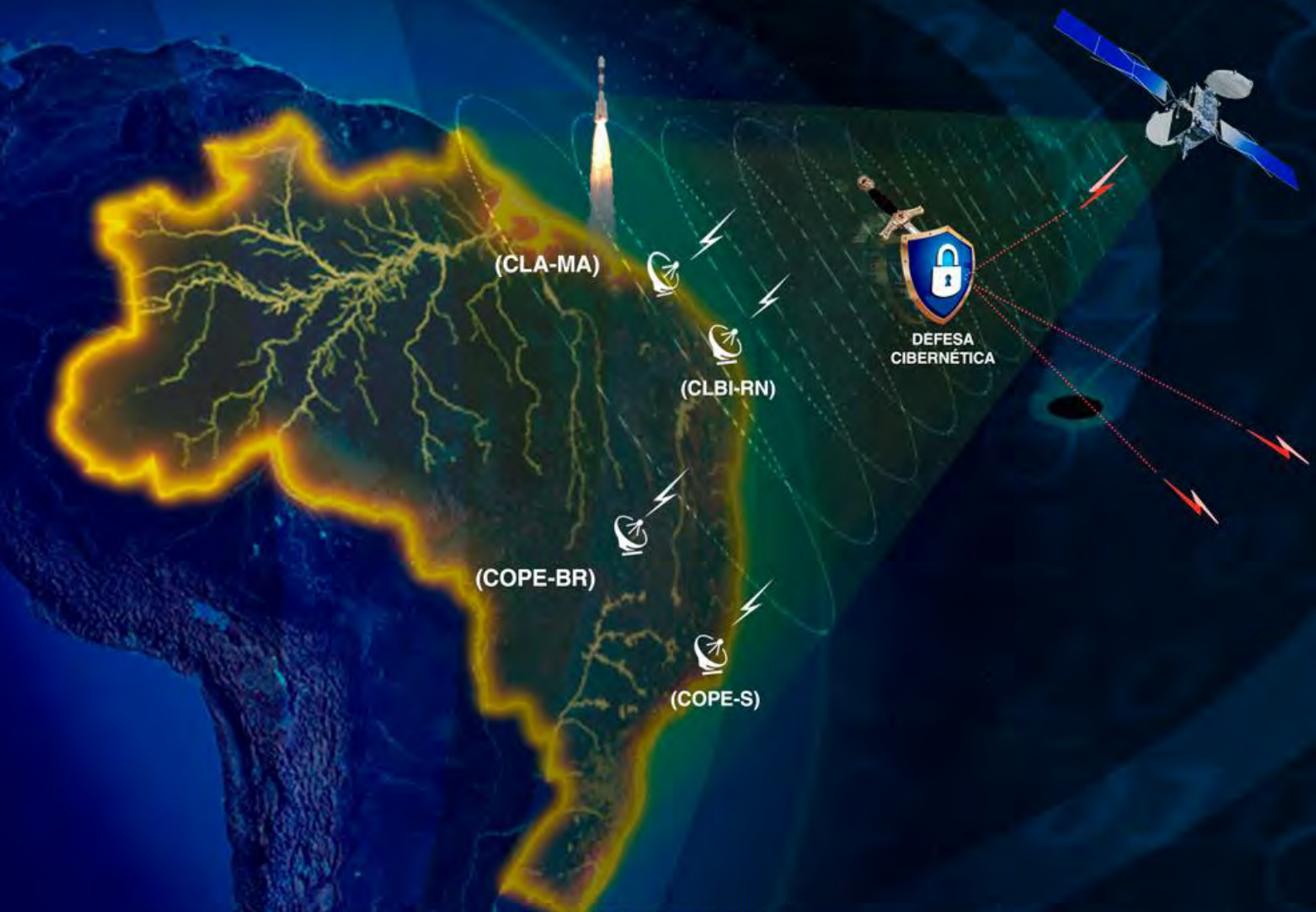
UNIVERSIDADE DA FORÇA AÉREA

II SEMINÁRIO DE SEGURANÇA E DEFESA CIBERNÉTICA

"Desafios da Defesa Cibernética na Projeção Espacial Brasileira"



ANAIS 2020

ORGANIZADORES:

Pedro Arthur Linhares Lima
Constança Maria Maia Arruda
Gills Vilar-Lopes
Rita Cristina Pedrosa de Paula Guimarães

FGV

REDE CTIDC

ANAIS DO II SEMINÁRIO DE SEGURANÇA E DEFESA CIBERNÉTICA

DESAFIOS DA DEFESA CIBERNÉTICA NA PROJEÇÃO ESPACIAL BRASILEIRA

Pedro Arthur Linhares Lima

Constança Maria Maia Arruda

Gills Vilar-Lopes

Rita Cristina Pedrosa de Paula Guimarães

(Organizadores)

Rio de Janeiro

2020

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DIRETORIA DE ENSINO
UNIVERSIDADE DA FORÇA AÉREA

Brig Ar Luís Renato de Freitas Pinto
Reitor

Brig Int Luiz Tirre Freire
Vice-Reitor Acadêmico

II SEMINÁRIO DE SEGURANÇA E DEFESA CIBERNÉTICA

Coordenadoria Geral
Cel Av Alexandre Nogueira de Sousa (CEA)
Cel Av R/1 Valdomiro Alves Fagundes (VRA)

Adjunto da Coordenadoria Geral e de Execução
Cel Av R/1 Francisco Sinval Nascimento e Souza (CEA)
SO QSS BMA R/1 Carlos José Gonçalves da Gama (CEA)

Comissão de Cerimonial
Cel Inf Refm Prof Dr Paulo Pereira Santos (CEA)
2º Ten QOCON REP Pollyana Rodrigues Pessoa Escalante (SCS)
3S QSS SAD Victor Hugo da Silva Gargalhone Corrêa (ACI)
2S QSS SAD Marcella Esteves Vita Santos (CEAD)

Coordenadoria de Controle, Execução Acadêmica e Avaliação dos Trabalhos Científicos
Brig Ar José Vagner Vital (CCISE)
Brig Int R/1 Pedro Arthur Linhares Lima (VRA)
Cel Av R/1 Mauro Barbosa Siqueira (VRA)
Ten Cel Av R/1 Paulo Roberto Batista (CEA)
Cap SV1 Rita Cristina Pedrosa de Paula Guimarães (CCA-RJ)
Prof Dr Gills Vilar Lopes (VRA)
Prof Me Catarina Labouré Madeira Barreto Ferreira (VRA)
Prof Me Constança Maria Maia Arruda (CCA-RJ)
Prof Dr Marcos Aurélio Guedes de Oliveira (UFPE)
Dr Cristiano Augusto Trein (AEB)

Apoio de Infraestrutura
Cel Av R/1 Antônio Paulo Monteiro de Miranda (SPAT)

Coordenadoria Técnica e Informacional
Cel Av Alexandre Nogueira de Sousa (CEA)
Cel Av R/1 Luiz Afonso Souza Henriques (SRT)
Maj Esp Com R/1 Renaldo Geronimo da Silva (SRT)

CB SGS Lessandro Augusto da Silva Queluci (VRA)

Apoio de Subsistência

Ten Cel Int Gustavo da Silva Welte (BAAF)

Comissão de Ligação com Palestrantes

Cel Av R/1 Francisco Sinval Nascimento e Souza (CEA)
Ten Cel Av R/1 Paulo Roberto Batista (CEA)
Cap SV1 Rita Cristina Pedrosa de Paula Guimarães (DECEA)
2º Ten QOCON PED Débora Leonel Peluso (PROFESP)
1º Ten QOAP BIB Izabel Cecília Yumi Tsuboi Mélo (PROAPE)
2º Ten QOCON PED Cleide Lisbôa de Almeida da Cruz (VRA)
2º Ten QOCON PED Thaíza Silva dos Santos (CEAD)

Comissão de Comunicação Social

2º Ten QOCON REP Pollyana Rodrigues Pessoa Escalante (SCS)
2S QSS SAD Luana Caroline Correa Rodrigues (SCS)
S2 QSD SNE Douglas Mascarenhas Vidal (SCS)

Coordenadoria Administrativa, Certificados, Divulgação, Convites, Inscrições e Credenciamento

Cel Av R/1 Francisco Sinval Nascimento e Souza (CEA)
Ten Cel Av R/1 Paulo Roberto Batista (CEA)
SO QSS BET Refm Jorge Luiz de Souza Azevedo (CEA)
SO QSS BMA R/1 Carlos José Gonçalves da Gama (CEA)

Apoio

Fundação Getúlio Vargas (FGV)
RedeCTIDC/Pró-Defesa IV (CAPES/MD)

As manifestações expressas por convidados que participaram dos eventos e transmissões on-line relativos ao II Seminário de Segurança e Defesa Cibernética, bem como dos autores de trabalhos, representam, exclusivamente, as suas próprias opiniões e não, necessariamente, a posição institucional da Universidade da Força Aérea (UNIFA) e das instituições parceiras neste evento.

Crédito das fotos das páginas 6, 11 e 269**:** www.flickr.com/photos/portalfab.
Site do evento**:** www.fab.mil.br/unifa/index.php/seminario.
Canal da UNIFA: www.youtube.com/c/unifa.
1ª edição, dez. 2020.

Ficha catalográfica elaborada pela Biblioteca da UNIFA

S471 Seminário de Segurança e Defesa Cibernética (2. : 2020 : Rio de Janeiro).
Anais do II Seminário de Segurança e Defesa Cibernética: desafios da defesa cibernética na projeção espacial brasileira / Universidade da Força Aérea; organizado por Pedro Arthur Linhares Lima, Constança Maria Maia Arruda, Gills Vilar-Lopes, Rita Cristina Pedrosa de Paula Guimarães. – Rio de Janeiro : Universidade da Força Aérea, 2020.
277 p.

ISBN 978-65-89535-00-3

1. Ciência política. 2. Defesa cibernética. 3. Segurança. I. Universidade da Força Aérea. II. Título.

CDU 007

SOBRE A UNIFA

Criada pelo Decreto nº 88.749, de 26 de setembro de 1983, a Universidade da Força Aérea (UNIFA) veio preencher uma lacuna no âmbito do Ensino Superior Brasileiro, particularmente, por se caracterizar como sucessora da tradição de ensino na Aeronáutica ao assumir a identidade de uma Organização de Ensino sediada no Campo dos Afonsos, berço da História e Tradições aeronáuticas no Brasil.

Sgt Batista / Força Aérea Brasileira

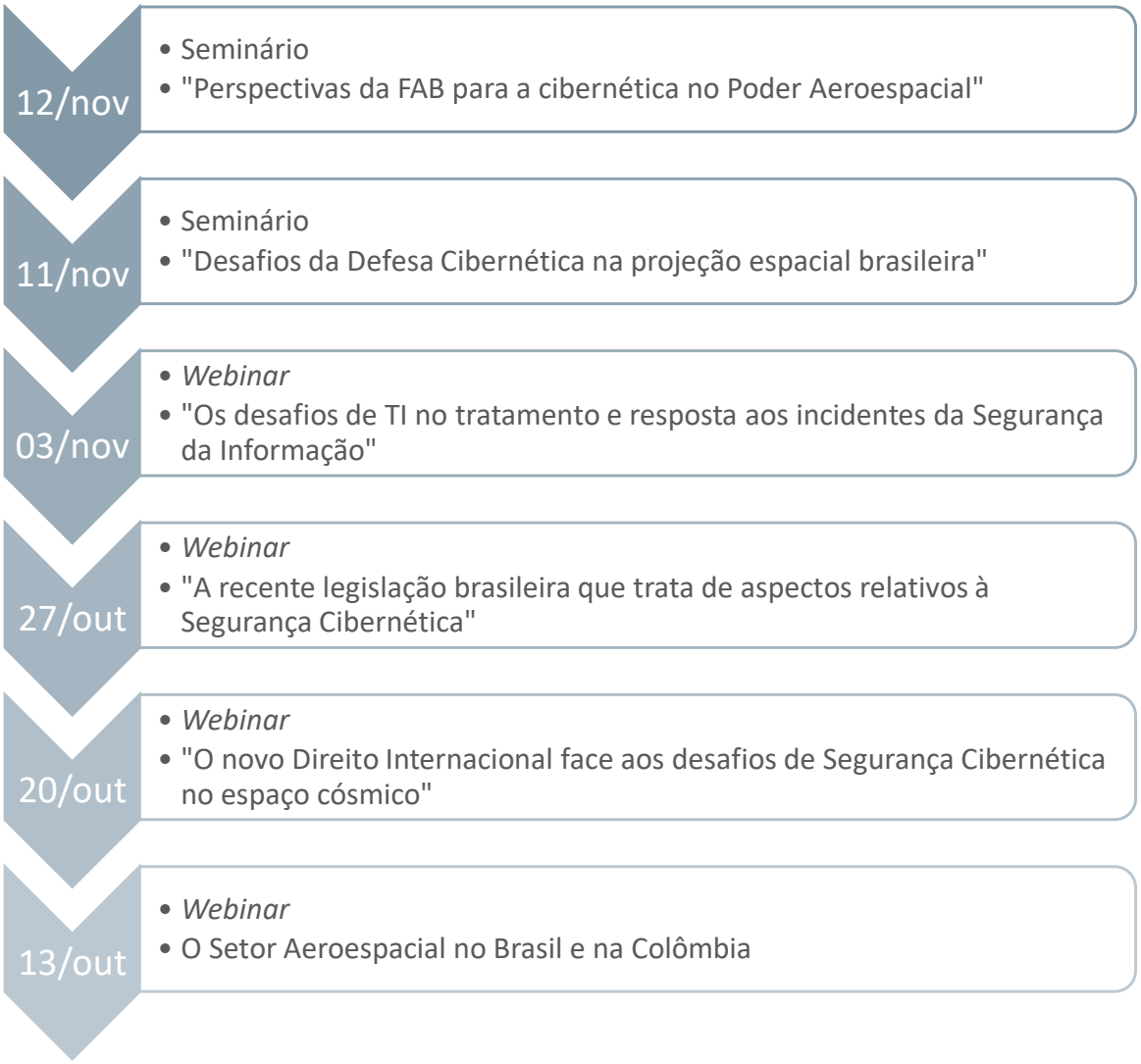
Seu caráter peculiar vem provocar uma reflexão sobre como processar o equilíbrio existente entre a historicidade acadêmica tradicional, desenvolvida em uma Universidade, e aquela de natureza militar e aeronáutica, influenciada pela própria representatividade do Campo dos Afonsos, apontando para o legítimo destino de atender a missões específicas em favor do avanço e fortalecimento do Poder Aeroespacial brasileiro.

A UNIFA, por sua singularidade, qualifica-se, então, como um *campus* ideal a debates de cunho científico, além da projeção de cenários às diversas temáticas, emanadas do ensino e da pesquisa, propiciando vasto potencial de estudos e conhecimentos sobre as atividades inerentes à concepção do Poder Aeroespacial.

