocar informações úteis e fornecer todo um mercado negro de acessos clandestinos, dados roubados e vulnerabilidade *zero-day*, o que implica a necessidade de aumentar consideravelmente a colaboração entre empresas e instituições dos setores público e privado no Brasil.

Um caminho a ser seguido é o uso de uma plataforma MISP (*Open Source Threat Intelligence Platform*) [13], que facilita o compartilhamento automático, bem como o fortalecimento de maior número de centros especializados em tratamento e resposta de incidentes, como o Comando de Defesa Cibernética (*ComDCiber*) e o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (*CTIR.Gov*).

Esses centros poderiam adotar um modelo parecido com a *Cybersecurity and Infrastructure Security Agency* (CISA) norte-americana, com exportação e enriquecimento automático de incidentes, com novos indicadores de comprometimento em tempo real, através da plataforma *Trusted Automated eXchange of Indicator Information* (TAXII). O caminho para o Brasil é estabelecer o equivalente ao controle do espaço aéreo, garantindo a supervisão no âmbito do espaço cibernético nacional em prol da soberania nacional.

As agências reguladoras ANATEL e ANEEL já têm certificações de segurança há alguns anos, no sentido de *safety*, em inglês, para certificar que a segurança da parte elétrica e da parte de irradiação eletromagnética de rádio estejam dentro de parâmetros de normalidade de segurança para os humanos que operam e usam o sistema. Entretanto, as supracitadas agências reguladoras precisam urgentemente instituir critérios e procedimentos de certificação mais rigorosos para a avaliação de riscos em segurança cibernética.

Os procedimentos de certificação terão que fazer uso de artifícios como *pentest* de produtos, avaliação de riscos de recursos e mesmo conformidade da equipe de desenvolvimento para que ela seja extremamente segura, use programação de qualidade, empregue bibliotecas de desenvolvimento atualizadas e trabalhe também com as melhores práticas de arquiteturas de *software* seguras.

Os equipamentos e redes definidas por *software* das redes 5G vão exigir grande esforço de certificação, para que a superfície de ataque, embora ampliada, seja mais robusta a ataques maliciosos.

Do ponto de vista da responsabilização por violações, o Brasil precisa ainda aprimorar a legislação e fazer com que as penas sejam mais pesadas, para que os *hackers* do mal sejam devidamente punidos.

Nessa área, a ANATEL tem a intenção de criar uma espécie de avaliação de mercado, onde os equipamentos e as cadeias de produtos envolvidos em 5G serão avaliados por meio de testes de segurança e, caso confirmados os vazamentos ou se as vulnerabilidades forem deixadas sem tratamento, eles serão excluídos imediatamente do rol de produtos à venda no Brasil.

Nesse ponto, a agência reguladora poderia ser mais incisiva, e não só proibir a venda, como também exigir o *recall* do produto imediatamente, como acontece com produtos defeituosos em veículos que podem levar à morte de usuários. Um equipamento de rede com vulnerabilidade conhecida, deixado sem responsabilização, é como um caminhão com pneu sem condições de rodagem, é preciso tirá-lo de circulação imediatamente para não ferir ninguém.

Também é necessário definir melhor os meios de inferir quais as reais responsabilidades nas cadeias de fornecedores que fazem os produtos, pois os itens de 5G são altamente complexos, e exigem peças e componentes de dezenas de fornecedores. Inserir um elemento de *hardware* malicioso que permita o sequestro do equipamento pode ser extremamente furtivo.

A rastreabilidade e o ranqueamento de risco dos fornecedores são importantes para aumentar o grau de segurança dos produtos que estão sendo implantados no Brasil. Para os setores de infraestrutura crítica, em especial, isso é mais que desejável, é mandatório.

No projeto *EU Toolbox on 5G Cybersecurity* [6] existe um levantamento completo dos provedores da cadeia de fornecimento de 5G, e há uma determinação de diminuir os monopólios através da diversificação de fornecedores, bem como é exigida uma maior responsabilização das operadoras de telecomunicações e infraestruturas críticas para obter certificações de qualidade em segurança.

Um dos exemplos do Brasil é a empresa Petrobras ter atingido um patamar maior de resposta a incidentes através da participação da organização *Forum of Incident Response and Security Teams* (FIRST) [14], na qual, para participar como membro, é preciso obter vários certificados e mostrar a melhoria da qualidade em pata-

mares elevados em segurança cibernética. Este deveria ser o caminho normal em todas as infraestruturas críticas do Brasil.

Do ponto de vista de pesquisa e desenvolvimento no Brasil, como o país não esteve tão atuante no desenvolvimento das tecnologias envolvidas no 5G, o caminho a ser seguido é começar a fomentar prospecção tecnológica na tecnologia 6G. Deve-se estabelecer novas parcerias com as multinacionais, para desenvolvimento conjunto das próximas gerações de produtos 6G com inteligência artificial, uso de *blockchain*, computação e rede de comunicações quântica, e segurança cibernética de ponta, para que os centros de pesquisa, desenvolvimento e inovação brasileiros estejam melhor preparados para as futuras versões da infraestrutura crítica de comunicação homem a homem e máquina a máquina.

5 Recomendações de Políticas Públicas

Na finalização deste *paper* de política para segurança cibernética em tecnologia 5G, são apresentadas sugestões de recomendação para curto e longo prazos em termos de políticas de Estado a serem implementadas no Brasil.

Um tema relevante é a baixa capacidade de investimento das empresas operadoras de telecomunicações brasileiras e a necessidade da completa substituição da rede 3G/4G por um número muito maior de antenas da rede 5G. É preciso tratar isso com criatividade, porque corre-se o risco de o leilão público da tecnologia 5G ocorrer e a rede não ser implantada na velocidade necessária às exigências do país.

Um modelo possível é abrir a possibilidade de redes privadas com CAPEX próprio, que podem ser implementadas por grandes empresas mineradoras, grandes indústrias e agronegócio, as quais conseguiriam absorver os custos operacionais e a operação da rede 5G. Existe uma vontade da indústria brasileira de se modernizar para a versão 4.0 e ela pode possuir mais recursos para adquirir antenas e atender à sua demanda, especialmente em lugares isolados.

Para outras empresas, médias e pequenas, o modelo de aluguel de *slicing* 5G pode ser mais atrativo, seja por meio de redes públicas operadas no Brasil ou por outros modelos possíveis de cooperativas que possam adquirir infraestrutura de redes 5G privadas. É mais simples, para as cooperativas, agregar os recursos, como acontece com o agronegócio, no âmbito de estocagem e enriquecimento de produção agrícola.

Os provedores de nuvem, como Amazon, ou Azure, da Microsoft, tem mostrado interesse em entrar no mercado de redes privadas 5G nos EUA, fornecendo serviços privados, isolados e integrados com as suas plataformas. Por exemplo, a *AWS Wavelength* [15] fornece serviços de computação em nuvem na borda da rede diretamente na rede 5G privada, com microlatência e as máquinas virtuais próximas das *IoTs* para processamento completo de baixa latência. Logicamente, esse novo tipo de oferecimento dos provedores de nuvem teria que ser supervisionado

de perto pela agência reguladora de telecomunicações ANATEL e pela Autoridade Nacional de Proteção de Dados.

