CEBRI

CENTRO BRASILEIRO DE
RELAÇÕES INTERNACIONAIS

NÚCLEO
SEGURANÇA
INTERNACIONAL

GRUPO DE ANÁLISE DE SEGURANÇA
CIBERNÉTICA (GRUPO CYBER)

SEGURANÇA CIBERNÉTICA E **REDES PRIVADAS 5G** PARA ACELERAÇÃO DA TRANSFORMAÇÃO DIGITAL NO BRASIL

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

---

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.

www.cebri.org

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

NÚCLEO
SEGURANÇA
INTERNACIONAL

GRUPO DE ANÁLISE DE SEGURANÇA
CIBERNÉTICA (GRUPO CYBER)

2º WEBINAR DO GRUPO CYBER
10 DE NOVEMBRO DE 2020

SEGURANÇA CIBERNÉTICA E **REDES PRIVADAS 5G** PARA ACELERAÇÃO DA TRANSFORMAÇÃO DIGITAL NO BRASIL

Paulo Sergio Melo de Carvalho
Senior fellow do CEBRI e General de Divisão da
Reserva do Exército Brasileiro

PARCERIA: SIEMENS SIEMENS energy

FICHA TÉCNICA

AUTOR

Paulo Sergio Melo de Carvalho

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

COORDENAÇÃO EDITORIAL

Julia Dias Leite
Diretora-Presidente do CEBRI

Luciana Gama Muniz
Diretora de Projetos do CEBRI

Cintia Hoskinson
Consultora de Projetos do CEBRI

APOIO EDITORIAL

Carlos Arthur Ortenblad Jr.

Gustavo Berlie

Larissa Vejarano

DIAGRAMAÇÃO

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

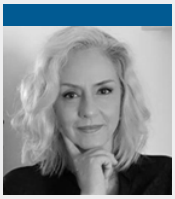
Julia Dias Leite

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.

Participantes do 2º Webinar do Grupo Cyber

10 de novembro de 2020

Agostinho Linhares
Gerente de Espectro, Órbita e Radiodifusão da Agência Nacional de Telecomunicações (ANATEL)



Márcia Tosta
Gerente Executiva de Segurança da Informação da Petrobras

André Clark
Conselheiro do CEBRI e General Manager da Siemens Energy no Brasil

Pablo Fava
CEO da Siemens

Luciana Gama Muniz
Diretora de Projetos do CEBRI

Paulo Sergio Melo de Carvalho
Senior Fellow do CEBRI e General de Divisão da Reserva do Exército Brasileiro

Marcia Ogawa Matsubayashi
Sócia Líder da Indústria de Tecnologia, Mídia e Telecom da Deloitte Brasil

Thiago Barçante Teixeira
Coordenador Substituto de Regulamentação Técnica da Gerência de Certificação e Numeração de Produtos da Agência Nacional de Telecomunicações (ANATEL)

Sumário Executivo

A Segurança Cibernética, no âmbito mundial, vive uma situação de efervescência em relação à proteção dos ativos de informação, sejam públicos ou privados, fruto da nova forma de convivência humana decorrente da pandemia da Covid-19 e do consequente trabalho remoto, o que gerou um incremento de serviço para os especialistas de segurança da informação e comunicações, buscando reduzir os inúmeros flancos vulneráveis para as ameaças cibernéticas.

Os *hackers* sempre estão na ofensiva, e os ataques coordenados por eles têm aumentado de forma exponencial, principalmente em relação às empresas que detêm informações críticas, tais como energéticas, de saúde, do setor de transporte, de âmbito bancário, do comércio atacadista e varejista, entre outras.

Estas investidas visam, primordialmente, ao sequestro de dados, com a imposição de pagamento para reposição das informações subtraídas, geralmente em criptomoedas.

No Brasil, os ataques ocorridos na atualidade atestam esta conjuntura preocupante para a segurança cibernética, conforme noticiado por órgãos midiáticos e pelas redes sociais, entre outras ações perpetradas pelos agentes das ameaças cibernéticas, muitas das quais não chegam ao conhecimento do público em geral:

- Supremo Tribunal Federal (STF) pede ajuda ao Exército para restaurar os seus sistemas de informática, invadidos por um ataque hacker na última terça-feira (O Antagonista, 05 de novembro de 2020);
- Além do Superior Tribunal de Justiça (STJ), outros órgãos sofrem tentativas de ataques: o Conselho Nacional de Justiça (CNJ) e o governo do Distrito Federal também passaram por investidas, e o Ministério da Saúde relatou que o órgão estava sem acesso à internet, linhas de telefone fixo e e-mails (Valor Econômico, 05 de novembro de 2020);

- Clientes da ENEL têm dados como CPF e celular vazados na internet (Veja São Paulo, 10 de novembro de 2020);
- *Hacker* invade site da Controladoria-Geral da União (CGU) e publica passo a passo no YouTube (Metrópoles, 11 de novembro de 2020); e, recentemente;
- Empresa Brasileira de Aeronáutica S.A. (Embraer) sofre ataque *hacker* e ainda avalia a extensão dos danos (Defesa em Foco, 01 de dezembro de 2020).