SOBRE O EVENTO

O II Seminário de Segurança e Defesa Cibernética da Universidade da Força Aérea (UNIFA) foi organizado pelo Centro de Estudos Avançados (CEA-UNIFA) e teve como tema central “Desafios da Defesa Cibernética na Projeção Espacial Brasileira”.

Realizado na modalidade a distância, esta segunda edição foi composta por quatro *webinars* (13, 20 e 27 de outubro e 03 de novembro de 2020) e dois dias de eventos *on-line* (11 e 12 de novembro de 2020), contando com convidados – autoridades, palestrantes, moderadores e comentador – civis e militares do Brasil, Colômbia, Estados Unidos da América (EUA) e Itália cujas apresentações foram proferidas em português, inglês e espanhol.



SOBRE OS AUTORES

Aline Marchesini Pinto
Mestre em Direito pela Universidade Federal do Estado do Rio de Janeiro (UNIRIO) e Graduada em Direito pela Universidade Federal da Bahia (UFBA). Membro dos Grupos de Pesquisa NPJuris e GDAC. Atualmente é Delegada de Polícia Federal (PF) e encontra-se na Chefia do Núcleo de Correições na Superintendência Regional da PF no Rio de Janeiro.

André Lucas Alcântara da Silva
Oficial Engenheiro de Computação da Força Aérea Brasileira (FAB). Especialista em Gestão e Governança de Tecnologia da Informação. Mestrando em Ciências Aeroespaciais pela Universidade da Força Aérea (UNIFA).

Carlos Alberto Ferreira Bispo
Doutor em Engenharia de Produção pela Universidade de São Paulo (USP). Docente na Academia da Força Aérea (AFA), há 23 anos nas disciplinas de Tecnologias da Informação e Sistemas de Informação, e por 4 anos na Escola de Aperfeiçoamento de Oficiais da Aeronáutica (EAOAR).

Cícero Araújo Lisboa
Mestrando do Programa de Pós-Graduação em Estudos Estratégicos Internacionais (PPGEEI) da Universidade Federal do Rio Grande do Sul (UFRGS). Especialista em Gestão da Segurança e Defesa Cibernéticas pela UFRGS e Tecnólogo em Segurança da Informação pela Universidade do Vale do Rio dos Sinos (Unisinos).

Constança Maria Maia Arruda
Analista de Sistemas da Carreira de Tecnologia Militar, Mestre em Matemática Aplicada a Sistemas pela Universidade Federal Fluminense (UFF), possui Especialização em Governança de Tecnologia da Informação pelo Centro Universitário do Sul de Minas (UNIS/MG), Pesquisadora do PPGCA, da Universidade da Força Aérea (UNIFA), em que faz parte do Grupo de Pesquisa Científica em Segurança e Defesa Cibernética. Atualmente exerce suas atividades na Assessoria de Sistemas do Centro de Computação da Aeronáutica do Rio de Janeiro.

Érica Maia Campelo Arruda
Advogada, pesquisadora da Escola de Ciências Jurídicas (ECJ) da Universidade Federal do Estado do Rio de Janeiro (UNIRIO), professora da Universidade Estácio de Sá (UNESA), Doutora

em Direito pela Universidade Estácio de Sá (UNESA), Mestre em Direito e Políticas Públicas pelo Centro Universitário de Brasília (UniCEUB), Mestre em Projetos Sociais pelo Centro de Pesquisa e Documentação de História Contemporânea do Brasil (CPDOC/FGV) e Bacharel em Direito pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio).

Gills Vilar-Lopes
Professor de Relações Internacionais do PPGCA/UNIFA. Doutor e Mestre em Ciência Política pela Universidade Federal de Pernambuco (UFPE), com período-sanduíche na *Université Laval*, no Canadá. *Specialized Course* em *Cybersecurity: Issues in National and International Security* pela *National Defense University* (NDU), nos EUA. Pesquisador da RedeCTIDC/Pró-Defesa/CAPES/MD. Acadêmico de Direito na Faculdade Nacional de Direito (FND) da Universidade Federal do Rio de Janeiro (UFRJ).

Guilherme Ziebell
Professor colaborador do Programa de Pós-Graduação em Estudos Estratégicos Internacionais (PPGEEI) da Universidade Federal do Rio Grande do Sul (UFRGS). Doutor em Ciência Política pelo PPGPOL/UFRGS e mestre em Estudos Estratégicos Internacionais pelo PPGEEI/UFRGS.

Lucas França de Jesus
Cursa o último ano do Curso de Formação de Oficiais Aviadores na Academia da Força Aérea (AFA), em Pirassununga, SP.

Luciana Quagliane Ribeiro
Mestre em Saúde da Família pela Universidade Estácio de Sá (UNESA), Especialista em Saúde da Família pelo Ministério da Saúde e Universidade Estadual do Rio de Janeiro (UERJ). Bacharel e pós-graduanda em Direito. Servidora pública na Prefeitura Municipal do Rio de Janeiro, atualmente na gestão da Atenção Básica na Área Programática.

Patricy Barros Justino
Advogada, Doutoranda em Direito, na área de concentração em Direito Público e Evolução Social, pela UNESA, Mestre em Direito na área de concentração Estado e Cidadania pela Universidade Gama Filho. Professora da Escola da Magistratura do Estado do Rio de Janeiro (EMERJ). Pesquisadora do Projeto de Extensão da Liga de Direito e Literatura, da ECJ-UNIRIO. Pesquisadora do Instituto Nacional de Pesquisa e Promoção de Direitos Humanos (INPPDH).

Pedro Arthur Linhares Lima

Mestre em Ciência da Computação pelo *Air Force Institute of Technology*. Doutor em Engenharia de Produção pela UFRJ. MBA em Planejamento Estratégico pela COPPE-UFRJ. É professor do Programa de Pós-graduação em Ciências Aeroespaciais da Universidade da Força Aérea (UNIFA). É o coordenador da UNIFA no Projeto Ciência, Tecnologia e Inovação em Defesa: Cibernética e Defesa Nacional, do Programa Pro-Defesa IV. Participa de grupos de pesquisas na área de Segurança e Defesa Cibernética.

Rita Cristina Pedrosa de Paula Guimarães

Profissional da área de Tecnologia da Informação (TI) do Comando da Aeronáutica, atuante nas áreas de governança de TI, gestão de serviços de TI, análise e mapeamento de processos, docente na formação e capacitação do pessoal do Comando da Aeronáutica nessas áreas. Como fruto de sua pesquisa de mestrado intitulada "Governança de Tecnologia da Informação: aspectos relevantes para o emprego operacional da Força Aérea", dentre outros, participou da elaboração de normatizações técnicas e cursos nas áreas de Governança e Gestão de TI.

Silvio Roberto Assunção de Oliveira Filho

MSc Eng Comp ITA/SP – Instituto Tecnológico de Aeronáutica (ITA), São José dos Campos. Mestre na área de Comando e Controle com aplicação de Inteligência Artificial. Doutorando no ITA em Processos de Gestão e Políticas de Segurança Cibernética.

Viviane Souza da Costa

Doutoranda do Programa de Doutorado Profissional em Propriedade Intelectual e Inovação pelo Instituto Nacional da Propriedade Industrial (INPI). Membro do Grupo de Estudos Estratégicos em Propriedade Intelectual e Inovação para o Setor de Defesa (GEPID/INPI).

AGRADECIMENTOS

Ao Centro de Estudos Avançados (CEA) da Universidade da Força Aérea (UNIFA), sob a Chefia do Cel Av Alexandre Nogueira de Sousa, pela organização geral do evento.

À Fundação Getúlio Vargas (FGV), em especial à FGV Projetos, por dispor de seus melhores recursos humanos e tecnológicos em favor da divulgação, gravação e disponibilização dos seis dias de evento *on-line*.

À Rede de Ciência, Tecnologia e Inovação em Defesa Cibernética e Defesa Nacional (RedeCTIDC), no âmbito do Programa de Apoio ao Ensino e à Pesquisa Científica em Defesa Nacional (Pró-Defesa IV/CAPES/MD), coordenada pelo Prof Dr Marcos Aurélio Guedes de Oliveira (UFPE), pelo apoio acadêmico e divulgação científica.

Às Tenentes Mélo, Salles e Marinho, da UNIFA, pelo apoio na obtenção do ISBN.

Aos membros da Comissão Científica, pelas avaliações – de forma e conteúdo – dos trabalhos submetidos.

A todos os convidados, inscritos, autores de trabalho e colaboradores que contribuíram para o sucesso do II Seminário de Segurança e Defesa Cibernética da UNIFA.

Sgt Batista / Força Aérea Brasileira

O ambiente cibernético também se apresenta como um fator sensível ao desempenho de uma força aérea. Este aspecto tende a ter sua importância exacerbada no futuro. Portanto, é primordial que a FAB mantenha-se continuamente atualizada no uso do espaço cibernético.

CONCEPÇÃO ESTRATÉGICA FORÇA AÉREA 100, 2018.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABIMDE	Associação Brasileira das Indústrias de Materiais de Defesa e Segurança
ABNT	Associação Brasileira de Normas Técnicas
AEB	Agência Espacial Brasileira
A&D	Aeroespaço e Defesa
AFA	Academia da Força Aérea
APF	Administração Pública Federal
ASAT	Arma antissatélite
Av	Aviador
Bacen	Banco Central
BDICN	Base de Dados da Identificação Civil Nacional
BID	Base Industrial de Defesa
Brig	Brigadeiro
Brig Ar	Brigadeiro do Ar
Brig Int	Brigadeiro Intendente
CCA-BR	Centro de Computação da Aeronáutica de Brasília
C^2	Comando e Controle
CCISE	Comissão de Coordenação e Implantação de Sistemas Espaciais
CDCAER	Centro de Defesa Cibernética da Aeronáutica
CDCiber	Centro de Defesa Cibernética do Exército
CEA	Centro Espacial de Alcântara
	Centro de Estudos Avançados da UNIFA
CERT.br	Centro de Estudos, Tratamento e Resposta a Incidentes de Segurança no Brasil
CID	Confidencialidade, integridade e disponibilidade
CISB	Centro de Pesquisa e Inovação Sueco Brasileiro
COMAER	Comando da Aeronáutica
ComDCiber	Comando de Defesa Cibernética
COPE	Centro de Operações Espaciais
COPUOS	*United Nations Committee on the Peaceful Uses of Outer Space*
CF88	Constituição da República Federativa do Brasil de 1988
CSIRT	*Computer Security Incident Response Team*
CTIR.FAB	Centro de Tratamento de Incidentes de Redes da Força Aérea Brasileira
CTIR Gov	Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo
COTS	*Commercial Off-The-Shelf*
CVM	Comissão de Valores Mobiliários
DMDC	Doutrina Militar de Defesa Cibernética
DICA	Direito Internacional dos Conflitos Armados
	Disponibilidade, integridade, confidencialidade e acessibilidade

DoS	*Denial Of Service*
Dr/Dra	Doutor/Doutora
DTI	Diretoria de Tecnologia da Informação da Aeronáutica
E-Ciber	Estratégia Nacional de Segurança Cibernética
ED	Empresas de Defesa
EED	Empresas Estratégicas de Defesa
EMAER	Estado-Maior da Aeronáutica
EMCFA	Estado-Maior Conjunto das Forças Armadas
EMERJ	Escola da Magistratura do Estado do Rio de Janeiro
EnaDCiber	Escola Nacional de Defesa Cibernética
END	Estratégia Nacional de Defesa
EPFAC	*Escuela de Postgrados de la Fuerza Aérea Colombiana*
ESA	*European Space Agency*
ETIR	Equipe de Tratamento e Resposta a Incidentes Cibernéticos
EUA	Estados Unidos da América
Europol	*European Union Agency for Law Enforcement Cooperation*
FA	Forças Armadas
FAB	Força Aérea Brasileira
FGV	Fundação Getúlio Vargas
GDPR	*General Data Protection Regulation*
Gen Bda	General de Brigada
GPS	*Global Positioning System*
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
IA	Inteligência Artificial
IC	Instalações críticas
ICT	Instituição Científica e Tecnológica
INPI	Instituto Nacional da Propriedade Industrial
ITA	Instituto Tecnológico de Aeronáutica
ITU	União Internacional de Telecomunicações
LAI	Lei de Acesso à Informação
LBDN	Livro Branco de Defesa Nacional
LGPD	Lei Geral de Proteção de Dados Pessoais
Maj Brig	Major-Brigadeiro
Maj Brig Ar	Major-Brigadiero-do-Ar
MD	Ministério da Defesa
Me	Mestre/a
MECB	Missão Espacial Completa Brasileira
MPF	Ministério Público Federal
MRE	Ministério das Relações Exteriores
NASA	*National Aeronautics and Space Administration*

NIST	*National Institute of Standards and Technology*
NSA	*National Security Agency*
Nu CDCiber	Núcleo do Centro de Defesa Cibernética do Exército
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OM	Organização Militar
OND	Objetivos Nacionais de Defesa
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
PbD	*Privacy by Design*
PCD	Política Cibernética de Defesa
PEB	Programa Espacial Brasileiro
PESE	Programa Estratégico de Sistemas Espaciais
PI	Propriedade Intelectual
PMA	Poder Militar Aeroespacial
PNCS	Política Nacional de Cibersegurança do Chile
PND	Política Nacional de Defesa
PNSI	Política Nacional de Segurança da Informação
PNSIC	Política Nacional de Segurança de Infraestruturas Críticas
PNTIR	Plano Nacional de Tratamento e Resposta a Incidentes Computacionais
PPGCA	Programa de Pós-Graduação em Ciências Aeroespaciais
Prof	Professor/a
PSM	*Problem Structuring Methods*
RedeCTIDC	Rede de Ciência, Tecnologia e Inovação em Defesa Cibernética e Defesa Nacional
RF	Radiofrequência
SAE	Secretaria de Assuntos Estratégicos da Presidência da República
SBDA	Associação Brasileira de Direito Aeronáutico e Espacial
SC	Segurança Cibernética
SDR	Rádio Definido por Software
SGDC	Satélite Geoestacionário de Defesa e Comunicações Estratégicas
SISMC²	Sistema Militar de Comando e Controle
SMDC	Sistema Militar de defesa Cibernética
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
SWF	*Secure World Foundation*
TCU	Tribunal de Contas da União
TED	Termo de Execução Descentralizada
Ten Brig Ar	Tenente-Brigadeiro-do-Ar
Ten Cel	Tenente-Coronel
TI	Tecnologia da Informação
TIC	Tecnologias da informação e da comunicação

TPI	Tribunal Penal Internacional
TJRJ	Tribunal de Justiça do Estado do Rio de Janeiro
UE	União Europeia
UNIFA	Universidade da Força Aérea
USSF	*United States Space Force*
VFT	*Value-Focused Thinking*

SUMÁRIO

PREFÁCIO

Brig Ar Luís Renato de Freitas Pinto
Comandante Interino da Universidade da Força Aérea

Esta coletânea resulta da compilação de uma série de trabalhos apresentados no II Seminário de Segurança e Defesa Cibernética, realizado pela Universidade da Força Aérea (UNIFA) e que abordou o tema "Desafios da Defesa Cibernética na Projeção Espacial Brasileira".