Em resumo, nessa questão do licenciamento do espectro do 5G, nossa recomendação é que o leilão do espectro para oferecimento público e a concessão das redes privadas 5G deveriam acontecer concomitantemente.

Desse modo, os investimentos de todos os setores poderiam acontecer juntos e em grupos separados, garantindo que os equipamentos e o *software* para uma rede 5G ampla sejam realmente efetivados em tempo curto, dentro de uma janela de oportunidade de dois anos.

Seguindo a linha europeia do 5G seguro e sua diversificação, uma recomendação de política pública é facilitar a entrada de fornecedores de categorias chamadas desagregadoras de rádio e equipamentos de rede. A tendência mundial é que a desagregação de equipamentos integrados de rede em equipamentos *white box* possibilita a flexibilidade de reprogramar o produto e menor custo, uma vez que não tenta resolver todo o problema de maneira holística.

Destacam-se, nessa área, novos produtos e empresas na área de desagregação de redes cabeadas Ethernet, com variados *white boxes* de alto desempenho, bem como equipamentos de redes ópticas desagregados que viabilizam preços mais em conta para funções de *Dense Wavelength Division Multiplexing* (DWDM)[5]. E, nesse momento, também acontece a desagregação de equipamentos de rádio em componentes separados de *hardware* e *software*, e a softwarização dos processamentos de rádio nos chamados 5G SD-RAN (*software defined radio access network* para 5G).

Não é muito comum, no Brasil, que produtos inovadores como esses equipamentos *white boxes* e desagregados estejam nas redes de operadoras devido a sua criticidade, confiabilidade e disponibilidade, mas as redes privadas 5G podem ter requisitos menores de segurança e mais recursos de funcionalidades. Portanto, liberar esses produtos pode criar maior diversidade de oferta de fornecedores 5G, o que já é um objetivo na Europa.

Outro ponto importante é a liberação de faixas de transmissão mais amplas de espectro para as redes privadas 5G. Algumas das faixas liberadas pela ANATEL, de 10 MHz, não têm a banda mais potente para aplicações de Indústria 4.0, como o controle remoto de veículos autônomos, e, portanto, não trazem nenhum diferencial competitivo.

---

5. É uma tecnologia que pode combinar dezenas de canais em uma única fibra, economizando fibras e equipamentos de transmissão.

Assim, é sugerido reforçar a liberação de faixas mais amplas, como as de 100 MHz liberadas pela *Bundesnetzagentur*, a agência da Alemanha que lida com telecomunicações, usando a faixa semelhante de guarda da ANATEL, de 3.7 a 3.8 GHz, para esse tipo de aplicação.

Do ponto de vista da segurança cibernética em 5G, já apresentamos algumas ideias ao longo do documento, mas reforçamos as seguintes recomendações: é preciso que haja a criação de um perfil de risco nacional de fornecedores de equipamentos ligados a 5G, pois ele listaria equipamentos, vulnerabilidades, velocidade de conserto dos bugs e interoperabilidade com outros equipamentos.

Também é necessário criar um perfil de risco nacional de operadoras, provedores de Internet e empresas com acesso a redes privadas 5G, de modo a identificar empresas que sejam utilizadas por criminosos, as chamadas "*rogue ISPs*", que possam perder a licença por não se adequarem a critérios mais fortes de segurança.

Caberia à ANATEL, como recomendação de política pública, uma gestão contínua de riscos do 5G no Brasil, avaliando cada operadora, provedor de Internet e redes privadas, segundo um critério de criticidade, se a estratégia multifabricantes estaria efetivamente sendo adotada e medir o nível de dependência de um único fornecedor no Brasil.

Embora um único provedor possa otimizar melhor seus produtos em conjunto, a possibilidade de domínio tecnológico completo, em um ambiente de instabilidade geopolítica, pode causar problemas graves em reação. Além disso, essa avaliação crítica de riscos precisa focar também em dispositivos e recursos mais importantes na rede, como funções de *core*, gerência segura, orquestração e acesso.

Do ponto de vista de normatizações e regulamentos em nível de Estado, é a oportunidade única de melhorar a governança da segurança cibernética como um todo, a partir da demanda do 5G. Uma recomendação é implementá-la por intermédio da descrição e separação dos papéis, interfaces e modos de interação entre agências de fomento, governo e empresas. Pode-se criar sistemáticas de atuação inspiradas em normas como o Sistema de Busca e Salvamento Aeronáutico (SISSAR) que estabelece normas, interfaces e controles para a cooperação em operações de salvamento coordenadas pelo Comando da Aeronáutica.

Desse modo, deve-se atuar, do ponto de vista estratégico e político, com o tempo, para que o tático e operacional possam focar em sua missão de proteção da infraestrutura cibernética mais crítica.

A competência do setor público para os acordos de cooperação deve caminhar

para estabelecer mecanismos de regulação e acompanhamento dos processos e metodologias, enquanto que o setor privado deve contribuir com capital intelectual, ferramentas e investimento.

O governo deve realizar um sistema de certificação com regras próprias para facilitar o trabalho diversificado de empresas privadas, evitando a ocorrência de monopólios. O setor privado deve buscar conciliar os interesses públicos, trazendo os investimentos para desenvolver tecnologia e compartilhar conhecimentos.

O segredo do sucesso nos acordos de cooperação é incentivar que os diversos atores interajam em um ambiente colaborativo, com o governo executando a certificação, sem limitar a criatividade dos especialistas, fundamental para realizar a proteção dos ativos de informação frente aos constantes e contínuos ataques.

O modelo de acordos de cooperação no setor cibernético conduz para um sistema híbrido, onde o privado deve desenvolver as ferramentas, realizando o investimento e a operação, enquanto que o governo deve ser o ente regulador e coordenador.

Em relação à pesquisa e ao desenvolvimento no Brasil, os órgãos de fomento do Ministério da Ciência, Tecnologia, Inovação e Comunicação (MCTIC), sejam CAPES e CNPq, ou mesmo as fundações de fomento estaduais, precisam estar mais estrategicamente alinhados com os objetivos macro do país e sua soberania nacional. Isso já está, em certa medida, acontecendo quando o MCTIC atrela os projetos de pesquisa a atuarem mais em áreas estratégicas definidas como Inteligência Artificial.

Como recomendação, em Ciência e Tecnologia, é preciso aprofundar esse investimento público direcionado, para buscarmos maior expertise em segurança cibernética. Precisamos formar mão de obra especializada que aplique Inteligência Artificial no problema de segurança, que desenvolva métodos inovadores de busca de vulnerabilidades de maneira industrial, que faça a proteção automatizada por meio de inteligência de ameaças, e que também trabalhe em tecnologias 6G como alvo estratégico para o futuro.