As supracitadas circunstâncias demonstram que o mundo da segurança e defesa vai ao encontro do mundo dos negócios, pois os ativos de informação estão presentes em ambos, sejam dados pessoais ou de Estado, impondo uma atuação integrada, criativa colaborativa entre órgãos públicos e empresas na proteção destes dados, para tentar retirar a vantagem do elemento surpresa dos perpetradores da ameaça cibernética.

A discussão sobre a tecnologia móvel 5G no mundo tem trazido novos atores para a geopolítica, que influenciam as medidas a serem tomadas pelos países para regulamentar as atividades de tecnologia da informação e comunicações, que terão ascendência em relação ao cotidiano da população, da economia, da indústria, dos transportes, da segurança e da saúde, facilitando a automação e a comunicação no mundo digital e chegando, inclusive, a um enorme acréscimo dentre todos os dispositivos elétricos e eletrônicos, os quais constituem a Internet das Coisas.

As redes privadas de tecnologia 5G, com as correspondentes medidas de proteção cibernética, devem influenciar a competividade das indústrias no Brasil e contribuir para um melhor desempenho das infraestruturas críticas nacionais, nomeadamente, energia, saúde, transporte, telecomunicações e setor financeiro. Ou seja, estas redes já são realidade no mundo atual da economia digital e merecem uma atenção especial dos Estados-Nação para sua implantação e operacionalização.

A Segurança Cibernética com a Rede 5G e a Sociedade Brasileira

Quando se aborda o tema da segurança cibernética e das redes privadas 5G, enfatiza-se o futuro do Brasil. Aqui, esta tecnologia deverá gerar grandes impactos para a sociedade, decorrentes de nossas características, relacionadas com as condições socioeconômicas da população, o cenário geopolítico no continente sul-americano, a matriz tecnológica nacional, as dimensões continentais do território brasileiro e as condições dos serviços prestados pela rede de infraestrutura do setor de telecomunicações.

A tecnologia 5G deve ser compreendida como um conjunto de tecnologias que envolve inteligência artificial, *Edge, Cloud, Ethical Tour, Big Data* e *Internet of Things* (IoT). Ela terá um grande poder de transformação na sociedade, evitando a economia de escala e alterando o fundamento econômico tradicional, saindo da lógica linear para a exponencial. Os usuários nas tecnologias móveis 2G, 3G e 4G estão restritos às pessoas físicas. Já na tecnologia 5G, haverá também usuários não-humanos.

As fábricas terão milhares de dispositivos conectados e tudo estará em rede. Por exemplo, em um corpo humano, o acompanhamento de uma gota de sangue poderá ser realizado de forma virtual, o que ajudará na realização dos diversos diagnósticos e intervenções cirúrgicas, com maior facilidade para os profissionais da área de saúde e, naturalmente, também para os pacientes.

A tecnologia 5G aborda, fundamentalmente, os dados e não somente a conectividade. Eles transformam as empresas e geram as estratégias corporativas, as quais incorporam novas tecnologias e telecomunicações. Antigamente, a tecnologia era o suporte dos negócios, ou seja, o meio. Agora, em época de economia digital, é o fim.

Atualmente, todas as corporações trabalham com a engenharia integrada à estratégia, primordialmente nas áreas de tecnologia da informação e teleco-

municações, inclusive aquelas que não são da área tecnológica, tais como empresas petroquímicas, mineradoras e de manufatura.

Com o avanço acelerado das tecnologias de telefonia móvel, os CEOs têm trabalhado para o potencial competitivo da tecnologia 5G com uma janela de oportunidade de dois a quatro anos. Nos últimos sete meses, foram desenvolvidos no mundo cerca de 245 projetos relacionados com as redes privadas de 5G devido à pandemia da Covid-19, a qual acelerou a necessidade de maior controle e monitoramento das redes de telecomunicações e da internet, em decorrência do aumento do trabalho remoto.