Abordagens ligadas aos setores cibernético e espacial são primordiais para o fortalecimento da Defesa nacional, elencados como prioritários pela Estratégia Nacional de Defesa – para a Força Aérea Brasileira, com forte dependência de um alto grau de desenvolvimento tecnológico e de um adequado nível de capacitação profissional, tais temas tornam-se essenciais. Por tais características, o desenvolvimento de estudos relacionados aos assuntos no âmbito da UNIFA se mostra primordial para o alcance do panorama futuro desejado para a Organização, exposto na visão de *"ser reconhecida nacional e internacionalmente como Universidade de referência na produção e na difusão de conhecimentos relacionados ao Poder Aeroespacial".*

Estabelecida no formato de um *campus* universitário, localizado no legendário Campo dos Afonsos, a UNIFA incorpora as principais escolas de pós-formação de oficiais da Força Aérea Brasileira – a Escola de Comando e Estado-Maior da Aeronáutica (ECEMAR) e a Escola de Aperfeiçoamento de Oficiais da Aeronáutica (EAOAR). Primeira universidade militar a ser criada na América Latina, e até o presente momento a única do Brasil, tem como missão *"promover a pós-formação acadêmica e profissional por meio das atividades de ensino, pesquisa e extensão, com vistas ao desenvolvimento do Poder Aeroespacial Brasileiro".*

Com este foco, o Seminário foi conduzido por meio de quatro *webinars,* seguidos por dois dias de evento *on-line*, e contou com palestrantes civis e militares nacionais e internacionais, centrados em dois eixos temáticos: "Convergência estratégica entre os setores cibernético e espacial" e "A dimensão da cibernética no Poder Aeroespacial: perspectivas para a FAB".

Entendemos assim ser possível contribuir com a construção de um conhecimento que se mostra fundamental, além de propiciar o estreitamente de laços e parcerias com outras Instituições acadêmicas que desenvolvem estudos sobre o tema.

A difusão destes conhecimentos converte-se ainda em poderoso instrumento de projeção do Brasil e de suas capacidades, enquanto figura emergente em um mundo complexo e interligado. Como Universidade, seguimos firmes na abnegada missão de contribuir para o desenvolvimento da nossa Força Aérea, da nossa sociedade e do nosso País.

Uma excelente leitura a todos!

APRESENTAÇÃO

Pedro Arthur Linhares Lima
Constança Maria Maia Arruda
Gills Vilar-Lopes
Rita Cristina Pedrosa de Paula Guimarães

A Universidade da Força Aérea (UNIFA), por meio do seu Centro de Estudos Avançados (CEA), promoveu a segunda edição do Seminário de Segurança e Defesa Cibernética, evento que foi, pela primeira vez, totalmente realizado por meio digital.

O tema deste ano foi "Desafios da Defesa Cibernética na Projeção Espacial Brasileira", o qual foi escolhido por estar em alinhamento às diretrizes superiores para o fortalecimento da pesquisa e do desenvolvimento em áreas estratégicas para o País, como são os casos da espacial e da cibernética.

Ao longo do evento, ficou latente que os desafios postos à Projeção Espacial Brasileira também tocam diretamente a dimensão cibernética, fazendo, portanto, da Defesa Cibernética uma Ação de Força Aérea. Ao mesmo passo, discutiu-se como a segurança e a defesa cibernéticas do Setor Espacial são estrategicamente pensadas e postas em prática pela Força Aérea Brasileira (FAB) e por *stakeholders* e pesquisadores dos setores espacial e/ou cibernético. Dessa forma, foram convidados palestrantes nacional e internacionalmente reconhecidos em suas áreas de atuação, entre civis e militares.

Como público/audiência interna, tivemos profissionais ligados ao Preparo e Emprego da FAB, bem como civis e militares cujas áreas de interesse estão voltadas para os setores cibernético e/ou espacial. Além disso, o público externo foi composto majoritariamente por representantes da comunidade acadêmica, cujas áreas de pesquisa foram ao encontro das temáticas propostas pelo II Seminário.

Acreditamos que os debates oriundos da interação entre palestrantes e público-alvo proporcionaram uma oportunidade singular para a construção de uma visão abrangente em prol tanto da soberania quanto do desenvolvimento nacional brasileiro. Isso ficou comprovado pelo número de visualizações do evento tanto em tempo real quanto remoto.

Tendo em vista a modalidade digital, o Seminário foi dividido em dois momentos. No primeiro deles, tivemos os *webinars*, que trataram de temas preparatórios, sendo transmitidos sempre às terças-feiras das 10h às 12h. E, no segundo momento, o evento

principal se desenrolou nos dias 11 e 12 de novembro de 2020, com três horas de duração cada um deles.

Assim, com o objetivo de fomentar a pesquisa acerca dos Desafios da Defesa Cibernética na Projeção Espacial Brasileira, o II Seminário de Segurança e Defesa Cibernética buscou estabelecer debates sobre áreas de convergência estratégica entre os Setores Espacial e Cibernético. Para tanto, houve a publicação de um edital de chamadas de trabalhos científicos destinado para discentes e docentes de cursos de pós-graduação, pesquisadores e autônomos. Em linhas gerais, os trabalhos versaram sobre dois eixos temáticos. O primeiro foi *Convergência estratégica entre os setores cibernético e espacial, com os subtemas*: O "novo" Direito internacional face aos desafios da segurança cibernética no espaço cósmico; A recente legislação brasileira que trata de aspectos relativos à segurança cibernética; e Os desafios da Tecnologia da Informação no tratamento e resposta aos incidentes de segurança da Informação. E o segundo Eixo Temático foi *A dimensão da cibernética no Poder Aeroespacial – perspectivas para a FAB,* com os subtemas: O setor aeroespacial brasileiro; e A indústria de Defesa no setor aeroespacial brasileiro.

Diante desse curto espaço de tempo e da atualidade dos temas, vale destacar que foram recebidos 12 trabalhos. Isso pode indicar que se faz necessária uma maior sensibilização dos assuntos tratados neste II Seminário, junto à comunidade acadêmica, para que juntos possamos atender ao previsto na Estratégia Nacional de Defesa (END) brasileira, que elegeu os Setores Cibernético e Espacial como Estratégicos para a Defesa Nacional, pois ambos requerem alto grau de desenvolvimento tecnológico, aperfeiçoamento militar e análises de conjuntura.

Para deixar esta obra o mais didática possível, dividimo-la em duas partes principais: a primeira traz dados mais gerais sobre o evento, como quantidade de inscritos, visualizações e participantes, bem como resume o conteúdo debatido ao longo dos seis dias de evento.

Já a segunda parte traz a íntegra dos trabalhos aprovados e apresentados neste Seminário. No primeiro trabalho, Lucas França de Jesus e Carlos Alberto Ferreira Bispo realizam uma análise acerca dos benefícios de *pentests* regulares nas redes do Comando da Aeronáutica (COMAER). Em seguida, Silvio Roberto Assunção de Oliveira Filho apresenta uma metodologia de classificação e priorização de ativos de tecnologia da informação (TI) para a área da Segurança Cibernética. Por sua vez, Cícero Araújo Lisboa e Guilherme Ziebell discutem a relevância e as possibilidades do conceito de dissuasão cibernética. Já André Lucas Alcântara

da Silva elenca e discorre sobre as principais ameaças cibernéticas para os sistemas espaciais. Viviane Souza da Costa, por sua vez, proporciona uma defesa da propriedade intelectual contra ataques cibernéticos nas infraestruturas do setor aeroespacial brasileiro, enquanto Patricy Barros Justino e Érica Maia Campelo Arruda relacionam a recente Lei Geral de Proteção de Dados (LGPD) com os riscos cibernéticos e o chamado “seguro cibernético". Patricy Barros Justino retorna para, conjuntamente com Patricy Barros Justino, compararem a Estratégia Nacional de Segurança Cibernética (E-ciber) com estratégias de outros países, demonstrando a importância da política e do direito internacional comparado para os estudos cibernéticos. Por seu turno, Aline Marchesini Pinto e Érica Maia Campelo Arruda trazem à tona os desafios que envolvem o *compliance* para a adequação à LGPD. Por fim, Érica Maia Campelo Arruda e Patricy Barros Justino retornam para trazer novamente a LGPD ao centro dos debates, correlacionando-a com os cometimentos de crimes cibernéticos e a adesão do Brasil à Convenção de Budapeste.

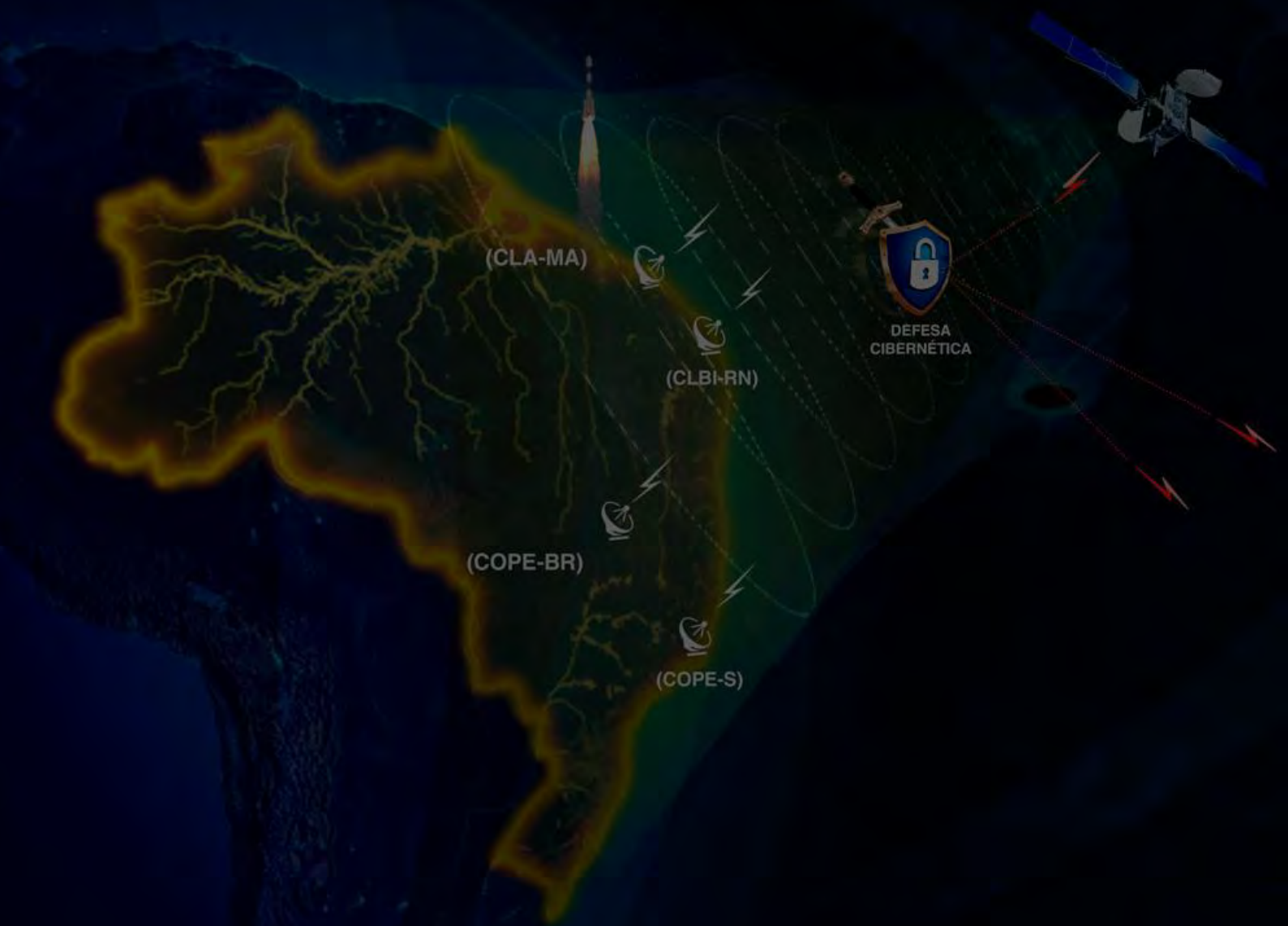
Ao final da obra, encontram-se, ainda, as Considerações Finais sobre o evento, o tema e os desafios que, acreditamos, foram superados na medida em que, de um lado, a UNIFA conseguiu organizar um seminário internacional com envergaduras logística, tecnológica e acadêmica compatíveis com a relevância estratégica das discussões arroladas neste II Seminário de Segurança e Defesa Cibernética. A título de complementação e memória institucional, incluímos, como Apêndices, alguns documentos que auxiliaram na organização acadêmica deste evento

Assim, esperamos que a publicação destes Anais contribua com a divulgação e o debate científicos sobre os Setores Estratégicos Espacial e Cibernético, bem como incentive pesquisadoras e pesquisadores a desenvolverem, cada vez mais, trabalhos afetos a essas áreas, ou melhor, entre elas. Logo, o ledor encontrará aqui uma pequena, mas significativa, amostra do cenário atual em relação aos Desafios da Defesa Cibernética na Projeção Espacial Brasileira.

Campo dos Afonsos/RJ, 15 de dezembro de 2020.

Os organizadores.

PARTE 1



EVENTOS & PALESTRAS

FGV

REDE CTIDC

Introdução

Devido à pandemia do Covid-19, o II Seminário de Segurança e Defesa Cibernética da UNIFA foi realizado 100% *on-line*, por meio de: quatro *webinars* com 2h (duas horas) de duração cada um, sempre às terças-feiras pela manhã; e duas manhãs seguidas, com duração de 3h (três horas) cada. Assim, a carga horária (CH) total do evento, para fins de certificação dos ouvintes, foi de 14h (quatorze horas).

O Quadro 1 apresenta a programação completa de todos esses seis eventos que compuseram o II Seminário, bem como os *links* para seus respectivos vídeos, que estão disponíveis no canal da UNIFA no YouTube (www.youtube.com/c/unifa).