A rede 5G traz muitos benefícios e novos serviços para a sociedade brasileira, mas também muitos desafios, em especial na área de segurança cibernética. É preciso agir rápido, a janela de oportunidade está se fechando, e precisamos aproveitar para não só proteger essa infraestrutura crítica e estruturante da sociedade do futuro, como também todo o remanescente, com segurança cibernética de ponta.

Os problemas de segurança cibernética em 5G são os mesmos da segurança cibernética em geral, apenas potencializados pela nova e expandida superfície de

ataque, então o melhor a fazer é endurecer a superfície com medidas eficazes de capacitação de recursos humanos, desenvolvimento de *softwares* e investimento de recursos financeiros nas áreas específicas de proteção, exploração e resposta.

Deve ser buscada a tão almejada atividade de colaboração entre órgãos públicos e privados em um ambiente de confiança. Trata-se de uma tarefa de difícil execução, mas não é uma missão impossível. Basta que o nível político-estratégico defina as orientações estratégicas e forneça os meios para que o nível operacional implemente os processos e procedimentos em prol da gestão cibernética em tempos de tecnologia 5G.

Por fim, todas estas iniciativas, incluindo os acordos de cooperação internacionais, buscam efetivar um latente sistema nacional de segurança cibernética, o qual contribuirá para uma maior resiliência nas atividades de defesa frente aos ataques cibernéticos na era da tecnologia 5G no cenário brasileiro.

Referências Bibliográficas

[1] S. Gallagher and A. Brandt, “Facing down the myriad threats tied to COVID-19,” 2020, https://news.sophos.com/en-us/2020/04/14/covidmalware/ (Acessado em 20 Nov 2020).

[2] Mobilise Global White Paper. 5G – An Opportunity or Threat for MVNOs? Set 2019, https://www.mobiliseglobal.com/wp-content/uploads/2019/09/Mobilise-5G_WhitePaper.pdf (Acessado em 20 Nov 2020).

[3] Kazmi, S.M.A., Khan L. U., Tran. N.H, Hong C.S.H. Network Slicing for 5G and Beyond Networks. 1st ed. 2019 Edition. ISBN 3030161692. Springer.

[4] DECRETO N. 7.175, DE 12 DE MAIO DE 2010. Institui o Programa Nacional de Banda Larga - PNBL. (posteriormente substituído pelo Decreto n.9.612 de 2018).

[5] Aikat, Baldin, Berman, et al. (2018). The Future of CISE Distributed Research Infrastructure. ACM SIGCOMM Computer Communication Review. 48. 10.1145/3213232.3213239.

[6] European Commission Press Release. Secure 5G networks: Questions and Answers on the EU toolbox. Brussels, 29 January 2020.

[7] 3GPP TS 29.520 - Network Data Analytics Services (Release 15), 3rd Generation Partnership Project Technical Specification, Rev. V15.2.0, Dec. 2018. http://www.3gpp.org/ftp/Specs/archive/29_series/29.520/ (Acessado em 20 Nov 2020).

[8] Paris Call. For trust and security in cyberspace - The 9 principles. https://pariscall.international/en/ (Acessado em 20 Nov 2020).

[9] Galis A., Contreras L., Serrat J., Rothemberg C., Papadimitriou P., Marcondes, C. NECOS Project: Towards Lightweight Slicing of Cloud-Federated Infrastructures” In Workshop on advances in slicing for softwarized infrastructures (S4SI 2018) – IEEE conference on network softwarization (NETSOFT), June 2018.

[10] DECRETO N. 10.222, DE 5 DE FEVEREIRO DE 2020 - Estratégia Nacional de Segurança Cibernética.

[11] INSTRUÇÃO NORMATIVA N° 4, DE 26 DE MARÇO DE 2020 – Presidência da República/Gabinete de Segurança Institucional (GSI). Dispõe sobre os requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G.

[12] ANATEL CONSULTA PÚBLICA Nº 13 DE 2020. Proposta de requisitos mínimos de segurança cibernética 5G. https://sistemas.anatel.gov.br/SACP/Contribuicoes/TextoConsulta.asp?CodProcesso=C2326&Tipo=1&Opcao=finalizadas

[13] Wagner C., Dulaunoy A., Wagener A, Iklody A. MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. pgs 49-56 (2016).

[14] FIRST - Forum of Incident Response and Security Teams. https://www.first.org/ (Acessado em 20 Nov 2020).

[15] Amazon Web Services. Edge Computing for 5G Networks with AWS Wavelength - White Paper. https://d1.awsstatic.com/Wavelength2020/Wavelength-Solution-Brief-FINAL-Aug2020.pdf (Acessado em 20 Nov 2020).

1 The importance of 5G Technology

Society is increasingly dependent on the digital world. Most individuals use digital technologies to perform many different activities on a daily basis. The use of these technologies has grown significantly worldwide since the emergence of COVID-19, as a result of the spread of remote work and the intensification of digital services.

While the increased use of such technologies and services has generated great interpersonal proximity in the virtual world, it has also helped increase and strengthen cyberattacks. Therefore, all nation-states need to pay special attention to protecting their information assets, whether public or private. Companies, seeking to ensure a secure digital expansion for their businesses and consumers, also consider investments in information technology and communications as strategic to operate in today's world.

In Brazil, the population as a whole has increasingly used the Internet and social networks, and government agencies and public companies have sought data network protection solutions, particularly concerning the transit of information between the corporate world and consumers.

Currently, the world is experiencing an unprecedented revolution in human society with the arrival of 5G technology in the area of telecommunications, which will transform the way we work and live: from an environment where the use of mobile technology is carried out almost exclusively to exchange messages between

humans, we will move to a new reality where billions of things will interact and talk to each other, forming a digital mesh for a fully connected world.

The technological disruption brought by 5G technology will occur in three main aspects:

a) Increased bandwidth potential for applications achieving up to double the order of magnitude of Brazil's 4G technology, where it will be possible to use high definition public security cameras to capture details of people's faces or virtual and augmented reality videos, as well as superimposing them in real time to assist in operations in factories, for example;

b) Drop in latency in one order of magnitude that allows instant response time. For example, an autonomous car can be ordered to stop in nanoseconds; and

c) Increase in two orders of magnitude in the number of devices connected simultaneously allowing, among others, for thousands of industrial control systems to work in complete coordination wirelessly.

The impact of 5G technology for society, in 10 to 25 years, will be very broad because the business models will be readjusted to an optimization and engineering standard, and will be highly automated.

Therefore, production, transportation and logistics management processes will be coordinated by Artificial Intelligence and we will have industrial robots working as orchestras, smart energy grids, personalized and domestic medicine, and remote controlled mining.

Smart cities will be able to provide ground and air space control services for autonomous vehicles for delivery, as well as public security will have better investigation and control capabilities. However, all of this involves risks with these technologies due to the fact that the network architecture is centralized on the operators, to the increased processing power at the network's edge and, mainly, the increased number of antennas and the use of software-defined networks in 5G, which will increase the attackers' surface exponentially.