Grandes conglomerados de vários países ditos desenvolvidos já iniciaram projetos-piloto relacionados com a tecnologia 5G nas redes privadas em diversas áreas, tais como portos, aeroportos, empresas de mineração, plantas tecnológicas e automotivas e companhias de energia.

Um caso de sucesso nas redes particulares de 5G tem ocorrido na Alemanha, onde o *Bundesnetzagentur*, órgão regulador responsável, liberou uma banda de 100 MHz na faixa de frequências de 3.7 a 3.8 GHz, permitindo que a nação alemã seja líder mundial em relação à quantidade de redes privadas 5G em funcionamento na atualidade. Os Estados Unidos da América, o Japão e o Reino Unido também têm avançado neste tema, com ênfase na distribuição de frequências para as redes privadas.

Como dado global, a tecnologia 5G poderá impactar 5% da atividade econômica em todo o mundo no longo prazo e, no Brasil, deverá gerar R$ 323 bilhões relacionados a benefícios em setores estratégicos, o que corresponderá a 5% do Produto Interno Bruto (PIB) anual. Ocasionará um grande incremento na economia brasileira, impulsionando os setores da aviação, portuário, industrial, saúde, entre outros.

Em relação à tecnologia, existe uma grande tendência de virtualização, os *hardwares* irão se transformar em commodities e tudo será *software*, além de ocorrer uma desagregação das camadas de redes de telecomunicações, o que permitirá a chegada de novos *players* nesta cadeia de valor de desagregação.

Os impactos na economia, em relação à demanda, poderão ocorrer com as operadoras construindo redes com baixo custo em um ambiente de inovação e com as grandes corporações possuindo parte de suas próprias redes. No lado da oferta, haverá oportunidades para novos participantes e o ambiente possibilitará a atração de novos investidores, dinamizando a economia digital com uma maior densidade tecnológica e gerando mais empregos, com o incremento da correspondente pesquisa e desenvolvimento.

No que se refere à segurança cibernética, a tecnologia 5G não traz mais riscos comparativamente com as gerações anteriores. De fato, ela é mais segura, por ser desenvolvida de acordo com a metodologia de *security by design*, trazendo mais elementos de segurança em relação ao 4G, com regras mais rígidas de autenticidade, criptografia, confidencialidade e integridade.

As Redes 5G e a Segurança Cibernética no Setor Privado

A tecnologia móvel 5G deve ser adotada com urgência, o que impõe o desenvolvimento de protocolos seguros que tenham uma forma rápida de implementação, congregando o setor privado, os órgãos governamentais e os usuários, com destaque para o agente regulador.

A transformação digital da economia brasileira deve ser apoiada pela conectividade da tecnologia 5G, com base em três características principais, a saber:

- a velocidade de comunicação é 100 vezes superior à da tecnologia 4G, o que modificará a forma como as pessoas poderão enviar pacotes de dados, gerando uma grande disrupção tecnológica;
- a latência da rede será 1/25 da rede 4G, o que vai permitir trabalhar em *real time* com grande volume de dados; e, principalmente,
- a grande quantidade de dispositivos que estarão conectados em rede, permitindo tornar realidade a Internet das Coisas, ou a Internet da Energia, que é uma forma diferente de visualizar o mesmo fenômeno.

No setor privado, os serviços que serão disponibilizados para atender, em melhores condições, a indústria manufatureira, infraestruturas, hospitais, aeroportos e o transporte metropolitano, deverão gerar grande impacto. Por exemplo, em um metrô, será possível realizar a supervisão de atividades em tempo real, o que tornará os trabalhos de segurança mais eficientes.

Um fator importante a considerar é a questão da cobertura geográfica, principalmente em países de dimensões continentais como o Brasil. Pode ocorrer que, em regiões afastadas dos grandes centros, a cobertura da rede de telecomunicações 5G fornecida pela rede pública seja deficitária e que, assim, faça-se necessário que as empresas, como as relacionadas ao agronegócio, por exemplo, instalem redes privadas ou contratem um ente, especificamente para projetar, construir e operar redes privadas para atender às suas necessidades.

Outra situação que está acontecendo em escala mundial é a tendência de retirar as pessoas do trabalho *in loco* na indústria de mineração. Estas deverão atuar com controle remoto, e até mesmo os veículos utilizados para o transporte dos minérios deverão ser autônomos.