Quadro 1 – Programação completa do evento

Data/hora	Eixo	Tema	Convidado/a	*Link*
13/10/2020 10h-12h	O Setor Aeroespacial no Brasil e na Colômbia	Palavras de Abertura	Prof Me André Coelho (FGV)	
		Comentários Introdutórios	Brig Int Pedro Arthur Linhares Lima (UNIFA)	
		Os desafios para implantação e desenvolvimento do Setor Aeroespacial Brasileiro	Brig Ar José Vagner Vital (CCISE)	
		As capacidades da Base Industrial de Defesa e Segurança (BIDS) em cibernética para o Setor Espacial	Dr Roberto Gallo (ABIMDE)	▶
		Desafios multidomínios para a Força Aérea Colombiana	Ten Cel Rodrigo Mezu Mina (EPFAC)	
		A formação de *clusters* para o desenvolvimento tecnológico espacial e cibernético	Prof Dr Álvaro Cyrino (FGV)	
		Mediação	Cel Av Donald Gramkow (EMAER)	
20/10/2020 10h-12h	O novo Direito Internacional face aos desafios de Segurança Cibernética no espaço cósmico	Palavras de Abertura	Prof Dr Bianor Scelza Cavalcanti (FGV)	
		Comentários Introdutórios	Brig Int Pedro Arthur Linhares Lima (UNIFA)	
		Segurança Cibernética no espaço exterior: a próxima fronteira para segurança das atividades espaciais	Me Victoria Samson (SWF)	
			Me Ana Cristina Galhego Rosa (Dipteron)	▶
		Como tratar os crimes cibernéticos no espaço extra-atmosférico	Prof Dr Sergio Marchisio (*Università La Sapienza di Roma*)	
			Dra Tatiana Ribeiro Viana	

		Mediação	Maj Brig Ar Adyr da Silva (SBDA)	
27/10/2020 10h-12h	A recente legislação brasileira que trata de aspectos relativos à Segurança Cibernética	Palavras de Abertura	Prof Me André Coelho (FGV)	
		Comentários introdutórios	Brig Int Pedro Arthur Linhares Lima (UNIFA)	
		A Política Nacional de Segurança da Informação e a Estratégia Nacional de Segurança Cibernética (E-Ciber)	Desembargador Nagib Slaibi Filho (TJRJ e EMERJ)	
		O impacto da Política e Estratégia Nacional de Segurança Cibernética e a entrada em vigor da Lei Geral de Proteção de Dados (LGPD)		
		Mediação	Prof Walter Aranha Capanema (EMERJ)	
03/11/2020 10h-12h	Os desafios de tecnologia da informação no tratamento e resposta aos incidentes da Segurança da Informação	Palavras de Abertura	Prof Dr Bianor Scelza Cavalcanti (FGV)	
		A importância e maturidade dos CSIRTs e a cooperação em âmbito nacional e internacional	Dra Cristine Hoepers (CERT.br)	
		Centro de Tratamento e Resposta a Incidentes de Rede da FAB (CTIR.FAB)	Cel Eng Willian Henrique da Silva Gomes (DTI/CCA-BR)	
		Mediação	Brig Int Pedro Arthur Linhares Lima (UNIFA)	
11/11/2020 9h-12h	Desafios da Defesa Cibernética na projeção espacial brasileira	Comentários Introdutórios	Prof Dr Carlos Ivan Simonsen Leal (FGV)	
		Abertura Oficial	Brig Ar Luís Renato de Freitas Pinto (UNIFA)	
		Palestra de Abertura	Ten Brig Ar Marcelo Kanitz Damasceno (EMAER)	
		Os recentes avanços do Governo Federal em prol da Segurança Cibernética	Gen Bda Antônio Carlos de Oliveira Freitas (GSI)	
		Diálogo entre as esferas do Setor Cibernético no País	Gen Bda Jomar Barros de Andrade (CDCiber)	
		A Defesa Cibernética no Brasil e o Poder Aeroespacial	Brig Ar Marco Aurélio Martins Gabriel (ComDCiber)	
		Os desafios do Setor Estratégico Cibernético no Poder Aeroespacial	Brig Int Luiz Fernando Moraes da Silva (DTI)	
		Mediação	Brig Int Pedro Arthur Linhares Lima (UNIFA)	
12/11/2020 9h-12h	Perspectivas da FAB para a	Comentários Introdutórios	Brig Int Pedro Arthur Linhares Lima (UNIFA)	

	cibernética no Poder Aeroespacial	Palestra de Abertura	Maj Brig Ar João Campos Ferreira Filho (EMAER)	
		O componente cibernético na Política Espacial Brasileira	Brig Ar Paulo Eduardo Vasconcellos (AEB)	
		Interferências cibernéticas nas atividades espaciais – tratamento dispensado	Diplomata André João Rypl (MRE)	
		A dimensão cibernética no Satélite Geoestacionário Brasileiro (SGDC)	Ten Cel Av Luis Felipe de Moura Nohra (COPE)	
		Mediação	Brig Ar José Vagner Vital (CCISE)	

Fonte: os autores.

Vale ressaltar que, em todos esses dias, a audiência pode interagir com os palestrantes via plataforma Slido (www.sli.do), cujo *link* foi previamente disponibilizado pela equipe da FGV na descrição das respectivas transmissões. A sistemática de tal aplicativo se mostrou assaz simples e eficiente: a audiência realizava perguntas – as quais, inclusive, puderam ser feitas de forma anônima –; a organização do evento as triava e repassava ao mediador; e este as endereçava a um/a determinado/a palestrante.

Todo o evento foi transmitido ao vivo no canal do YouTube da FGV (https://www.youtube.com/channel/UC8DhN1cJi0QklBQot5hv_kg), cujas gravações estão atualmente disponíveis tanto naquele repositório quanto no da UNIFA. Para se ter uma dimensão dessa estatística, apresentamos a Tabela 1, que mostra algumas informações importantes acerca do alcance e do impacto quantitativo do evento.

Tabela 1 – Estatísticas dos vídeos do evento

Data	Visualizações	Cliques em "Gostei"	Cliques em "Não gostei"
13/10/2020	1.138	130	2
20/10/2020	1.584	95	0
27/10/2020	793	84	4
03/11/2020	2.846	112	4
11/11/2020	2.425	141	4
12/11/2020	938	96	0
	9.724	**658**	**14**

Fonte: https://www.youtube.com/channel/UC8DhN1cJi0QklBQot5hv_kg e https://www.youtube.com/c/unifa.
Nota: Última atualização: 12 dez. 2020.

Como se vê na Tabela 1, foram ao todo, até 12/12/2020, 9.724 visualizações, *i.e.*, uma média de 1.621 visualizações por transmissão. Isso supera muito as 633 inscrições formalizadas – por meio de formulário do Google Docs – de 24 de setembro a 24 de novembro

de 2020. Até mesmo a transmissão do dia 27/10/2020, que apresenta o menor número de visualizações, 793, supera igualmente o de inscritos totais no evento.

Ademais, o número de visualizações e cliques no botão "Gostei" aponta para uma predileção da audiência em torno do *webinar* transmitido no dia 03 de novembro – cujo tema foi "Os desafios de tecnologia da informação no tratamento e resposta aos incidentes da Segurança da Informação" – e do primeiro dia do Seminário, em 11 de novembro, cujo Eixo Temático foi "Desafios da Defesa Cibernética na projeção espacial brasileira". Neste último dia também foi registrada a maior quantidade de cliques no botão "Gostei" em um único dia: 141, ao todo. Em suma, acreditamos que muito desse sucesso advém da pertinência dos temas tratados e debatidos, bem como da qualidade das palestras e do perfil dos convidados, cuja listagem completa é apresentada no Quadro 2.

Quadro 2 – Convidados do evento (por ordem alfabética)

Id	Nome	País	Atuação profissional	Formação acadêmico
01	Adyr da Silva, Maj Brig Ar		Presidente da Associação Brasileira de Direito Aeronáutico e Espacial (SBDA)	Doutor em Direito e Economia pela *Université Paul Cézanne Aix Marseille III*, na França
02	Alvaro Bruno Cyrino, Prof Dr		Professor Adjunto e vice-diretor da Escola Brasileira de Administração Pública e de Empresas (EBAPE) da Fundação Getúlio Vargas (FGV)	Doutor em Estratégia e Política de Empresas pela *Ecole de Hautes Etudes Commerciales*, na França.
03	Ana Cristina Galhego Rosa, Me		Fundadora e CEO da Dipteron	Mestre em *Air and Space Law* pela *Universiteit Leiden*, na Alemanha
04	André Meyer Coelho, Prof Me		Gerente de Projetos da FGV Projetos	Doutorando no Programa de Pós-graduação em Políticas Públicas, Estratégias e Desenvolvimento do Instituto de Economia (PPED) da Universidade Federal do Rio de Janeiro (UFRJ)
05	André João Rypl, Dip		Diplomata de carreira do Itamaraty e membro do *United Nations Committee on the Peaceful Uses of Outer Space* (COPUOS)	Formado no Instituto Rio branco (IRBr)
06	Antônio Carlos de Oliveira Freitas, Gen Bda		Assessor Especial de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR)	Doutor em Ciências Militares pela Escola de Comando e Estado-Maior do Exército (ECEME)
07	Bianor Scelza Cavalcanti, Prof Dr		Professor Titular na Escola Brasileira de Administração Pública e	Doutor em *Public Administration and Policy* pela *Virginia*

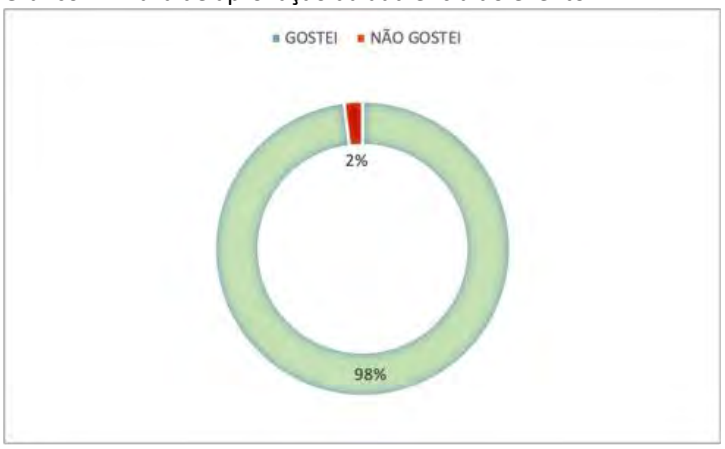
			de Empresas (EBAPE) da Fundação Getúlio Vargas (FGV)	*Polytechnic Institute and State University* (Virginia Tech)
08	Carlos Ivan Simonsen Leal, Prof Dr		Presidente da FGV	Doutor em Economia pela *Princeton University*, nos EUA
09	Cristine Hoepers, Dra		Analista de Segurança Senior e Gerente Geral do Centro de Estudos, Tratamento e Resposta a Incidentes de Segurança no Brasil (CERT.br)	Doutora em Computação Aplicada pelo Instituto Nacional de Pesquisas Espaciais (INPE)
10	Donald Gramkow, Cel Av		Chefe da Seção de Atividades Espaciais do Estado-Maior da Aeronáutica (EMAER)	Bacharel em Ciências da Computação pela Universidade Federal de Santa Maria (UFSM)
11	João Campos Ferreira Filho, Maj Brig Ar		Chefe da Terceira Subchefia do Estado-Maior da Aeronáutica (EMAER)	
12	Jomar Barros de Andrade, Gen Bda		Chefe do Centro de Defesa Cibernética (CDCiber)	Mestre em Ciências Militares pela Escola de Comando e Estado-Maior do Exército (ECEME)
13	José Vagner Vital, Brig Ar		Vice-Presidente da Comissão de Coordenação e Implantação de Sistemas Espaciais (CCISE/FAB)	Mestre em *Microwave Engineering* pelo *Institute of High Frequency Engineering* da *Technische Universitaet Muenchen*, na Alemanha
14	Luis Felipe de Moura Nohra, Ten Cel Av		Chefe da Seção de Análise de Operações Espaciais do Centro de Operações Espaciais (COPE)	Mestre em Engenharia Eletrônica e Computação pelo ITA
15	Luiz Fernando Moraes da Silva, Brig Int		Diretor da Diretoria de Tecnologia da Informação da Aeronáutica (DTI)	Pós-graduado em Análise e Projeto de Sistema pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio)
16	Luís Renato de Freitas Pinto, Brig Ar		Reitor da Universidade da Força Aérea (UNIFA)	Especialista em Desenvolvimento Gerencial Avançado pela Universidade Federal Fluminense (UFF)
17	Marco Aurélio Martins Gabriel, Brig Ar		Chefe do Estado Maior Conjunto do Comando de Defesa Cibernética	Especialista em Análises de Sistema pelo Instituto Tecnológico da Aeronáutica (ITA)
18	Marcelo Kanitz Damasceno, Ten Brig Ar		Chefe do Estado-Maior da Aeronáutica (EMAER)	Administração de Empresas pela Universidade de Santa Catarina
19	Nagib Slaibi Filho, Desembargador		Desembargador do Tribunal de Justiça do Rio de Janeiro (TJRJ)	Presidente do Comitê de Governança de Tecnologia da Informação e Comunicação (CGTIC/TJRJ)
20	Paulo Eduardo Vasconcellos, Brig Ar		Diretor da Diretoria de Inteligência Estratégica e Novos Negócios da Agência Espacial Brasileira (AEB)	MBA em Gestão Estratégica da Tecnologia da Informação pela FGV
21	Pedro Arthur Linhares Lima, Brig Int		Professor do Programa de Pós-Graduação em Ciências Aeroespaciais	Doutor em Engenharia de Produção pela Universidade Federal do Rio de Janeiro (UFRJ)

			(PPGCA) da Universidade da Força Aérea (UNIFA)	
22	Roberto Gallo, Dr		Presidente da Associação Brasileira das Indústrias de Materiais de Defesa e Segurança (ABIMDE)	Doutor em Ciência da Computação pela Universidade Estadual de Campinas (UNICAMP)
23	Rodrigo Mezu Mina, Ten Cel		Comandante do Grupo Acadêmico nº 2 da *Escuela de Postgrados de la Fuerza Aérea Colombiana* (EPFAC)	Doutorando em Ciência Política pela *Universidad de los Andes*, na Colômbia
24	Sergio Marchisio, Prof Dr		Professor Titular de Direito Internacional e Direito Espacial da *Università La Sapienza di Roma* e pesquisador na *European Space Agency* (ESA)	PhD
25	Tatiana Ribeiro Viana, Dra		Consultora Jurídica em Direito Espacial	Doutora em Direito Público, Comparado e Internacional pela *Università La Sapienza di Roma*, na Itália
26	Victoria Samson, Me		Diretora do Escritório em Washington da *Secure World Foundation* (SWF)	Mestre em Relações Internacionais pela *Johns Hopkins School of Advanced International Studies*, nos EUA
27	Walter Aranha Capanema, Prof		Advogado. Coordenador-Geral e Professor do Curso de Extensão em Direito Eletrônico da Escola da Magistratura do Estado do Rio de Janeiro (EMERJ)	Graduação em Direito pela Universidade Santa Úrsula
28	Willian Henrique da Silva Gomes, Cel Eng		Chefe do Centro de Computação da Aeronáutica de Brasília (CCA-BR)	Pós-Graduado em Direito Civil e Processo Civil pela Escola Paulista de Direito (EPD)

Fonte: Os autores.