Recently in Brazil, when cybersecurity was necessary in the context of the so-called major events in Brazil (World Cup and Olympics), the national cyber environment was still precarious, the level of mutual sharing between government agencies was low, and the space for private companies was reduced. However, the environment today is much more connected.

For example, in COVID-19 pandemic times, ransomware[1] attacks have multiplied, in which data hijacking can affect the performance of companies and institutions [1]. Moreover, in the 5G technology scenario, these threats are enhanced by the greater number of devices and the automation of flows and processes between cyber-physical systems.

The impact of dealing with ransomware at an electric power station, which can leave citizens without power for days, is much higher than that of deleting or destroying data from a company database on the market.

An advantage from the point of view of 5G technology is that it was designed and standardized with the "security by design" mentality. In other words, the protocols, the physical layer and the link layer[2] presume threat models that are more advanced than that of the simple model from the beginning of the Internet architecture, which had no formalities. Therefore, many mechanisms are present to guarantee link-level and application-level communication with the mobile network, in an appropriate manner and with strong authentication and encryption. But still, it is necessary to oversee the deployment of 5G technology projects to make sure that all of these features are enabled.

So far, in Brazil, the cybersecurity regulatory standards are not mandatory, but with the advent of 5G technology and a more advanced society that is connected in higher bandwidth and low latency[3] plus thousands of industrial control devices and autonomous vehicles, it is strategic to maintain national sovereignty from the point of view of understanding technologies and their risks.

In fact, the international cyber environment has become more militarized with the growing presence of advanced persistent threats (APT) that can be developed by the nation-state. Furthermore, this scenario changes the relationship between the public (civil and military) and private entities to an even greater interaction and a deep pact for sharing information and the consequent accountability of entities involved in malicious actions.

It is also known that the current scenario imposed by the COVID-19 pandemic caused a change in the way people work worldwide. This new reality brings

1. Ransomware is a form of malware (software designed to cause damage to a single computer, server, or computer network) that encodes the victim's files. The intruder then requests a ransom to restore access to the data, which is usually paid in Bitcoins (CSO - United States).

2. It is one of the seven layers of the OSI model (ISO reference computer network model, which is divided into function layers). Its basic purpose is to ensure reliable data transfer between systems connected directly by a physical means.

3. Latency is the amount of time it takes for a data package to go from one designated point to another. Low latency equals delay.

new challenges for agencies and companies, whether public or private. In the Information Technology (IT) sector, one of the challenges is to define policies and means to keep equipment safe and to protect access to corporate networks, considering the growing number of equipment outside the security perimeter of the network that needs to access it.

In this context, the implementation of effective policies for cybersecurity gains even more importance, since employees, in many cases, access corporate networks remotely for the maintenance of public and private services. Thus, secure access policies must be established and solutions implemented to ensure the security of the networks where 5G technology will be introduced, whether public or private.

This paper will address Brazil's role in this cybersecurity scenario of 5G technology by discussing the main challenges and opportunities that will emerge, Brazil's current position in relation to these issues, and the paths that we believe are important for the country to follow in order to be inserted in and plan a positive 5G technology agenda. In conclusion, long-term public policy actions at the State level will be recommended for better success in the future digital society.

2 Opportunities and Challenges

From a technological point of view, the 5G network brings impressive advances in radio communication technologies with high rates, in spectrum frequencies of 3.7 GHz for example, which require smaller cells and, therefore, have greater spatial multiplexing.

Additionally, it brings about the creation of greater computational capacity coupled to the network, with cloud computing environments at its edge. All of this brings great opportunities for new applications in Brazil.

Initially, we will address the opportunities and the beneficial side of the technologies and then the challenges and impediments with a focus on security.

A. OPPORTUNITIES

A natural candidate for these new applications is the agribusiness, which today uses satellite communication, refined control for precision agriculture, and highly sophisticated agricultural machinery. Therefore, 5G network applications are possibly fit for the agribusiness environments.

Brazilian mining companies such as Vale, Petrobras and Votorantim also have been working to eliminate risks to humans, replacing their fleets of mega trucks with autonomous vehicles and replacing humans with robots in mines and drilling works, especially in harsh environments.

But there are many more possible applications. The Brazilian industrial park is the largest in the southern hemisphere and has a large window of opportunities with the advent of 5G technology in the manufacturing environment called Industry 4.0. The window of opportunity to make a difference with 5G technology will be a maximum of three years [2]. After that, most companies will already be employing it to some extent, making it commoditized.

Industries will be automated, and data from machines, sensors, controllers and actuators will be transferred at high speed and in real time via 5G technology allowing the complete orchestration of the product manufacturing cycle.

In this field there is a special opportunity in so-called 5G private networks. These are networks that are controlled by companies, with complete isolation of transfer of sensor records from the external environment.

These private networks can be created and managed by large companies, as is currently the case of Vale and Eletrobras, but a specific spectrum allocation is required for this application. In Germany, the spectral range allocated is between 3.7 and 3.8 GHz with 100 MHz bands per project, providing high flow rate and broad device connectivity.

In Brazil, there are already decisions by the regulatory agency ANATEL to release a 30 MHz band in the 1.5 GHz frequency, but the matter is not yet fully regulated. There are also possible opportunities for other business models, where the operator rents its 5G antennas for industrial applications through network slicing technologies.

This model may have better performance and less need for initial investments by the company, since the costs of purchasing 5G base stations and also the qualification of operational technical personnel to keep the network running can be prohibitive.

Network slicing [3] may be the way to deal with 5G technology in Industry 4.0 in high-connectivity regions and a way for operators to shorten their payback period. However, in remote and isolated areas of Brazil, there must be a dedicated 5G network, where the window of opportunity can favor lone investments by a large company or joint investments by a group of companies.

Here, we may add the opportunity to regionalize 5G solutions, as there is no abundant electrical network in certain regions of Brazil, such as the state of Amapá. Therefore, regionalized base stations will need to use solar energy, satellite connection or even subfluvial fiber optic networks in Amazonian rivers and in the Pantanal region. Such regionalizations favor the national industry in aspects already mastered by Brazilian companies regarding the technology to reach these regions.

Another opportunity perspective is within the scope of smart cities. As of 2010, national investments have been made in the creation of metropolitan fiber optic networks in small and medium-sized cities in Brazil. These investments were part of a National Broadband Program (PNBL) [4]. However, many of these deployments did not reach their transforming potential, often due to low coverage in the city. The problem with the last mesh involved the passage of additional optical fibers to the metropolitan fiber system. Additionally, integration between city systems was

still in its first stages. Now, ten years later, we have a more favorable environment with technological solutions for smart cities, where health and public security systems, as well as city control centers, can be better organized, and the use of private 5G networks can be a great opportunity to leverage this transformation.

Private 5G networks based in smart cities can allow huge savings in areas such as real-time public transport synchronization, generating fuel savings with closed-loop control systems, as well as in the synchronization of health services and in new applications for air and ground traffic control for drones delivering products such as essential and time-sensitive medical items (defibrillators for example).