Desse modo, a responsabilidade das empresas em rede proprietária de 5G é compensadora, em virtude das operações de *Capital Expenditure* (CAPEX) e *Operational Expenditure* (OPEX) serem mais simples e facilitarem as atividades de investimento dos empresários.

Uma questão primordial em relação à tecnologia 5G diz respeito à privacidade de dados, pois se uma empresa dispõe de uma rede proprietária, ela pode deixar, com segurança, os dados restritos a esta infraestrutura. Existem dados relacionados com a cadeia de produção e outros com restrição de propriedade intelectual, por exemplo, os quais não podem ser do conhecimento de outras empresas ou pessoas em uma rede pública, por colocar em risco o próprio negócio.

A rede privada deve ser uma alternativa da rede pública. Esta última, na maioria dos casos, atende às empresas plenamente e sem inconvenientes. Entretanto, o Brasil precisa oferecer alternativas para determinadas indústrias, infraestruturas, aeroportos, companhias metropolitanas e hospitais, entre outras organizações, disponibilizando um polígono de frequências para licenciar para as empresas, por exemplo, a faixa de frequências de 3.7 a 3.8 GHz, a qual funciona como a frequência de guarda da Agência Nacional de Telecomunicações (ANATEL), e devem ser realizados testes para a sua utilização pelas redes privativas.

Isto permitirá um ganho de potencial para as empresas, aumentando a sua eficiência e alavancando ganhos de investimentos. Haverá uma revolução na indústria de manufatura, com processos autônomos na produção e logística. A atuação de robôs nos diversos setores das indústrias manufatureiras será cada vez mais difundida, inclusive com a elevação da eficiência dos centros de distribuição. Tudo isto só será possível graças às funcionalidades da tecnologia 5G, que permitem a execução destas atividades, onde o *real time* é um fator crítico para o sucesso.

Contudo, convém destacar que a tecnologia 5G apresenta uma janela de vulnerabilidades, apesar de ser um sistema desenvolvido com mais segurança, tratando-se de *security by design*, conforme previamente abordado neste relatório. A grande quantidade de dispositivos conectados aumenta consideravelmente a superfície de ataque, gerando muitas oportunidades para acessos indevidos e tornando-se um terreno fértil para a atuação dos agentes das ameaças cibernéticas.

A Gestão da Segurança Cibernética com o advento da Tecnologia 5G

A chegada da tecnologia 5G trará enormes benefícios para o futuro que se avizinha, com uma grande ampliação na velocidade de transmissão de dados, o que irá potencializar a Internet das Coisas e a inteligência artificial, impondo uma mudança de paradigmas na gestão da segurança cibernética em um ambiente de infraestrutura de telecomunicações com uma maior cobertura e com elevada qualidade do sinal, gerando um aumento da superfície de exposição.

Este aprimoramento nas redes de telecomunicações com o advento da tecnologia 5G, com o aumento do alcance, da velocidade de transmissão de dados e da quantidade de dispositivos conectados, será explorado pelos criminosos cibernéticos em suas ações ofensivas com mais facilidade e em um amplo espectro de flancos vulneráveis no espaço cibernético.

Os agentes das ameaças cibernéticas estão sempre na ofensiva e, com a chegada da tecnologia do 5G, agora contam com uma grande superfície de exposição. Assim, os fornecedores de *software* precisam dedicar ainda mais esforços para minimizar os *bugs* nos programas e ter um cuidado constante com a segurança no desenvolvimento dos sistemas e programas.

A Internet das Coisas está presente no dia a dia das pessoas, de soluções simples até sistemas mais complexos, como o monitoramento da umidade de tijolos para ser utilizado na previsão de terremotos, acompanhamento do desempenho dos marca-passos e vasos sanitários que coletam urina para realização de exames de laboratório e envio para os médicos. São exemplos que denotam a importância da gestão das pessoas, dos procedimentos e da tecnologia no âmbito da segurança cibernética nos órgãos públicos e privados, desde o nível operacional até o político-estratégico, em tempos de redes de telecomunicações, públicas e proprietárias, com tecnologia móvel de 5G.

Os *hackers* possuem um eficiente sistema de gestão das melhores práticas de seu trabalho de gerar riscos e danos no espaço cibernético, utilizando-se de redes como a *Deep Web* e a *Dark Web* para compartilhar inteligência e informações que facilitem suas ações futuras. Isto não ocorre com aqueles que estão na defesa e sofrendo com estes ataques maliciosos. Ou seja, é indispensável que um sistema similar ou superior ao dos transgressores seja elaborado para colaboração e trocas relativas à proteção contra ataques e ao fortalecimento da segurança no espaço cibernético.