Além disso, por meio desses dados agregados, podemos ter uma ideia do grau de aprovação da audiência em relação ao conteúdo do evento, mediante uma relação entre o número de cliques nos botões “Gostei” (658) e “Não Gostei” (14), conforme mostra o Gráfico 1.

Gráfico 1 – Taxa de aprovação da audiência do evento



Fonte: os autores.

Como dito, certamente inúmeras variáveis e possibilidades contribuíram para o sucesso – quantitativo e qualitativo – do II Seminário, entre elas podemos destacar a pertinência dos debates proferidos entre audiência, por meio de suas perguntas, e palestrantes, mediantes suas respostas. Nesse sentido, após analisarmos as leituras das perguntas feitas por quem estava assistindo ao vivo o evento, pudemos construir uma nuvem de palavras acerca dos principais temas que foram efetivamente respondidos pelos convidados, conforme nos mostra a Figura 2.

Figura 1 – Palavras extraídas das perguntas da audiência

Fonte: os autores.
Nota: Elaboração a partir de www.wordclouds.com.

Feita essa breve contextualização, partimos agora para o resumo das atividades que ocorreram durante os seis dias do II Seminário de Segurança e Defesa Cibernética da UNIFA, dando ênfase ao conteúdo apresentado pelos palestrantes convidados e sua interação com a audiência.

13/10/2020: O Setor Aeroespacial no Brasil e na Colômbia

Figura 2 – Composição do *webinar* de 13/10/2020
Fonte: https://youtu.be/CRAdoXKAAYU.

O primeiro *webinar* tomou lugar em 13 de outubro de 2020 e teve como Eixo Temático "O Setor Aeroespacial no Brasil e na Colômbia" e contou com palestrantes civis e militares brasileiros, bem como um militar colombiano, dotando, assim, o evento de uma dimensão internacional.

Antes, porém, de os debates iniciarem, o **Prof Me André Meyer Coelho**, da FGV Projetos, teceu um introito acerca da importância de se discutir os impactos da Segurança Cibernética – tanto do ponto de vista técnico quanto das relações internacionais – no setor aeroespacial brasileiro.

Em seguida, o **Brig Int R/1 Pedro Arthur Linhares Lima**, da UNIFA, deu boas-vindas a todas as pessoas presentes, em nome do Reitor da UNIFA, e passou a palavra ao mediador, que, nesta ocasião, foi o **Cel Av Donald Gramkow**, do EMAER, o qual, por seu turno, apresentou cada um dos palestrantes do dia e franqueou-lhes a fala.

O primeiro a discursar foi o **Brig Ar José Vagner Vital**, Vice-Presidente da Comissão de Coordenação e Implantação de Sistemas Espaciais (CCISE) da FAB. Ele iniciou, portanto, falando sobre o Programa Estratégico de Sistemas Espaciais (PESE), cuja concepção advém da Estratégia Nacional de Defesa (END), que, não por menos, elegeu os Setores Nuclear, Cibernético e Espacial como Estratégicos à Nação, ficando o desenvolvimento deste último a cargo da FAB. Do ponto de vista histórico, lembrou que em 1994 – ano de criação da Agência Espacial Brasileira (AEB) – o desenvolvimento das atividades espaciais no Brasil foi vocacionado praticamente para fins civis e que foi em 2008, quando da aprovação da END, que o País voltou a encarar militarmente o espaço exterior, sempre em respeito ao Tratado do Espaço, de 1967, com fins pacíficos e de autodefesa. Vale frisar que, de acordo com o expositor, um aspecto importante sobre o PESE diz respeito ao fato de que seus sistemas necessitam ter uso dual, ou seja, ser aplicados não só em atividades militares, mas igualmente transbordar para a esfera civil. Isso, de fato, evidencia uma busca pela concretização de que tanto fala a END sobre seus Setores Estratégicos: precisam estar alinhados não só às necessidades das Forças Armadas (FA), como também ao Desenvolvimento Nacional. Nesse viés, o Brig Av Vital exemplificou essa busca por meio da ativação do Centro de Operações Espaciais (COPE), sediado em Brasília e com uma estrutura de redundância no Rio de Janeiro, o qual, desde 2017, controla o Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC). Outro exemplo trazido é o redesenho do agora denominado Centro Espacial de Alcântara (CEA), que proverá, cada vez mais, o lançamento de veículos não militares, principalmente daqueles relacionados ao Edital de Chamamento Público lançado pela AEB em 2020.[1] Por fim, o Brigadeiro comentou sobre os desafios atuais do PESE, tendo como foco principal a implantação de um colegiado de ministérios para que haja uma governança política mais adequada que consiga equilibrar os interesses civis e militares brasileiros em relação ao uso estratégico do espaço exterior, no que pontuou também como a segunda corrida espacial está trazendo oportunidade para novos negócios e desenvolvimentos para as indústrias do setor aeroespacial nacional, apresentando o modelo argentino e o CEA como algo a ser levado em conta também pelos pares brasileiros.

Em seguida, **Dr Roberto Gallo**, Presidente da Presidente da Associação Brasileira das Indústrias de Materiais de Defesa e Segurança (ABIMDE), iniciou sua fala tratando das

[1] https://www.gov.br/aeb/pt-br/programa-espacial-brasileiro/chamamento-publico-public-call/chamamento-publico-1.

principais ameaças cibernéticas para o setor espacial nacional. Para ilustrar as preocupações que o País deve ter ao versar sobre a proteção de suas capacidades espaciais duais, o palestrante lembrou casos nas relações internacionais envolvendo o *hacking* de dois satélites que acabaram sendo sabotados em 1998 e 1999, bem como, em anos mais recentes, como a *National Aeronautics and Space Administration* (NASA) dos Estados Unidos da América (EUA) vem sofrendo ataques cibernéticos por parte de atores estrangeiros. Partindo dessa lógica, o expositor apresenta argumentos no sentido de demonstrar que ainda falta, por parte das FAs brasileiras, um olhar mais estratégico para inserir requisitos de Segurança Cibernética nos contratos com fornecedores de sistemas não só espaciais, mas também de outros segmentos críticos da base industrial de defesa (BID). Além disso, de acordo com ele, a chamada guerra cibernética migrou completamente para as operações híbridas – ou cibereletrônicas. Nesse prisma, apregoa que, para evitar sabotagens nos satélites brasileiros e naqueles contratados pelo País, faz-se imperioso o fomento à indústria nacional, pois, somente assim, ter-se-ia total controle e independência sobre seus próprios *software* e *hardware*, mitigando ingerências estrangeiras.

O terceiro palestrante do dia foi o **Ten Cel Rodrigo Mezu Mina**, da *Escuela de Postgrados de la Fuerza Aérea Colombiana* (EPFAC), que iniciou sua fala apresentando como as chamadas ações multidomínios têm sido planejadas no âmbito da Força Aérea Colombiana (FAC). Do ponto de vista do seu Entorno Estratégico amazônico, tanto Colômbia quanto Brasil guardam semelhanças em relação à proteção de suas respectivas porções amazônicas, as quais têm servido de palco para crimes transnacionais, em especial o narcotráfico. Além disso, o Ten Cel Mezu Mina apresenta um panorama de como a força área de seu país têm buscado acadêmica, doutrinária e operacionalmente incorporar a tríade estratégica composta por ar, espaço e ciberespaço, para melhor se adequar à Revolução da Informação a que estão inseridas as FAs de todo o mundo. Tais preocupações passaram a fazer parte da caserna colombiana há pouco tempo, frisa o palestrante, uma vez que só foi em 2007 que o país conseguiu pôr em órbita seu primeiro satélite. Essa preocupação pode ser consubstanciada pelo fato de que a formação dos Cadetes, hoje, encontra grande porcentagem de estudos para a área espacial, bem como, inclusive, já existe um departamento sobre essa área subordinada diretamente à Vice-Presidência da República daquele país. O resultado prático disso tudo é que, segundo o convidado, está havendo uma mudança de mentalidade sobre a importância do poder multidomínio, que passa pela formação do Cadete até o Oficial, inclusive com ofertas

de mestrados e doutorados nessa área. Mas, assim como no Brasil, a questão orçamentária também se configura como um óbice a que a FAC tem se deparado para continuar nessa nova linha de pensar os conflitos do século XXI.

Prof Dr Alvaro Bruno Cyrino, Vice-Diretor da Escola Brasileira de Administração Pública e de Empresas (EBAPE) da Fundação Getúlio Vargas (FGV) foi o palestrante seguinte a falar, no que introduziu a necessidade de que os *clusters* brasileiros do segmento aeroespacial tenham a seu dispor condições e incentivos para fornecer maiores oportunidades de negócios, a exemplo do que ocorreu com a bem-sucedida SpaceX. Levantando o fato de o Brasil já ter historicamente desenvolvido pré-condições para o desenvolvimento de *clusters* aeroespaciais, é preciso pensar como direcionar uma sinergia dual, em que o lado comercial possa gerar mais prosperidade tanto em termos de desenvolvimento tecnológico para a indústria em si quanto de geração de empregos qualificados. O professor, nesse ponto, traz novamente à baila o caso de Alcântara, em que um desenho de *cluster* pode ser efetivamente colocado em prática se se pensar nele não em termos tradicionais que atrelam *cluster* à localidade, mas, sim, inserindo-o em escala global, segmentada, por conseguinte. Assim, o principal desafio brasileiro residiria em compreender como unir importantes atores e tecnologias internacionais do setor aeroespacial para desenvolver um nicho de produtos e serviços que teriam como principais externalidades a produção de conhecimento e o desenvolvimento de tecnologias a serem incorporadas no futuro de forma dual. Do ponto de vista organizacional, ele pondera três pontos como sendo primordiais para esse intento. Primeiro, é preciso pensar na melhoria dos serviços e da infraestrutura disponibilizada de Alcântara, de modo a atrair grandes parceiros e clientes. Segundo, o papel do governo é fulcral nesse processo de adequação do Centro, ao fomentar melhorias estruturais e infraestruturais, bem como promover incentivos ao desenvolvimento tecnológico que aumente o uso racional do CEA. O terceiro e derradeiro ponto toca a questão do capital intelectual, isto é, mapear e fomentar os centros capazes de produzir, isolada ou em conjunto, as tecnologias de ponta de que tanto necessita o País. Para tanto, Prof Cyrino não tira de mente os desafios estratégicos que isso acarreta, a exemplo da proteção à propriedade intelectual, segurança da informação, tempo de maturidade e sistemática orçamentária; porém, lembra casos de sucesso, como o Vale do Silício, a NASA e a própria EMBRAER.

Feitas as apresentações, o mediador passou à leitura e ao redirecionamento das perguntas da audiência, no que foram tocados temas como: dependência orçamentária do

setor aeroespacial brasileiro em relação ao governo; presença militar no espaço exterior; legalidade das operações multidomínios na Colômbia; e a relação entre produção de conhecimento (compartilhamento) e sigilo (segurança) que é tão inerente aos produtos da base industrial aeroespacial.

20/10/2020: O novo Direito Internacional face aos desafios de Segurança Cibernética no espaço cósmico

Figura 3 – Composição do *webinar* de 20/10/2020
Fonte: https://youtu.be/tS4LXM6PCiA.

Diferentemente dos demais dias, o evento de 20/10/2020 foi realizado inteiramente em inglês, sem tradução simultânea e contou com convidados de três nacionalidades, sediados em quatro países diferentes (Brasil, EUA, Itália e Alemanha). O Eixo Temático para este *webinar* foi "O novo Direito Internacional face aos desafios de Segurança Cibernética no espaço cósmico".

As palavras iniciais ficaram a cargo do **Prof Dr Bianor Scelza Cavalcanti**, da EBAPE/FGV, que apresentou um panorama de como as relações internacionais, por séculos, foram moldadas por meio de acordos internacionais acerca de assuntos como fronteiras e conflitos. Hoje, entretanto, as novas oportunidades e ameaças que surgem não apenas dos domínios tradicionais – terra, mar e espaço – potencializam-se com as novas ameaças, oriundas do espaço e do ciberespaço. Lembrou, ainda, que analisar tais questões não requerem apenas um suporte tecnológico, mas também político, social e de engenharia, visando à formação de

um arcabouço normativo que dê conta de tamanho desafio, no que espera que a realização do evento desta data possa contribuir com tais esforços.

Como no primeiro dia de evento, o **Brig Int R/1 Pedro Arthur Linhares Lima**, da UNIFA, deu as boas-vindas aos presentes, em nome do Reitor da UNIFA, apresentando, em seguida, um breve resumo do mediador, **Maj Brig Ar Adyr da Silva**, Presidente da Associação Brasileira de Direito Aeronáutico e Espacial (SBDA), e passando-lhe a palavra, para que este, por sua vez, pudesse apresentar o tema central do dia e introduzir os palestrantes internacionais deste segundo *webinar*.

A primeira convidada a usar da palavra foi a **Me Victoria Samson**, Diretora do Escritório em Washington da Secure World Foundation (SWF), cuja apresentação girou em torno do ciberespaço enquanto uma capacidade *counterspace*. Inicialmente, contextualizou suas ideias a partir da importância de haver uma estabilidade espacial, tendo em vista o número cada vez maior e diversificado de novos atores nessa seara concorrendo com uma crescente importância do espaço para a vida cotidiana da humanidade. Por um lado, essa estabilidade recairia no acesso confiável e previsível ao espaço. Por outro, o ciberespaço aparece como uma opção atrativa para negar tal acesso, uma vez que há, de um lado, menos uso de ataques cinéticos, de outro, guerras eletrônica e cibernética aumentam. Nesse estado de coisas, a desestabilização espacial se torna evidente porque não há uma clareza sobre como aplicar o Direito Internacional dos Conflitos Armados (DICA) ao espaço exterior. Atualmente, o que se tem são iniciativas pontuais ainda em desenvolvimento, como o Manuais MILAMOS e Woomera. Na avaliação da cientista política, muitos países – como EUA, Rússia, China, Coreia do Norte e Irã – já possuem capacidades que poderiam ter como alvo sistemas espaciais, uma vez que (i) já demonstraram interesses em alvos não espaciais e (ii) ataques cibernéticos a sistemas espaciais são similares àqueles não espaciais. Todas essas informações dão subsídios para a palestrante projetar quatro tipos de ataques cibernéticos contra sistemas espaciais e seus principais alvos, a saber: (i) vulnerabilidades na cadeia de suprimento global; (ii) *links* entre satélites e estações de controle terrestres; (iii) estações de Comando e Controle (C^2) ou de transmissão de dados; e (iv) ataques cibernéticos contra o segmento de usuário de um sistema espacial. A pesquisadora do SWF também pontuou que, por um lado, atores estatais têm tomado vantagem dessa intersecção entre espaço exterior e ciberespaço principalmente por causa da flexibilidade e da natureza dos efeitos, da dificuldade de atribuição, por seu potencial em ser mais barato e rápido etc. Por outro lado, as desvantagens nesse meio

também são evidentes, a exemplo do desafio que é avaliar exatamente quais os danos causados. Portanto, realizar essa balança é certamente o grande desafio que as FAs têm ao realizar operações cibernéticas contra sistemas espaciais.