B. CHALLENGES

Despite all the interesting opportunities that arise from the use of 5G technology, there are many uncertainties, especially in the field of cybersecurity. From fear of international espionage to sabotage and even cyber warfare. A major challenge in 5G is how to maintain national security, with the increasing exposure of cyber-physical systems, in a context of distrust towards suppliers.

This challenge will have to be overcome by a series of certifications that ensure a wide validation of the safety of suppliers and their responsibility according to their actions.

Deployments of 5G network designs, whether public or private, will also need to go through a standardization of secure networks as a minimum requirement for connectivity with other networks.

In other words, the standardization challenge will have to be overcome, by cooptation, through stricter entry rules, with minimum configuration standards and security resources implemented for later participation. An example of this type of procedure is seen in the American academic networks connected to the Internet, which only receive financial support from National Science Fundation (NSF) [5] if they meet high-security conditions. Another excellent example of this safety standardization process is the EU 5G Toolbox project [6].

The European 5G cybersecurity recommendation (EU 5G Toolbox) attempts to create strict rules between member States of the European Union to minimize the risks of deploying 5G networks without strong security criteria.

This is due to the suspicion that these networks, which will be the foundation of the digital society of the future, may be a point of attack by enemies. It is noteworthy that the main security flaw in a network will always be at its weakest link.

Thus, European requirements go through refined device security inspection processes, in particular core 5G network products, network management products, service orchestration products and access network products.

Requirements include measures to increase competition and decrease the possibility of monopoly through rules for operators to present a certain diversity of interoperable equipment in their networks, and finally, the recommendation also calls for strong regulation from member countries regarding accountability in case of breaches and espionage.

Another challenge, more related to Brazil, is that telecommunications operators have low CAPEX investment capacity, and the need to purchase a large number of 5G equipment, due to smaller cells, can be an obstacle for a successful implantation in Brazil.

Moreover, regions that already face coverage deficiency in 4G will also tend to have gaps in 5G, and, therefore, the use of this 5G coverage for the management of industrial processes in these areas can be problematic.

On the other hand, according to the mapping of the opportunities above, the popularization of 5G private networks can increase this coverage, placing other companies, for example, regional or local Internet providers, in areas with low coverage and bringing private investments by these small and medium-sized companies. Additionally, the existing optical fibers of electric companies, road toll companies and others can backhaul[4] private 5G networks to smart cities, thus filling the coverage gap.

From a more technical point of view regarding the technology itself, there is a challenge in terms of monitoring this new type of network. Slicing technologies separate traffic and spectrum by client and, this way, much information is lost, as the possible horizontal monitoring is performed only at the level of the network slice defined by software.

Therefore, it will be necessary to develop technologies that allow for a more vertical monitoring, going deeper into the network's virtualization layers, up to the level of billing and connectivity (radio signals). There are some initiatives to address this challenge such as the Network Data Analytics Functions (NMDAF) [7], but much more must be done.

4. These are high-capacity telecommunications network infrastructures used in the provision of telecommunications services. A backhaul consists of equipment that connects to the backbones (the central networks of the Internet), located in the operators' central stations. This connection can be made by fiber optic cable, radio, satellite or other technologies.

Finally, the area of data protection is the big challenge in 5G: with the large volume of data available and the need to store data for the long term, it becomes a target for data hijackers. Despite the new Brazilian legislation, the General Data Protection Law (LGPD), it is necessary to couple the security of the 5G system with the protection of users' data via accountability.

The 5G security management has to be well conducted and the level of cybersecurity awareness in this context has to increase to avoid attacks on these critical operator systems. There are several initiatives that list principles to prevent attacks on critical infrastructure, such as those discussed under the Paris Call [8].

3 Brazil in the discussion of 5G Technology and its safety

Unfortunately, Brazil is lagging behind in the development of technology and also in the representativeness of its standardization. Within academia, there are few relevant research and patent examples in the areas of millimeter waves or radios with massive number of antennas (MIMOs) for this type of application, with only a few research institutes standing out.

Some relevant developments in research and innovation stand out, especially in the area of network slicing, such as the EU-Brazil NECOS Project (Novel Enablers for Cloud Slicing) [9]. However, even these efforts do not generate many practical results, due to the lack of an incentive for the generation of cutting edge companies, in this highly competitive area.

Our active national industry of network equipment is strong in optical networks and wired networks in which the companies Padtec and Datacom stand out, respectively. There are some isolated initiatives, but most of the mobile network products used by operators and other Brazilian companies are foreign. Brazil ended up as a receiver of 5G technology from abroad, namely suppliers from other countries such as Sweden (Ericsson), Finland (Nokia), China (Huawei) or Samsung (South Korea).

With this technological perspective, Brazil was left no alternative but to understand the technology through partnerships with these foreign companies that already operate in the country and carry out proofs of concept in private 5G networks and laboratory tests, as well as work to improve the validation maturity of technologies.

On the other hand, the government's top management is highly concerned about cybersecurity in 5G technology, because, as mentioned, it is this technology that will enable the digital society of the future, so it is necessary to take the appropriate precautions. In addition, there is the geopolitical discussion of alignment between countries. In this sense, several norms and regulations have been put forth in the past year to provide security for this transition to 5G technology.

From the point of view of safety regulation, the federal government issued decree No. 10,222 in February 2020, regarding the National Cybersecurity Strategy [10], which provides guidelines for the entire federal administrative management system on how to deal with cybersecurity and what is our strategy for becoming stronger as a country in this area.

This strategy guides public and private bodies towards permanent technical monitoring due to the relevance of the topic and constant technological developments in the cybersecurity area. It is a legal framework that did not exist before, and it allows us to show the increased awareness about the cybersecurity problem and to increase mechanisms for monitoring and accountability for misconduct.

In the specific scope of 5G technology, a norm that stands out is Normative Instruction No. 4 published by the Institutional Security Office linked to the President's office, and provides for the minimum requirements for Cybersecurity that must be adopted in the establishment of 5G networks [11].

Particular attention is paid to the question of possible vulnerabilities and backdoors in equipment, which, if implemented intentionally or involuntarily, can compromise the security of national communications systems.

It is important to highlight the audit mechanism that must be performed monthly by operators, according to Normative Instruction No. 4. Operators must inform the versions of hardware equipment and software, so that security audits can constantly monitor this attack surface.

Finally, in line with these State regulations, ANATEL, the telecommunications regulatory agency, held public consultations 6/2020, 11/2020 and 12/2020 on aspects that approach 5G from the point of view of equipment certification and one in particular on cybersecurity, 13/2020 [12].

This consultation addresses the minimum security requirements in order to reduce the possibility of vulnerabilities, through software/firmware updates and also recommendations on best practices in settings and remote management.