Uma iniciativa que já está acontecendo neste sentido é a *Cyber Security Body of Knowledge*, que busca compartilhar as ameaças em um ambiente colaborativo e produtivo, replicando-as, com sincronismo e velocidade, para a rede dos defensores, além de ampliar a superfície de defesa com o comprometimento das ameaças dos criminosos cibernéticos e compartilhando processos e tecnologias.

A atividade das telecomunicações com o advento da Tecnologia 5G e a Segurança Cibernética

A ANATEL vem trabalhado há algum tempo no tema da regulamentação da tecnologia 5G e realizou gestões no corrente ano para liberar faixas de frequências para a telefonia celular móvel, com as correspondentes licitações, incluindo os serviços privados.

O mundo da tecnologia 5G não será unicamente uma evolução ou revolução dos tempos contemporâneos, mas contará com características de ambas. Além de melhoria dos requisitos em relação às gerações anteriores, a tecnologia 5G irá obrigar as operadoras comerciais a deixar de atuar de forma B2C (*Business to Consumer*), vendendo apenas para o consumidor final, para trabalhar no modelo de negócio B2B (*Business to Business*), comercializando com outras empresas, inclusive fornecendo serviços para as conexões com as redes privadas.

As empresas proprietárias destas redes poderão atuar de forma *stand-alone*, que é, grosso modo, quando a entidade é dona de todos os recursos, incluindo as infraestruturas ativas e passivas, mas também terão a possibilidade de contratar infraestrutura das operadoras comerciais, além de trabalhar combinando os dois modelos e chegar a vários cenários de utilização da tecnologia 5G nas redes privadas.

Em novembro de 2020, a ANATEL e a Agência Brasileira de Desenvolvimento Industrial (ABDI) assinaram acordo de cooperação técnica para testes de redes privadas em 5G, no intuito de buscar contribuir para a melhoria da competividade da indústria nacional, com soluções efetivas para a conectividade, de forma a permitir que as empresas brasileiras possam competir em qualquer parte do mundo, independentemente de estarem geograficamente distantes de potenciais clientes, graças à utilização da tecnologia 5G.

O Brasil ainda está na infância da tecnologia 5G, mas não está tão defasado em relação aos países que já a implantaram, pois o mundo, na área de te-

lecomunicações, ainda trabalha com o *3GPP Release 13* com a Internet das Coisas. O *release 15* em 5G permite a banda larga otimizada, e os *releases 16* e *17*, ainda em fase de implementação, irão possibilitar a comunicação de grande confiabilidade e baixa latência, além de permitir a comunicação massiva máquina-a-máquina.

A ANATEL tem autorizado a implantação de redes privativas que atendam aos requisitos técnicos na banda de 10 MHz na frequência de 2.3 GHz, e liberou, ainda, várias faixas de frequências para redes privativas, a saber: 250 MHz; 410, 415, 420 e 425 MHz (não é a faixa que foi licitada em 440 MHz); 2485 a 2495 MHz, que permite redes privativas na região; e ondas milimétricas de 27.5 a 27.9 GHz com faixa de 400 MHz; bem como o Conselho Superior do Centro de Altos Estudos em Telecomunicações (Ceatel) da Agência aprovou 30 MHz adicionais na frequência de 1.5 GHz. Encontra-se em estudo a utilização da banda de 100 MHz na faixa de 3.7 a 3.8 GHz, já utilizada por vários países no mundo, conforme já foi exposto neste texto.

Em relação à segurança do ciberespaço, a ANATEL tem dedicado especial atenção à certificação dos produtos de telecomunicações, desde sensores sem fio até o *core* das operadoras, com uma grande diversificação do material a ser homologado.

Nos dias atuais, esta certificação de segurança é baseada na parte elétrica, por intermédio de compatibilidade de irradiação eletromagnética e radiação não-ionizante. Contudo, a dimensão cibernética não tem a relevância almejada.

Isto está mudando. Foi realizada uma consulta pública e estão sendo estabelecidos requisitos de segurança cibernética baseados em *frameworks* e melhores práticas, com o apoio de laboratórios de ensaio e considerando a grande diversidade das aplicações.

Uma vez definidos os requisitos de avaliação de segurança cibernética, será estabelecido um programa de supervisão do mercado com o objetivo de manter a integridade da rede, garantir a confiabilidade das telecomunicações e permitir a execução de auditoria.