A convidada a palestrar em seguida foi **Me Ana Cristina Galhego Rosa**, fundadora e CEO da Dipteron, na Alemanha. Em sua apresentação, ela destacou que devemos primeiramente situar sobre qual tipo de Segurança Cibernética estamos querendo falar: é no espaço exterior? Ou seria em missões espaciais? Em todo o caso, as técnicas e táticas seriam assaz semelhantes ao que comumente se utilizam em ataques cibernéticos tradicionais, como: espionagem, *jamming* e sequestro de informações. Fazendo eco ao que Dr Gallo já havia alertado no primeiro *webinar*, a palestrante também abordou alguns *cases* da literatura e da casuística das relações internacionais em que fica patente a fragilidade dos sistemas de alguns satélites, possibilitando seu controle e manipulação por terceiros. Nesse sentido, a tecnológica quântica se apresenta, no horizonte de possibilidades, como forte candidata a contornar as questões de Segurança Cibernética que rondam a proteção dos ativos espaciais, aliada a um novo arranjo normativo internacional sobre Segurança Cibernética Espacial. Assim, como não existe vácuo de poder nas relações internacionais, a expositora chama a atenção para o fato de que, no silêncio das normas e convenções, Estados – como França, Reino Unido e Irã – têm aplicado suas próprias interpretações para confrontar ataques cibernéticos contra ativos espaciais, a exemplo da *Space Policy Directive-5* norte-americana, de 2020, sobre os princípios de Segurança Cibernética aplicados aos sistemas espaciais[2].

Em seguida, **Prof Dr Sergio Marchisio**, da *Università La Sapienza di Roma*, iniciou sua fala sobre a relação entre ataques cibernéticos e Direito Espacial já apontado sua opinião de que, caso um ataque cibernético provoque um sério dano a uma infraestrutura crítica nacional, ele pode, sim, ser considerado um ato de guerra. Ao tocar neste ponto, o professor italiano traz à tona a distinção entre crime cibernético e guerra cibernética, em que o primeiro se enquadro em arcabouços legais nacionais, bem como na Convenção de Budapeste[3] de 2001, já a segunda, não encontra respaldo em convenções e tratados internacionais. Todavia, a questão se torna ainda mais complexa, do ponto de vista do Direito Internacional Público, quando se percebe que, embora o Tratado do Espaço não versa especificamente sobre

[2] https://www.whitehouse.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems.

[3] Sobre esse assunto, conferir o trabalho "A LGPD, os cibercrimes e a adesão do Brasil à Convenção de Budapeste", na próxima Parte destes anais.

questões cibernéticas, mas já traz a proibição de haver armas nos artefatos satelitais. Mas, como lembrado pelo professor, nos dias atuais um ataque cibernético a um satélite pode gerar sérios danos na Terra, como interrupção de comunicações e sistemas informacionais, e, pior, um efeito cascata devido aos detritos gerados por uma colisão ou autodestruição de um satélite provocado por uma arma cibernética, por exemplo.

A última convidada a palestrar neste dia foi a **Dra Tatiana Ribeiro Viana**, Consultora Jurídica em Direito Espacial, sediada na Itália. Fazendo um tributo inicial ao pai da aviação, Santos Dumont, sua apresentação buscou apontar como o Direito Internacional lida com os crimes cibernéticos no espaço extra-atmosférico. Contextualizando os crimes e ataques cibernéticos, a expositora trouxe conceitos extraídos da Organização do Tratado do Atlântico Norte (OTAN) para lançar luz, em seguida, ao regime internacional sobre o espaço exterior, em cuja base se encontra o Tratado do Espaço, passando por outras convenções e resoluções de organizações internacionais, como as Nações Unidas. Como se viu durantes todos os dias de evento, um tema recorrente quando se versa sobre ciberespaço e espaço exterior é a questão da responsabilidade estatal aplicada aos ataques cibernéticos, no que Dra Tatiana demonstra como atores não estatais – como *crackers* individuais, organizações criminosas, terroristas e próprios *insiders* – concorrem com atores estatais para complexar ainda mais esse estado de coisas incerto. Em suma, a palestrante afirma que a atribuição de um ataque cibernético a um Estado é um elemento-chave para construir um regime legal funcional que mitigue esses ataques. Trazendo uma contribuição para o Brasil, ela sugere a inclusão de item sobre ativos espaciais ao item 2.3.5 da Estratégia Nacional de Segurança Cibernética (E-Ciber)[4].

Finalizadas as apresentações dos convidados, Maj Brig Ar Adyr da Silva lhes redirecionou algumas perguntas da audiência referentes aos seguintes temas: ataques cibernéticos à luz do Direito Espacial; ações terroristas contra nações no espaço; e responsabilidade estatal por ataque cibernético à luz do Direito Internacional.

[4] Sobre a E-Ciber, conferir o trabalho "Estratégia Nacional de Segurança Cibernética (E-Ciber): comparativo com estratégias de outros países", na Parte II destes Anais, *infra*.

27/10/2020: A recente legislação brasileira que trata de aspectos relativos à Segurança Cibernética

Figura 4 – Composição do *webinar* de 27/10/2020
Fonte: https://youtu.be/xSQiByUZ8D8.

O terceiro *webinar* ocorreu no dia 27 de outubro de 2020 e teve como Eixo Temático "A recente legislação brasileira que trata de aspectos relativos à Segurança Cibernética". Inovando mais uma vez, o formato deste evento foi diferente dos demais, contando apenas com um palestrante e um mediador, os quais, como se pode observar, mantiveram-se em constante interação.

Da mesma maneira com que ocorreu no primeiro *webinar*, o **Prof Me André Meyer Coelho**, da FGV Projetos, teceu um introito acerca da importância dos marcos regulatórios para a formação de uma base industrial e dar garantias a investidores de que o Programa Espacial Brasileiro (PEB) é de padrão internacional, no que o arcabouço jurídico nacional contempla a Lei Geral de Proteção de Dados (LGDP) e a proteção jurídica no tema da Segurança Cibernética.

Na sequência, o **Brig Int R/1 Pedro Arthur Linhares Lima**, da UNIFA, saudou os presentes, em nome do Reitor da UNIFA e apresentou o mediador, **Prof Walter Aranha Capanema**, advogado e docente da Escola da Magistratura do Estado do Rio de Janeiro (EMERJ), que, por seu turno, introduziu o palestrante do dia, **Desembargador Nagib Slaibi Filho**, Presidente do Comitê de Governança de Tecnologia da Informação e Comunicação (CGTIC) do Tribunal de Justiça do Rio de Janeiro (TJRJ).

De forma introdutória, Prof Capanema contextualizou a entrada em vigor da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), no sentido de que ela vem para se somar a outros dispositivos legais de proteção à liberdade do cidadão. Feito isso, passou a palavra ao Des Nagib, que, antes de transcorrer sobre as repercussões da LGPD, realizou um panorama histórico e jusfilosófico sobre as ideias de "Política", "Nacionalidade" e "Liberdade" – sendo esta última, a antítese da segurança, ou seja, aquilo que restringe –, termos que compõem o cerne da Política Nacional de Segurança da Informação (PNSI), lembrando, ainda, que Segurança da Informação visa a assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação. É nesse diapasão que o palestrante informou que foi criada na EMERJ o Fórum Permanente da Justiça na Era Digital justamente para demonstrar com o Estado brasileiro está buscando adaptar-se aos novos tempos de globalização da informação, no que a LGPD e a PNSI, por exemplo, vêm na esteira de outras ações, como a Lei do Processo Eletrônico, de 2006.

Como observado pelo mediador, cada vez mais, recursos tecnológicos são utilizados para engendrar e trafegar informações, fazendo surgir a necessidade de se proteger eficazmente a quantidade volumosa de dados que é produzida a cada instante. Daí surge a pertinência de se discutir a PNSI e a LGPD com instituições de outros Poderes além do Judiciário, como é o caso das FA, buscando salvaguardar as estruturas e infraestruturas que servem de suporte para a materialização da Segurança Cibernética do País.

Ao analisar a PNSI, o Desembargador Nagib argumenta que essa norma peca pelo fato de não ser, *de facto*, nacional, ou seja, não se aplicar aos três níveis de governo – municipal, estadual e federal –, pois, no seu entendimento, a Segurança da Informação é um direito-dever de todos. Por sua vez, o Prof Capanema lembra do caso do *ransomware*, que acometeu no ano passado aeroportos da França, e que esse exemplo ilustra como as infraestruturas críticas aeroespaciais também estão a mercê de ameaças cibernéticas não apenas oriundas

de Estados-nação, mas igualmente de atores não-estatais, como já havia pontuado, por exemplo, a **Dra Tatiana** no *webinar* anterior.

Após as considerações finais do palestrante, o mediador iniciou o repasse de algumas perguntas que estavam chegando da audiência e que versaram sobre os seguintes objetos: aplicação da LGPD em relação às questões de defesa nacional; conceito jurídico de segurança nacional; autodeterminação informativa; plano de implantação da LGPD nos tribunais brasileiros; potenciais mudanças na LGPD, que acaba de entrar em vigor; e crimes cibernéticos contra a soberania nacional.

03/11/2020: Os desafios de TI no tratamento e resposta aos incidentes da Segurança da Informação

Figura 5 – Composição do *webinar* de 03/11/2020
Fonte: https://youtu.be/GQ5se_YxRgU.

O quarto *webinar* foi realizado em 03 de novembro de 2020, costumeiramente das 10h às 12h, tendo como Eixo Temático "Os desafios de TI no tratamento e resposta aos incidentes da Segurança da Informação". Para este evento, foram convidados dois especialistas brasileiros para discorrer sobre os desafios e ameças que impactam centros de tratamentos de respostas tanto na seara civil quanto militar.

Antes, porém, o **Prof Dr Bianor Scelza Cavalcanti**, da FGV, proferiu palavras de introdução aos trabalhos, pontuando que a importância da temática abordada neste dia reside, especialmente, na certeza de que ocorrências de incidentes críticos, senão catastróficos, em sistemas tecnológicos de alto risco só poderão ser mitigadas e dotadas de resiliência por meio de seus oportunos e eficientes reportes e tratamentos. Esta resiliência, apregoa, está relacionada tanto a compromissos institucionais e pessoais, de modo que a

chave para seu desenvolvido repousa, em última instância, na produção do conhecimento científico centrada no elemento humano. Assim, finaliza suas palavras na certeza de que os debates realizados ao longo do evento possam contribuir par ao esforço brasileiro e internacional nessa área de enorme relevância estratégica.

Feito isso, a palavra foi passada ao moderador, **Brig Int R/1 Pedro Arthur Linhares Lima**, que, em nome do Reitor da UNIFA, abriu oficialmente os trabalhos e os debates deste dia. Em seguida, apresentou os dois palestrantes, direcionando algumas perguntas.

A primeira convidada a falar foi a **Dra Cristine Hoepers**, Gerente Geral do Centro de Estudos, Tratamento e Resposta a Incidentes de Segurança no Brasil (CERT.br), a qual iniciou apresentando sua percepção sobre o cenário atual em que as organizações devem estar preparadas para fazer a gestão de incidentes em seus ambientes informáticos. Indo ao encontro do que o professor Bianor havia pontuado na introdução, partiu do pressuposto de que não existem sistemas informáticos 100% seguros.

Apontou que, tendo em vista que instituições militares, como a FAB, utilizam ambientes de operações e infraestruturas críticas, é necessário perceber que a ainda predomina a mentalidade de *safety* – que foca na tolerância a falhas –, em que os projetos não preveem mecanismos de atualização e gerência remota. Além disso, os sistemas legados geralmente utilizam *software* de uso geral – a exemplo dos sistemas operacionais (SO) "de prateleira". Assim, a gestão dos riscos cibernéticos tem de estar constantemente focada mais nos processos e nas pessoas do que nas ferramentas. Para tanto, elencou casos que mostram o quão difícil é impedir a invasão de sistemas, a exemplo dos comprometimentos gerados por furtos de informações, inclusive criptografada, a órgãos públicos nos EUA e na Holanda.

A título de investigação e sugestão, apresentou alguns *frameworks* que auxiliam na organização de pessoas, processos e tecnologias. Certamente o mais conhecido de todos é o NIST Cyber Security Framework, que possui cinco fases, a saber: identificar, proteger, detectar, responder e recuperar, sendo que é nas três últimas fases que reside o gerenciamento do incidente. Além dessa ferramenta do *National Institute of Standards and Technology* (NIST), apresentou também como o FIRST CSIRT Services framework se volta para o estabelecimento e a melhoria contínua da gestão de incidentes, no sentido de melhorar, cada vez mais, os processos e capacitar as pessoas neles envolvidas.

Ao versar sobre a dinâmica de trabalho dos grupos de resposta a incidentes de segurança em computadores (CSIRTs), a palestrante enfatizou a importância da relação entre

eficiência, efetividade e maturidade, na medida em que, quando se versa sobre tratamento de incidentes, pessoas e relações de confiança fazem toda a diferença. Portanto, a questão da maturidade, nessa área, evoluiu para modelos de acreditação e certificação, a exemplo da ferramenta *on-line* SIM3 e do TF-CSIRT Trusted Introducer, cujos parâmetros foram detalhados pela cientista da computação.

Por fim, Dra Cristine analisou a proposta do Plano Nacional de Tratamento e Resposta a Incidentes Computacionais (PNTIR), apontando como o fato de ele estar sendo apreciado na capital federal já inclui a questão do tratamento de incidente na agenda política e na mentalidade organizacional de que, realmente, incidentes vão ocorrer e que, portanto, o País precisa estar mais bem preparado.

Por sua vez, o **Cel Eng Willian Henrique da Silva Gomes**, Chefe do Centro de Tratamento e Resposta a Incidentes de Rede da FAB (CTIR.FAB), iniciou sua participação corroborando a exposição da Dra Cristine e exemplificando como a Engenharia Social tem sido um grande desafio para as organizações que lidam com informações sensíveis, daí a necessidade de atualizar e treinar pessoal. Aproveitou o ensejo para apresentar a estrutura do CTIR.FAB, órgão do COMAER responsável pelo tratamento, controle, monitoramento, análise forense e resposta a incidentes de segurança. Assim como a maioria dos centros de tratamentos de incidentes informáticos, o análogo da FAB tem como atribuição principal receber e notificar qualquer evento adverso (confirmado ou sob suspeita) relacionado à segurança dos sistemas de computação ou das redes de computadores. Mas aqui, ele pontua, houve uma inovação trazida pelo COMAER em julho de 2020, no sentido de que as Equipes de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) não atuam exclusivamente de forma reativa, mas incorporaram a função de Prevenção. Pontuou, ainda que, dentro dessa perspectiva, o CRTIR.FAB trata de categorias diversas de incidentes, a exemplo de: acesso não autorizado, exposição de informação sensível, hospedagem de *malware*, tentativa de autenticação por força bruta e vazamento de dados.