Other relevant aspects of ANATEL's regulation consist of suggesting which cryptographic methods are most suitable for data transmission and at rest, as well as establishing requirements for equipment suppliers, such as, a clear product support policy, accountability for updates and vulnerability fixes as soon as they appear, and also provide security updates, in real time, for at least two years.

Within the environment of the electricity sector, ANEEL, which is the electric power

regulatory agency, has been working on workshop discussions and whitepapers to advocate safer network architectures with in-depth defense and cyber-physical elements such as transformers and other controls. In this sense, Brazil moved towards the creation of an information exchange center specifically for incidents in industrial control systems, the ICS-CERT.

ANEEL and ANATEL have collaborated to allow the positioning of optical fibers in electric power poles, due to the exponential increase in network traffic that the 5G network will provide. They will also allow 5G private networks to use these poles that are already installed, instead of having to implant new underground optical fibers.

4 Ways for Brazil to insert itself in the context of 5G Technology

Brazil initiated its implementation of the 5G generation slowly. For example, there are countries that already have the technology in production. In addition, we did not have in-house technological developments like some European countries, thus, we need to quickly increase the number of technicians and engineers trained in the new technology in order to insert ourselves in this context of 5G.

There are some initiatives from the industrial sector, the National Confederation of Industry (CNI), via SENAI (National Industrial Learning Service) in training courses, driven by the transformation of Industry 4.0. There are also initiatives for training courses at the postgraduate level in several Brazilian universities such as Escola Politécnica da Universidade de São Paulo (Poli-USP) and Instituto Nacional de Telecomunicações (Inatel). But the tendency is for demand to increase even more.

As the 5G network, on the cybersecurity side, is essentially a technological problem equivalent to conventional computer security, it is important to reinforce a higher quality training for cybersecurity professionals in Brazil.

Although there are many courses in cybersecurity training in Brazil, in general, experience has shown that these professionals are still poorly trained when presented with critical security problems. The COVID-19 pandemic and the popularization of online courses by Brazilian universities can contribute to solve this problem by offering more courses, with improved quality and lower costs for Brazilians.

Another important aspect for Brazil to insert itself and be better protected using 5G technologies from the point of view of cybersecurity is to strongly increase the sharing of information between companies, public institutions and research centers. Sharing can be automated by an infrastructure of indicators of compromise (so-called IoCs), which may be implemented sectorally in the future.

At the moment, there is a tradition of information sharing in Brazil, due to the fact that the Brazilian Internet has been influenced by the Internet Steering Committee

in Brazil, where CERT.br acts as a central point in dealing with computer security incidents involving networks connected to the Internet, providing coordination and support, and making contacts to escalate incidents.

However, as malicious foreign groups meet on the Internet to exchange useful information and provide an entire black market of clandestine access, stolen data and zero-day vulnerability, it is necessary to increase the collaboration between companies and institutions in the public and private sectors in Brazil.

One path to be followed is the use of an Open Source Threat Intelligence Platform (MISP platform) [13] that facilitates automatic sharing, as well as the strengthening of a greater number of centers specialized in handling and responding to incidents, such as the Cyber Defense Command (ComDCiber) and the Brazilian Government Response Team for Computer Security Incidents (CTIR.Gov).

These centers should adopt a model similar to the North American Cybersecurity and Infrastructure Security Agency (CISA) with export and automatic enrichment of incidents with new indicators of compromise in real time, through the Trusted Automated eXchange of Indicator Information (TAXII) platform. The best option for Brazil is to establish the equivalent to airspace control, ensuring surveillance within the scope of the national cyberspace in favor of national sovereignty.

The regulatory agencies ANATEL and ANEEL have had safety certifications for some years now, to certify the safety of the electrical aspects and that radio electromagnetic irradiations are within normal safety parameters for the humans who operate and use the system. However, the aforementioned regulatory agencies urgently need to establish stricter certification criteria and procedures for cybersecurity risk assessment.

Certification procedures will have to use devices such as product pentest, resource risk assessment, and even development team compliance, for the team to be extremely secure, use quality programming, employ updated development libraries, and also work with architectural best practices for secure software.

The equipment and networks defined by software of the 5G networks will require a great certification effort so that the attack surface, although enlarged, is more robust against malicious attacks.

With regard to accountability for misconduct, Brazil still needs to further improve the legislation, and penalties need to be heavier so that the malicious hackers are properly punished.

In this area, ANATEL intends to create a kind of market assessment where the equipment and product chains involved in 5G will be evaluated through safety

tests, and if breaches or unresolved vulnerabilities are confirmed, they will be immediately excluded from the list of products for sale in Brazil.

The regulatory agency could be more incisive in that regard, not only banning the sale, but also demanding that the product be recalled immediately, as is the case with defective products in vehicles that can lead to the death of users. A network equipment with a known vulnerability, left without accountability, is like a truck with a defective tire, it must be taken out of circulation immediately so as not to injure anyone.

It is also necessary to better define the means of inferring the real responsibilities in the supply chains that manufacture the products, since 5G products are highly complex and require parts and components from dozens of suppliers. Inserting a malicious piece of hardware that allows equipment to be hijacked can be extremely stealthy.

The traceability and risk ranking of suppliers are important to increase the level of safety of the products being inserted in Brazil. For critical infrastructure sectors in particular, this is more than desirable, it is mandatory.

In the EU Secure 5G Toolbox project [6] there is a complete survey of suppliers in the 5G supply chain, as well as a determination to reduce monopolies through the diversification of suppliers, and greater accountability and requirements for telecommunications and critical infrastructure operators to obtain quality certifications in safety.

An example in Brazil is the company Petrobras that reached a higher level of response to incidents through its participation in the organization FIRST (Forum of Incident Response and Security Teams) [14]. To participate as a member in this organization, it is necessary to obtain several certificates and show quality improvement at high levels in cybersecurity. This should be the norm for all critical infrastructure sectors in Brazil.

From the point of view of research and development, since Brazil was not so active in developing the technologies involved in 5G, it should start promoting technological prospection in 6G technology.

Establishing new partnerships with multinationals for joint development of the next generations of 6G products with artificial intelligence, use of blockchain, quantum computing and quantum communications network, and cutting-edge cybersecurity, so that Brazilian research, development and innovation centers are better prepared for future versions of the critical man-to-man and machine-to-machine communication infrastructure.

5 Public Policy Recommendations

To conclude this cybersecurity policy paper on 5G technology, we suggest short and long term recommendations in terms of State policies to be implemented in Brazil.

A relevant topic is the problem of low investment capacity of Brazilian telecommunications operating companies and the need to completely replace the 3G/4G network with a much larger number of 5G network antennas. This needs to be dealt with creatively, due to the risk of the 5G technology bidding occurring without the network being implemented at the speed that the country needs.

A potential model is to open the possibility for private networks to use their own CAPEX, which can be done by large mining companies, large industries and the agribusiness, which would be able to absorb the operational costs and the operation of the 5G network. The Brazilian industry wishes to modernize to version 4.0 and may have more resources to acquire antennas and meet the demand, especially in isolated areas.