Pretende-se que a ANATEL atue verificando os produtos e avaliando a segurança do ciberespaço de duas formas: ativa, com uma ação contínua baseada em ações preventivas, e reativa, com foco nos incidentes ocorridos, sempre buscando monitorar o mercado e corrigir as falhas existentes, as quais poderão levar à suspensão da homologação do produto até que a empresa envolvida elucide a questão.

A ANATEL procura contribuir para o desenvolvimento industrial do Brasil, buscando soluções em sua área de atuação, para que as empresas tenham ganho de produtividade, em tempos de economia digital, com a utilização de redes privadas, propiciando maior transmissão de dados em um adequado espectro de frequências e com efetiva segurança cibernética dos produtos utilizados nas diversas infraestruturas de telecomunicações.

Comentários finais

A adoção da tecnologia 5G é fundamental para o Estado Brasileiro, em virtude de gerar competividade e aumentar a eficiência das empresas e do setor governamental, permitindo agregar valor e conferir destaque para o país no contexto internacional.

O Brasil deve estudar as melhores práticas, inclusive no cenário global, para estabelecer as redes de tecnologia 5G, públicas e privadas, sem criar grandes riscos relacionados à tecnologia e buscando gerar impactos favoráveis à economia brasileira, de forma a ajudar a inserção brasileira no bloco dos países que lideram o cenário digital mundial.

A tecnologia 5G precisa ser regulamentada com urgência no Brasil para facilitar os trabalhos de implantação de infraestrutura necessária para suportá-la, sem olvidar das medidas de segurança cibernética para reduzir os riscos e danos decorrentes do aumento da superfície de ataque.

Novas metodologias devem ser buscadas para aperfeiçoar a gestão da segurança cibernética nas organizações com o advento da tecnologia 5G, principalmente em relação às novas funcionalidades decorrentes da inteligência artificial e da Internet das Coisas, e às facilidades para a ação dos criminosos cibernéticos, resultantes da maior velocidade e alcance de transmissão de dados, além de uma grande exposição no espaço cibernético, facilitando sobremaneira a ação dos agentes causadores das ameaças cibernéticas.

As infraestruturas críticas são fundamentais para o dia a dia das pessoas, sendo uma questão de segurança nacional e impondo procedimentos específicos para mantê-las em pleno funcionamento e com resiliência, principalmente no futuro, com as cidades inteligentes, quando deveremos ter sistemas seguros que atendam às seguintes recomendações:

- a necessidade de uma regulamentação nacional;
- a adequação dos requisitos mínimos dos editais para as exigências básicas de segurança cibernética; e

- o estabelecimento de uma rede colaborativa entre os diversos entes da sociedade brasileira, com a elaboração, por exemplo, de uma Carta de Confiança, a qual servirá de guia para todos os procedimentos de segurança cibernética.

A segurança cibernética deve atuar em prol da soberania nacional e o Brasil necessita estabelecer estratégias para executar uma gestão eficiente das capacidades de proteção dos diversos entes da sociedade, públicos e privados, pois o mundo vive uma *New Climate Change* com os benefícios decorrentes da tecnologia 5G, que, ao mesmo tempo, também apresenta facilidades para os agentes causadores das ameaças cibernéticas. Assim, para que a segurança prevaleça no espaço cibernético, é fundamental que seja construída uma eficaz rede de colaboração, fundamentada nos pilares da inteligência, competência e confiança.

CEBRI

CENTRO BRASILEIRO DE
RELAÇÕES INTERNACIONAIS

Associados

Instituições

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

Diretora-Presidente
Julia Dias Leite

Diretora Relações Institucionais e Comunicação
Carla Duarte

Diretora de Projetos
Luciana Gama Muniz

Projetos

Gerente de Projetos
Lara Azevedo

Consultoras
Cintia Hoskinson
Marianna Albuquerque

Estagiários
Gustavo Berlie
Larissa Vejarano

Relacionamento Institucional e Eventos

Gerente de Relações Institucionais e Eventos
Barbara Brant

Consultores
Caio Vidal
Nana Villa Verde

Estagiário
Lucas Bilheiro

Comunicação

Consultora
Gabriella Cavalcanti

Estagiário
Henrique Kress

Administrativo e Financeiro

Coordenadora Adminstrativa-Financeira
Fernanda Sancier

Assistente
Kelly C. Lima

CEBRI
CENTRO BRASILEIRO DE
RELAÇÕES INTERNACIONAIS

ONDE ESTAMOS:

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