Passo seguinte, Cel Willian apontou para o futuro, ao versar sobre os próximos desafios do órgão por ele chefiado, dentre os quais está a capacidade de a FAB lidar com novas ameaças inerentes às aos novos ativos tecnológicos críticos que são incorporados ao patrimônio tangível e intangível da instituição. Na sua visão, os principais desafios aeroespaciais brasileiros são de curto, médio e longo prazos. No curto prazo, sua atenção se volta à proteção do SGDC e do seu centro de operações. No médio prazo, está a nova projeção

geopolítica do CEA, uma vez que grandes *players* das relações internacionais começarão a utilizar sistematicamente o Centro, abrindo espaço para a potenciais inimigos querem sabotar ou atrapalhar suas missões. E, para ilustrar suas percepções sobre os desafios de longo prazo, o palestrante ilustrou sua preocupação projetando o System-Wide Information Management (SWIM), rede – ainda em desenvolvimento – de contato para os *stakeholders* do tráfego aéreo mundial, que pode também utilizada para a troca de informações e dados inerentes a essa atividade. Em seu exemplo, redes internacionais como o SWIM precisam estar protegidas contra ameaças como a hospedagem de *malware*. Portanto, de acordo com o candidato, o tratamento a incidentes deve permear prospecções de curto a longo prazos, e isso vem sendo perseguido pelo Departamento de Controle do Espaço Aéreo (DECEA).

Já encaminhando para o encerramento da sua fala, o palestrante pontuou algumas oportunidades de estudo e capacitação nessa área, a exemplo de: Inteligência Artificial (AI) e Machine Learning que buscam automatizar com alto grau de precisão análises de padrão de redes e suas anomalias; criptografia, essencial para a proteção e o tráfego de informações sensíveis; certificação no Brasil de produtos cibernéticos, especialmente para evitar *backdors* e outras intempéries de se adquirir produtos – ou partes deles – que possam trazer embutida algum imprevisto, a exemplo da recente proibição de adição de determinados componentes chineses no caça F-22 Raptor americano; e desenvolvimento de sistemas operacionais seguros, a exemplo do que a China vem fazendo, para superar o uso de *software* produzido nos EUA.

Concluídas as apresentações, o mediador da UNIFA redirecionou perguntas da audiência para os convidados, cujas temáticas giraram em torno dos seguintes temas: consolidação nacional dos dados estatísticos sobre Segurança Cibernética; PNTIR; proteção e mitigação de ataques cibernético a satélites; atuação de grupos internacionais voltados ao combate de *malware*; e cursos e treinamentos ofertados pelo CERT.br.

11/11/2020: Desafios da Defesa Cibernética na projeção espacial brasileira

Figura 6 – Composição do seminário de 11/11/2020
Fonte: https://youtu.be/GQ5se_YxRgU.

Como já relatado, após a realização de quatro *webinars* de duas horas de duração a cada uma semana, os dois dias de seminários tiveram três horas de duração cada um e ocorreram em dois dias seguidos.

O primeiro dia, 11 de novembro de 2020, apresentou como tema central "Perspectivas da FAB para a cibernética no Poder Aeroespacial" e contou com o maior número de convidados em único dia: oito.

Proferindo palavras introdutórias, o Diretor da FGV **Prof Dr Carlos Ivan Simonsen Leal** lembrou que o processo de digitalização em escala mundial não vai diminuir, fazendo com que a dependência humana na rede mundial de computadores – ou em parte dela – seja cada vez mais acentuada. Isso faz surgir inúmeros problemas de segurança. Nesse prisma, o professor

pontuou que é necessário um esforço de buscar entender quais são as tendências ora em curso, pautadas principalmente pelo crescimento exponencial da IA, das tentativas de rompimento da Lei de Moore até sua substituição pela lei quântica. O convidado finalizou suas palavras lembrando que tais desafios dizem – e muito – respeito também às FA e à segurança nacional, no que deseja a todos um excelente dia de debates.

Dando prosseguimento aos trabalhos, o **Brig Ar Luís Renato de Freitas Pinto**, Reitor da UNIFA, destacou a importância do II Seminário e a realização dos quatro *webinars* anteriores como exemplificativos do papel científico em que se insere a missão institucional da UNIFA, com suas pesquisas e estudos avançados voltados para o desenvolvimento do Poder Aeroespacial brasileiro. Encerrando sua fala, o Comandante da UNIFA desejou a todos os presentes um bom evento, passado, de pronto, a palavra ao mediador do dia, **Brig Int R/1 Pedro Arthur Linhares Lima**, da UNIFA, que, por seu turno, deu as boas-vindas a todos e apresentou as credenciais do primeiro convidado, passando-lhe a palavra.

Ten Brig Ar Marcelo Kanitz Damasceno, Chefe do EMAER, iniciou a Palestra de Abertura, cujo título coincide com o tema deste dia de seminário, apregoando a importância estratégica do domínio do espaço exterior como fator ora impulsionador, ora multiplicador de algumas capacidades duais. Para ilustrar essa ideia, elencou várias aplicações e usos de ativos espaciais, como o *Global Positioning System* (GPS), as imagens por satélite de áreas de risco ou derramamentos de óleo na costa brasileira e a própria viabilidade, em escala global, da Internet. Nesse viés, lembra que o espaço exterior é livre, pois permite que as nações possam eficaz e eficientemente gerenciar seu próprio território e também reduzir tensões e conflitos acerca da delimitação de fronteiras. Alertou que, por causa dessas enormes potencialidades, os ativos espaciais – a exemplo dos satélites e, mais especificamente, de sua carga útil – podem se tornar alvo de ameaças e ataques cibernéticos. Nesse ponto, o Ten Brig Ar Damasceno lembrou que, embora as PND e END tenham legado ao Exército Brasileiro a responsabilidade pelo desenvolvimento do Setor Estratégico Cibernético, a atenção da FAB deve se voltar não apenas para o ativo em órbita, mas também para todas as fases que o levam até lá, isto é, desde sua concepção ao lançamento, nas quais há vulnerabilidades que podem ser exploradas pelo atacante cibernético e causar perdas incalculáveis para o País. Salientou também que a atual corrida espacial tem incluído atores privados em torno de um mercado trilionário, causa uma outra corrida, paralela, em que alguns tentam impedir o sucesso de outros, inclusive no meio cibernético. Ao realizar um breve histórico da atividade

espacial brasileira, situou o PESE, que transpassa o Ministério da Defesa, em busca de tornar o país cada vez menos dependente de tecnologia estrangeira, no que as quatro frotas hoje em desenvolvimento (comunicação estratégica, comunicações táticas, imageadores ópticos e imageadores radar) vêm ao encontro desse mandamento. Finalizou sua exposição destacando como esses desafios da Defesa Cibernética para a projeção – e proteção – espacial brasileira apontam para características que são inerentes dos sistemas que se traduzem em vulnerabilidades que devem ser protegidas.

Dando continuidade a este penúltimo dia de eventos, o moderador apresentou os quatro palestrantes do painel, tendo como primeiro expositor o **Gen Bda Antônio Carlos de Oliveira Freitas**, Assessor Especial de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR). Em sua fala inicial, explicou quais são as competências do Gabinete no trato com a questão da Segurança Cibernética, sendo, portanto, o órgão central que planeja, coordena e supervisiona a atividade de segurança da informação no âmbito de toda a Administração Pública Federal. Ao apresentar o organograma do GSI, enfatizou que os órgãos-chave encarregados pelas áreas que dão nome a este Seminário são a Assessoria Especial de Segurança da Informação, o Departamento de Acompanhamento de Assuntos Espaciais (DAAE) e o Departamento de Segurança da Informação (DSI), os quais são responsáveis, dentre outros, por credenciar pessoas, habilitar órgãos, proteger sistemas e redes do Governo Federal. O palestrante mostrou, ainda, a evolução normativa do GSI no que concerne à temática da Segurança Cibernética, uma vez que o rol de parceiros institucionais passou a abranger órgãos dos três Poderes da Federação, nos mais diversos níveis. Com isso, tem-se que a PNSI é o principal marco que o GSI leva em conta para atuar ciberneticamente, seguida da E-Ciber. Vale frisar que ambas foram matéria de debate no terceiro *webinar*.

Em seguida, quem se utilizou da palavra foi o **Gen Bda Jomar Barros de Andrade**, atual Chefe do Centro de Defesa Cibernética do Exército (CDCiber), para, incialmente, explicar sobre a atribuição de coordenação das atividades de Defesa Cibernética que são atribuídas ao Comando de Defesa Cibernética (ComDCiber). Para tanto, contextualizou a estruturação do Setor Estratégico Cibernética, fazendo eco, assim, ao que o Ten Brig Ar Damasceno e ao Brig Ar Vital já haviam pontuado sobre a divisão tripartite dos Setores Estratégicos no Brasil. Seguindo o traçado, o palestrante relatou a experiência imprescindível para robustecer a Defesa Cibernética brasileira, que foi a atuação durante a realização dos grandes eventos – como os Jogos Mundiais da Juventude de 2013, a Copa do Mundo de 2014 e os Jogos

Olímpicos de 2016. Lembrou ainda da relevância do Exercício Guardião Cibernético, um exercício de simulação e grupos de estudos formados por entidades públicas e privadas, civis e militares, e que tem por alvo maior a proteção de infraestruturas críticas. Dialogando com o que a Dra Cristine Hoepers já havia destacado no quarto *webinar*, o General pontuou sobre a importância estratégica do PNTIR e o fortalecimento de interlocução com o nível político-estratégico. Especificamente sobre a relação entre o ComDCiber e o Poder Aeroespacial, o convidado lembrou que aquela organização militar (OM) profere apoio em termos de resiliência cibernética no CINDACTA IV e em Alcântara, bem como nas operações da Força, além de já ter capacitado, desde 2015, mais de 300 pessoas da FAB, por meio da Escola Nacional de Defesa Cibernética (EnaDCiber), no que destaca que o fator *sine qua non* para o sucesso nessa seara é justamente a colaboração. Em seguida, apresentou o argumento de que o ComDCiber se apoia nas melhores práticas internacionais para poder desempenhar seu mister de maneira ainda mais eficaz. Para tanto, informou que houve vários intercâmbios, treinamentos e visitas a nações amigas, no intuito de não apenas fortalecer as relações, como igualmente trocar experiências entre congêneres dessa área, a exemplo do já tradicional Fórum Ibero-Americano de Defesa Cibernética e de estágios que o ComDCiber oferece a países amigos. Nesse ponto, o convidado destacou que, com isso, fortalece-se não só a Defesa brasileira, mas também sua inserção nas relações internacionais.

O quarto convidado a palestrar foi o **Brig Ar Marco Aurélio Martins Gabriel**, Chefe do Estado Maior Conjunto do Comando de Defesa Cibernética (ComDCiber). Sua fala inicial girou em torno de realizar um panorama sobre como o COMAER estruturou sua Defesa Cibernética. Para tanto, valeu-se de robusto arcabouço normativo em que esse tema é visto tanto na Visão nos Desafios da FAB quanto nas Possibilidades de atuação do Poder Aeroespacial. Lembrou, ademais, que a dimensão estratégica da cibernética permeia o atual Plano Estratégico Militar da Aeronáutica (PEMAER), no que diz respeito à diretrizes para os macroprocessos de gestão e suporte – especificamente nas áreas de CT&I, C^2, TI e telecomunicações. Esses foram, portanto, alguns exemplos que ilustram como a questão da Defesa Cibernética vem sendo tradada no âmbito do COMAER, que, em suma, é concebida tanto para a defesa, ataque e exploração contra ameaças cibernéticas quanto para a resiliência de sistemas e redes informacionais enquanto imprescindíveis meios para a manutenção do Poder Aeroespacial. Ainda, saudou a Diretriz de Comando do Comandante da Aeronáutica, de fevereiro de 2019, em que a capacitação de profissionais nas áreas de Defesa Cibernética e Espacial farão parte

das ações de capacitação e habilitação dos recursos humanos para o exercício de cargos e funções de interesse do Poder Aéreo e Espacial brasileiro. O convidado pontuou ainda que o ComDCiber vem desenvolvendo ações conjuntas e outras formas de fortalecer a Defesa Cibernética no âmbito da FAB, que ocorre tanto por meio de simulados, encontros, capacitações e parceria (a exemplo da recém-assinada com o ITA) quanto de rubricas específicas no orçamento voltado a essa área.

Por seu turno, o **Brig Int Luiz Fernando Moraes da Silva**, Diretor da Diretoria de Tecnologia da Informação da Aeronáutica (DTI), contextualizou os desafios do Setor Estratégico no Poder Aeroespacial, por meio de três eixos principais: infraestrutura, operações e recursos humanos. No que diz respeito à infraestrutura – sistemas operacionais e tecnologia – necessária para uma proteção cibernética efetiva, requer-se: segregação e redundância de redes operacionais e administrativas; monitoramento do espectro eletromagnético; computação de alto desempenho que viabilize, entre outros, criptografia, IA e sistemas e simuladores de Defesa Cibernética; e a ativação de uma ETIR. Quanto às operações, elas estão diretamente relacionadas à segurança operacional e à integração entre as FA, no que se torna imprescindível, por exemplo, criar gestões de risco e à vida no CEA e fortalecer a atuação do Núcleo do Centro de Defesa Cibernética da Aeronáutica (CDCAER), com vistas a integrá-lo às demais Forças. Ademais, pontuou que um olhar estratégico sobre esse assunto passa necessariamente pelos recursos humanos, ou seja, pela formação de equipes, bem como de sua capacitação continuada, algo que, diga-se de passagem, também foi lembrado pelo **Ten Brig Ar Damasceno**, durante o final da Palestra de Abertura deste dia. O palestrante, por fim, pontuou o estado de coisas em que se encontra a estruturação do CDCAER, elencando suscintamente suas responsabilidades estratégicas e operacionais, as quais abarcam, no âmbito do COMAER, em grande medida, as discussões levadas a cabo durante este seminário.

Feitas as apresentações de praxe, o mediador procedeu à leitura e ao redirecionamento de perguntas feitas pela audiência, que versaram sobre os seguintes tópicos: tecnologia 5G; apoio do ComDCiber a outras organizações em caso de crises cibernéticas; eficácia do Sistema Militar de defesa Cibernética (SMDC); relação entre o DTI e o futuro CDCAER; capacitação em matéria de Segurança Cibernética; computação quântica e IA; cursos para civis no ComDCiber; e proteção integrada às infraestruturas críticas.

12/11/2020: Perspectivas da FAB para a cibernética no Poder Aeroespacial

Figura 7 – Composição do seminário de 12/11/2020
Fonte: https://youtu.be/z-YkdUS9Xkw.