For medium and small sized companies, the 5G slicing rental model may be more attractive, either through public networks operated in Brazil or other possible cooperative models that can purchase infrastructure from private 5G networks. Cooperatives are a simpler way to aggregate resources, as is the case with the storage and enhancement of agricultural production in agribusiness.

Cloud providers like Amazon or Azure from Microsoft have shown interest in entering the 5G private network market in the US, providing private services, both isolated and integrated with their platforms. For example, AWS Wavelength [15] provides cloud-computing services at the edge of the network directly on the private 5G network, with microlatency and virtual machines close to the IoTs for complete low-latency processing. Of course, this new type of offer from cloud providers would have to be closely supervised by ANATEL and the National Data Protection Authority.

In summary, regarding the issue of 5G spectrum licensing, our recommendation is that the spectrum auction for public offering and the concession of 5G private networks should happen concurrently.

This way, investments from all sectors can happen together and in separate groups, to ensure that the equipment and software for a broad 5G network are actually implemented in a short period of time, within a two-year window of opportunity.

Following the European line of secure 5G and its diversification, a public policy recommendation is to facilitate the entry of suppliers of the so-called disaggregated categories of radio and network equipment. The global trend is the disaggregation of integrated network equipment into white box equipment, which allows flexibility to reprogram the product and lower costs, due to it not attempting to solve the whole problem holistically.

Noteworthy in this field are new products and companies in the area of disaggregation of wired ethernet networks, with various high-performance white boxes, as well as unbundled optical network equipment that enables more affordable prices for DWDM (Dense Wavelength Division Multiplexing) functions[5]. And at the moment, there is also the unbundling of radio equipment into separate hardware and software components, and the softwarization of radio processing in the 5G SD-RAN (software defined radio access networks for 5G).

It is not very common in Brazil for innovative products such as these white boxes and unbundled equipment to be on operator networks due to their criticality, reliability and availability, but 5G private networks may have lower reliability requirements and more functionality features. So, releasing these products can create greater diversity in the array of 5G suppliers, which is already a goal in Europe.

Another important point is the release of broader-band transmission spectrum for 5G private networks. Some of the bands that ANATEL has released, of 10 MHz, do not have the most potent band for Industry 4.0 applications such as remote control of autonomous vehicles and, therefore, do not bring any competitive differential.

Thus, we suggest to reinforce the release of broader bands, such as those of 100 MHz released by the German telecommunications agency, using ANATEL's similar guard band from 3.7 to 3.8 GHz for this type of application.

From the point of view of cybersecurity in 5G, we have already presented some ideas throughout this paper, but we reinforce with the following recommendations:

---

5. It is a technology that can combine dozens of channels in a single fiber, saving fibers and transmission equipment.

It is necessary to create a national risk profile for equipment suppliers connected to 5G. This profile should indicate the equipment, vulnerability, speed of bug fixes, and interoperability with other equipment.

It is also necessary to create a national risk profile for operators, Internet providers and companies with access to 5G private networks, in order to identify companies that are used by criminals, the so-called "rogue ISPs", which may lose their license for not adapting to stronger security criteria.

As a public policy recommendation, we suggest that ANATEL should be responsible for continuously managing 5G risks in Brazil, evaluating each operator, Internet provider and private networks, according to a criticality criterion, if the multi-manufacturer strategy is effectively being adopted and measuring the level of dependence on a single supplier in Brazil.

Although a single supplier can better optimize its products altogether, the possibility of complete technological dominance in an environment of geopolitical instability can cause serious problems. In addition, this critical risk assessment must also focus on the most important devices and resources on the network, such as core functions, secure management, orchestration and access.

From the point of view of norms and regulations at the State level, this is a unique opportunity to improve the governance of cybersecurity as a whole, based on the 5G demand. A recommendation is to implement it through the description and separation of roles, interfaces and modes of interaction between development agencies, government and companies. You can create action systems inspired by standards such as the Aeronautical Search and Rescue System (SISSAR) that establishes norms, interfaces and controls for cooperation in rescue operations coordinated by the Air Force Command.

From a strategic and political point of view, we must make the best use of the time we have to ensure that the tactical and operational teams can focus on their mission to protect the most critical cyber infrastructure.

The responsibility of the public sector for cooperation agreements must move towards establishing mechanisms for regulating and monitoring processes and methodologies, while the private sector must contribute with intellectual capital, tools and investments.

The government must implement a certification system with proper rules to facilitate the diversified work of private companies and prevent the occurrence of monopolies. The private sector must seek to reconcile public interests, bringing investments to develop technology and share knowledge.

The secret to success in cooperation agreements is to encourage the various actors to interact in a collaborative environment, with the government implementing the certification without limiting the specialists' creativity which is essential to protect information assets from the constant and continuous attacks.

The model of cooperation agreements in the cyber sector leads to a hybrid system where the private sector must develop the tools, carrying out the investments and the operation, while the government must be the regulator and coordinator.

Regarding research and development in Brazil, the funding agencies linked to the Ministry of Science, Technology, Innovation and Communications (MCTIC), such as CAPES and CNPq, and even state funding foundations, need to be more strategically aligned with the country's macro objectives and national sovereignty. This is already happening, to a certain extent, when the MCTIC requires research projects to work in more strategic areas defined as Artificial Intelligence.

As a recommendation in Science and Technology, it is necessary to deepen the directed public investment in order to seek greater expertise in cybersecurity. We need to train specialized labor to apply Artificial Intelligence to the security problem, developing innovative methods of searching for vulnerabilities in an industrial way, making automated protection through threat intelligence, and, at the same time, working on 6G technologies as a strategic target for the future.

The 5G network brings many benefits and new services to Brazilian society, but it also brings many challenges, especially in the cybersecurity area. We need to act fast because the window of opportunity is closing and we need to take advantage of it not only to protect this important critical infrastructure that is also structuring of the society of the future, but also to protect everything else, with cutting-edge cybersecurity.

The problems of cybersecurity in 5G are the same as cybersecurity in general, only enhanced by the new and expanded attack surface, so the best thing to do is to strengthen the surface with effective measures of capacity building and training, software development, and financial investment in specific areas of protection, exploration and response.

The long-awaited collaborative activity between public and private bodies in an environment of trust must be sought. It is a difficult task, but not an impossible mission. It only takes the political-strategic level to define the strategic guidelines and provide the means for the operational level to implement the processes and procedures in favor of cyber management in times of 5G technology.

Finally, all these initiatives, including international cooperation agreements, seek to activate and implement a latent national cybersecurity system, which will contribute to greater resilience in defense activities to face cyber attacks in the era of 5G technology in the Brazilian scenario.

References

[1] S. Gallagher and A. Brandt, “Facing down the myriad threats tied to covid19,” 2020, https://news.sophos.com/en-us/2020/04/14/covidmalware/ (Accessed on Nov 20, 2020).

[2] Mobilise Global Whitepaper. 5G – An Opportunity or Threat for MVNOs? Sept 2019, https://www.mobiliseglobal.com/wp-content/uploads/2019/09/Mobilise-5G_WhitePaper.pdf (Accessed on Nov 20, 2020).

[3] Kazmi, S.M.A., Khan L. U., Tran. N.H, Hong C.S.H. Network Slicing for 5G and Beyond Networks. 1st ed. 2019 Edition. ISBN 3030161692. Springer.

[4] DECRETO N. 7.175, from May 12, 2010. Establishes the Programa Nacional de Banda Larga - PNBL (later replaced by Decreto N. 9.612 from 2018).

[5] Aikat, Baldin, Berman, et al. (2018). The Future of CISE Distributed Research Infrastructure. ACM SIGCOMM Computer Communication Review. 48. 10.1145/3213232.3213239.

[6] European Commission Press Release. Secure 5G networks: Questions and Answers on the EU toolbox. Brussels, January 29, 2020.

[7] S. Sevgican, M. Turan, K. Gökarslan, H. B. Yilmaz and T. Tugcu, “Intelligent network data analytics function in 5G cellular networks using machine learning,” in Journal of Communications and Networks, vol. 22, no. 3, pp. 269-280, June 2020, doi: 10.1109/JCN.2020.000019.

[8] Paris Call. For trust and security in cyberspace - The 9 principles. https://pariscall.international/en/ (Accessed on Nov 20, 2020).

[9] Galis A., Contreras L., Serrat J., Rothemberg C., Papadimitriou P., Marcondes, C. NECOS Project: Towards Lightweight Slicing of Cloud-Federated Infrastructures” In Workshop on advances in slicing for softwarized infrastructures (S4SI 2018) – IEEE conference on network softwarization (NETSOFT), June 2018.

[10] DECRETO N. 10.222, from February 5, 2020 - Estratégia Nacional de Segurança Cibernética.

[11] INSTRUÇÃO NORMATIVA N. 4, from March 26, 2020 – Presidência da República/Gabinete de Segurança Institucional (GSI). Establishes the minimum cybersecurity requirements that must be adopted in 5G networks.

[12] ANATEL CONSULTA PÚBLICA N. 13, from 2020. Proposal of minimum 5G cybersecurity requirements. https://sistemas.anatel.gov.br/SACP/Contribuicoes/TextoConsulta.asp?CodProcesso=C2326&Tipo=1&Opcao=finalizadas

[13] Wagner C., Dulaunoy A., Wagener A, Iklody A. MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. pgs 49--56 (2016).

[14] FIRST - Forum of Incident Response and Security Teams. https://www.first.org/ (Accessed on Nov 20, 2020).

[15] Amazon Web Services. Edge Computing for 5G Networks with AWS Wavelength - Whitepaper. https://d1.awsstatic.com/Wavelength2020/Wavelength-Solution-Brief-FINAL-Aug2020.pdf (Accessed on Nov 20, 2020).

CEBRI

CENTRO BRASILEIRO DE
RELAÇÕES INTERNACIONAIS

BRAZILIAN CENTER FOR
INTERNATIONAL RELATIONS

Associados / *Members*

Instituições / *Institutions*

Abiquim
Aegea
Aeróleo Táxi Aéreo
BAMIN
Banco Bocom BBM
BASF
BMA Advogados
BDMG
BNDES
BRF
Brookfield Brasil
Bunker One
Captalys Investimentos
CCCC/Concremat
Comerc Energia
Consulado Geral dos Países Baixos no Rio de Janeiro
Consulado Geral da Irlanda em São Paulo
Consulado Geral do México no Rio de Janeiro
Consulado Geral da Noruega no Rio de Janeiro
CTG Brasil
Dannemann, Siemsen, Bigler & Ipanema Moreira
Dynamo
EDP
Eletrobras
Embaixada da China no Brasil
ENEVA
ENGIE Brasil
Equinor
ExxonMobil
FCC S.A.
Grupo Lorentzen
Grupo Ultra
Huawei
IBÁ
IBRAM
Icatu Seguros
InvestHK
Ipanema Investimentos
Itaú Unibanco
JETRO
Klabin
Lazard
Light
Mattos Filho Advogados
Museu do Amanhã
Michelin
Neoenergia
Oktri Empreendimentos
Paper Excellence
Petrobras
Pinheiro Neto Advogados
Prumo Logística
Repsol Sinopec
Sanofi
Santander
Shell
Siemens Energy
Souza Cruz
SPIC Brasil
State Grid
Tecnoil
Total E&P do Brasil
Vale
Veirano Advogados
Vinci Partners

Senior Fellows

Adriano Proença
Ana Célia Castro
Ana Paula Tostes
André Soares
Benoni Belli
Carlos Milani
Clarissa Lins
Daniela Lerda
Denise Nogueira Gregory
Diego Bonomo
Evangelina Seiler
Fabrizio Sardelli Panzini
Fernanda Guardado
Fernanda Magnotta
Hussein Kalout
Izabella Teixeira
Larissa Wachholz
Leandro Rothmuller
Lia Valls Pereira
Mário Ripper
Matias Spektor
Miguel Correa do Lago
Monica Herz
Patrícia Campos Mello
Paulo Sergio Melo de Carvalho
Pedro da Motta Veiga
Philip Yang
Ricardo Sennes
Rogerio Studart
Sandra Rios
Tatiana Rosito
Vera Thorstensen
Victor do Prado

Equipe CEBRI / *CEBRI Team*

Diretora-Presidente
CEBRI CEO
Julia Dias Leite

Diretora Relações Institucionais
e Comunicação
Director of Institutional Relations and Communications
Carla Duarte

Diretora de Projetos
Director of Projects
Luciana Gama Muniz

Projetos
Projects

Gerente de Projetos / *Projects Manager*
Lara Azevedo

Consultoras / *Consultants*
Cintia Hoskinson
Marianna Albuquerque

Estagiários / *Interns*
Gustavo Berlie
Larissa Vejarano

Relacionamento Institucional e Eventos
Institutional Relations and Events

Gerente de Relações Institucionais e Eventos
Barbara Brant

Consultores / *Consultants*
Caio Vidal
Nana Villa Verde

Estagiário / *Intern*
Lucas Bilheiro

Comunicação
Communications

Consultora / *Consultant*
Gabriella Cavalcanti

Estagiário / *Intern*
Henrique Kress

Administrativo e Financeiro
Administrative and Financial

Coordenadora Adminstrativa-Financeira /
Administrative-Financial Coordinator
Fernanda Sancier

Assistente / *Assistant*
Kelly C. Lima

CENTRO BRASILEIRO DE
RELAÇÕES INTERNACIONAIS

*BRAZILIAN CENTER FOR
INTERNATIONAL RELATIONS*

ONDE ESTAMOS / *WHERE WE ARE*:

Rua Marquês de São Vicente, 336
Gávea, Rio de Janeiro – RJ - Brazil
22451-044

Tel: +55 (21) 2206-4400

cebri@cebri.org.br

www.cebri.org