Este derradeiro dia de evento foi realizado em 12 de novembro de 2020 e teve como tema central “Perspectivas da FAB para a cibernética no Poder Aeroespacial”, contando com a participação de cinco convidados, sendo um deles diretamente da Áustria.

Iniciando os trabalhos, o **Brig Int R/1 Pedro Arthur Linhares Lima**, da UNIFA, deu as boas-vindas a todos os presentes, em nome do Reitor da UNIFA, apresentando o currículo do mediador e passando-lhe a palavra. Nesta ocasião, a tarefa de coordenar os trabalhos ficou a cargo do **Brig Ar José Vagner Vital**, Vice-Presidente da CCISE/FAB, o qual, por sua vez, realizou um panorama das dimensões cibernética e espacial no preparo e emprego de uma força aérea, bem como apresentou brevemente os currículos dos quatro debatedores do dia.

O primeiro a usar a palavra foi o **Maj Brig Ar João Campos Ferreira Filho**, Chefe da Terceira Subchefia do Estado-Maior da Aeronáutica (EMAER), que relatou a evolução das

Teorias do Poder Aéreo, desde o século XX, no que a FAB, criada em 1941, já fora à guerra em 1944, absorvendo táticas e técnicas aprendidas durante a participação brasileira na Segunda Guerra Mundial. Destacou também que um ponto crítico na história da FAB aconteceu a partir da década de 1950, quando o País começou a investir no desenvolvimento tecnológico e doutrinário do setor aéreo, com a criação do ITA, do parque tecnológico e do programa espacial – inicialmente focada na tão almejada busca pela Missão Espacial Completa Brasileira (MECB). Finalmente, em 2012, a FAB passou a incluir, em sua Doutrina Básica, o termo Poder Aeroespacial e, mais recentemente, a atual Doutrina Aeroespacial já incorporou o domínio cibernético. Portanto, como lembra o palestrante, não há como falar em domínio espacial sem se referir ao cibernético e vice-versa[5]. O convidado também elencou e apresentou os principais setores críticos do Poder Aeroespacial brasileiro, quais sejam: a defesa aérea, o controle do espaço aéreo e as operações espaciais, enfatizando que os dois primeiros surgiram juntos, dentro da FAB, nos anos 1970 e que, portanto, seus sistemas integrados precisam estar eletônica e ciberneticamente bem protegidos. Esse desafio inclui também a produção nacional de *hardware* e *software*, fomentando, assim, a indústria nacional de que tanto versou Dr Gallo no primeiro *webinar*.

O próximo a palestrar foi o **Brig Ar Paulo Eduardo Vasconcellos**, Diretor de Inteligência Estratégica e Novos Negócios da Agência Espacial Brasileira (AEB), que relatou a profunda reestruturação sofrida pela Agência, de modo a se moldar, em grande medida, às novas perspectivas trazidas pelo *New Space*. Nesse viés, a segurança cibernética se mostra bastante relevante para a atividade espacial, porém a E-Ciber não cita o espaço – falha essa que a **Dra Tatiana**, no segundo *webinar* também havia comentado. Trazendo as discussões mais para o campo militar, o convidado pontuou que importantes atores das relações internacionais já fazem uso de armas antissatélites (ASAT), especialmente no segmento terrestre e em contexto de implementação do 5G e de satélites de órbita mais baixa, em que é possível ter uma comunicação direta. Tudo isso faz com que a segurança cibernética seja uma componente no cálculo das ações de defesa nacional a ser levada em conta. Ele finalizou sua fala apresentando como é salutar para o País que toda a sociedade adentre nas discussões sobre Defesa, uma vez que ela não é apenas uma responsabilidade das FA. Portanto, na sua opinião, esses temas deveriam entrar em uma próxima revisão da E-Ciber, no que informa que

[5] E este é, certamente, o mote que permeia praticamente todas as poucas doutrinas militares espaciais, no mundo, de que temos conhecimento.

a dimensão securitária do ciberespaço também precisa ser reforçada no âmbito da AEB, fazendo com que os debates deste II Seminário se tornem deveras oportunos para o fomento de tal discussão na Agência.

Até este ponto, as discussões se pautaram mais sob a ótica do arcabouço normativo nacional. Para falar sobre essas discussões nas relações internacionais, foi franqueada a palavra ao **Diplomata André João Rypl**, representante do Ministério das Relações Exteriores (MRE) do Brasil em Viena e membro do *United Nations Committee on the Peaceful Uses of Outer Space* (COPUOS). Inicialmente, relatou que o Brasil é visto nos fóruns multilaterais como um construtor de laços e entendimentos entre as nações, de modo que a propositura a presidência brasileira nesse foro da Organização das Nações Unidas (ONU) pode refletir essa ideia de que o espaço exterior é um bem público global que necessita da atuação integrada dos países em prol de sua segurança. Analisando criticamente o papel do COPUOS, o diplomata brasileiro acentuou que, paradoxalmente, não existe um debate estruturado sobre ataques cibernéticos estruturados no espaço exterior nesse foro onusiano nem mesmo sobre desarmamento, em Genebra. Portanto, o panorama traçado pelo palestrante é o de que ainda não houve uma problematização da Segurança Cibernética sobre o espaço nas relações internacionais, uma vez que o que existe são, sim, visões e perspectivas isoladas que se unem a depender dos interesses, especialmente, dos grandes atores internacionais nessa seara. Como uma espécie de corolário do art. 4º da Constituição da República Federativa do Brasil de 1988 (CF88), que dispõem sobre os princípios que regem o País em suas relações internacionais, o representante brasileiro em Viena mostrou que, dentro desse amálgama de visões sobre o uso militar do espaço, a brasileira vai na direção por seu uso pacífico, que se mostra assaz diferente da das grandes potências militares.

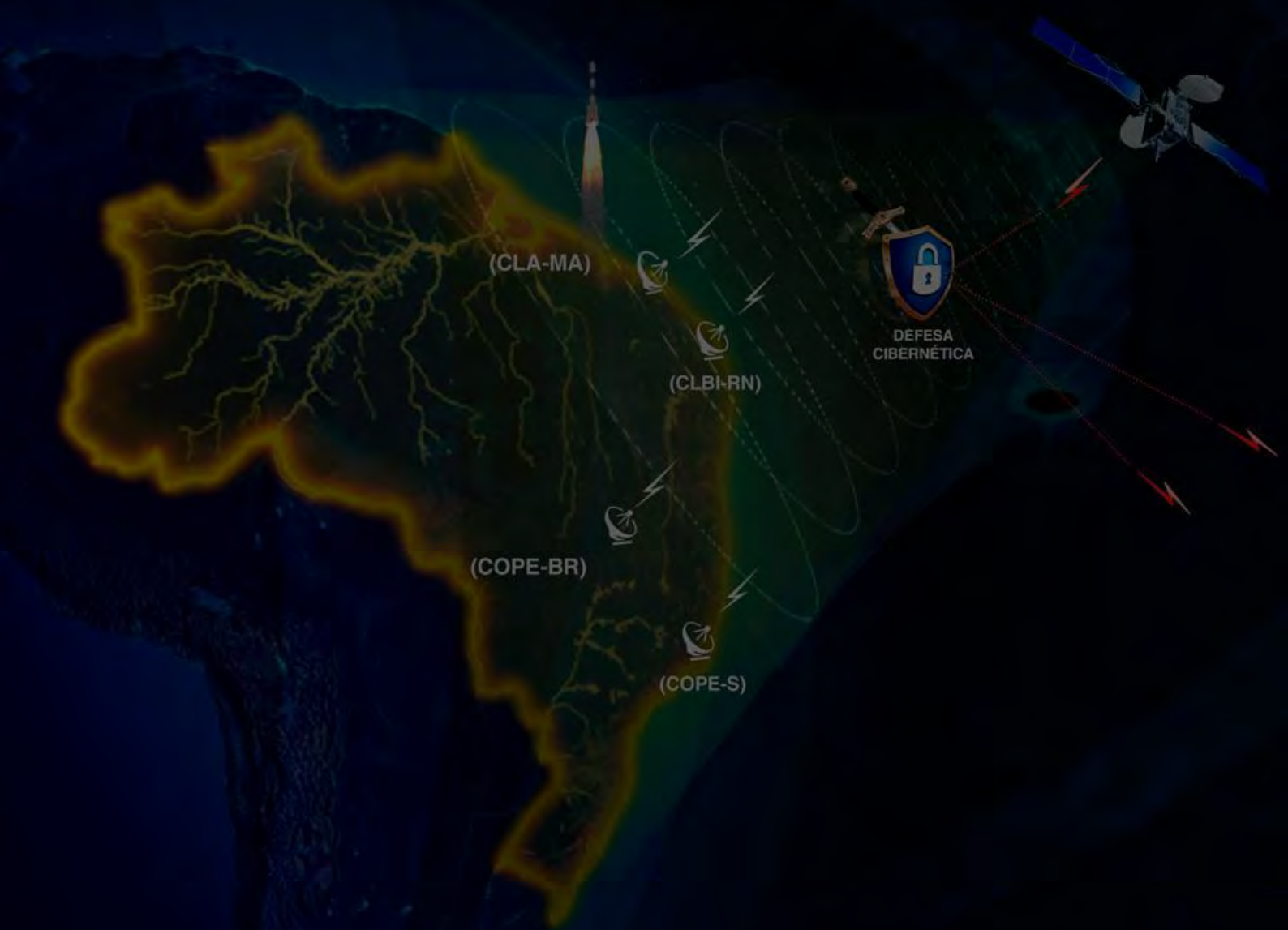
Nesse ponto, o mediador lembrou que, na falta desse diálogo político de que falou o diplomata convidado, já existe um interessante precedente que é o Direito do Mar, a partir do qual se pode pensar em soluções para problemas compartilhados também no espaço. Por falar em problemas e ameaças, **Brig Ar Vital** indagou ao próximo palestrante justamente sobre este ponto: como o COPE vem lidando com essas questões para a proteção cibernética dos satélites brasileiros.

Na sua vez de falar, o **Ten Cel Av Luis Felipe de Moura Nohra**, Chefe da Seção de Análise de Operações Espaciais do COPE, lembra alguns fundamentos da parte espacial de satélites que são: as panes ocorrem no prior horário, trabalhe-se arduamente sem garantias

de sucesso, tudo o que for projetado de *hardware* e *software* ou vai virar pó – quando da reentrada na atmosfera – ou lixo espacial. Portanto, por questões logísticas, a correção de eventuais falhas nesses ativos espaciais se dá há milhares de quilômetros da Terra, via espectro eletromagnético e cibernética. Para ilustrar a importância estratégica dessa dimensão, o palestrante ilustrou a discussão por meio do *case* do SGDC, cuja concepção já previra 14 camadas de segurança para torná-lo resiliente por, no mínimo, três lustros, no que a prospecção entrou também como um elemento tão importante quanto a tecnologia em si. Nesse prisma, apregoou como doutrinas militares, a exemplo da *United States Space Force* (USSF), vêm se amoldando a essa nova realidade de dependência entre espaço e ciberespaço, e que a versão brasileira de uma doutrina militar do emprego espacial, em desenvolvimento, vem ao encontro dessa necessidade de apresentar às sociedades brasileira e internacional a visão brasileira sobre assunto tão complexo e vital.

Terminados os ciclos de debates, o mediador passou à leitura e ao redirecionamento das perguntas feita por meio do aplicativo Slido, no que foram tocados temas como: proteção cibernética do SGDC; plano de atividades cibernéticas espaciais; ataques cibernéticos como ato de guerra; custos das missões brasileiras na exploração espacial; criação de uma força espacial brasileira.

PARTE 2



TRABALHOS CIENTÍFICOS

Relação dos trabalhos aprovados e apresentados

Quadro 3 – Relação dos trabalhos aprovados e apresentados

Tema	Título do artigo	Autor(es)	Currículo	Apresentação
Os desafios de tecnologia da informação no tratamento e resposta aos incidentes da Segurança da Informação	Análise dos benefícios de *pentests* regulares nas redes do Comando da Aeronáutica	Lucas França de Jesus		
		Carlos Alberto Ferreira Bispo		
	Metodologia de classificação e priorização de ativos de tecnologia da informação para a segurança cibernética	Silvio Roberto Assunção de Oliveira Filho		
	O conceito de dissuasão cibernética: relevância e possibilidades	Cícero Araújo Lisboa		
		Guilherme Ziebell		
	Principais Ameaças Cibernéticas aos Sistemas Espaciais	André Lucas Alcântara da Silva		
Perspectivas da FAB para a cibernética no Poder Aeroespacial	Defesa da propriedade intelectual contra *cyberattacks* nas infraestruturas do setor aeroespacial brasileiro	Viviane Souza da Costa		
A recente legislação brasileira que trata de aspectos relativos à Segurança Cibernética	A LGPD, riscos cibernéticos e o “seguro cibernético"	Patricy Barros Justino		
		Érica Maia Campelo Arruda		
	Estratégia Nacional de Segurança Cibernética (E-ciber): comparativo com estratégias de outros países	Patricy Barros Justino		
		Luciana Quagliane Ribeiro		
	Os desafios do *compliance* para adequação à LGPD	Aline Marchesini Pinto		
		Érica Maia Campelo Arruda		
	A LGPD, os cibercrimes e a adesão do Brasil à Convenção de Budapeste	Érica Maia Campelo Arruda		
		Patricy Barros Justino		

Fonte: Os autores.

Análise dos benefícios de *pentests* regulares nas redes do Comando da Aeronáutica

Lucas França de Jesus

Carlos Alberto Ferreira Bispo

Resumo: O crescimento acelerado do ciberespaço na sociedade atualmente faz com que os sistemas e as redes de computadores se tornem cada vez mais complexos, aumentando naturalmente a superfície de ataque de uma organização. Diante disso, é fácil ocorrer de que pontos periféricos da rede, isto é, de menor relevância para a atividade fim de uma grande instituição, sejam deixados em segundo plano na gestão da segurança cibernética interna, criando um perigo cada vez mais latente, possibilitando, assim, a entrada de um invasor à rede organizacional. Assim, este trabalho objetiva formular uma política de segurança que fortaleça o acompanhamento e proteção desses ativos por meio da utilização de testes de intrusão realizados regularmente em cada rede local por seus próprios administradores, invertendo o fluxo de informação atual, em que a identificação de vulnerabilidades parte do órgão central para os secundários, com base no princípio de que pequenos esforços conjuntos geram grande impacto no sistema como um todo. Quanto à metodologia, tem-se um estudo exploratório-descritivo, combinado do tipo quanti-qualitativa, utilizando-se para coleta de dados um teste de intrusão de pequena escala realizado em servidor especial da Academia da Força Aérea, cópia não funcional daquele que hospeda o *website* interno da organização, tornando possível avaliar a contribuição que esse tipo de ferramenta proporciona para o aumento da segurança cibernética da rede. Dessa forma, foi possível atingir o objetivo e recomendar uma nova forma de gerenciamento da segurança computacional no Comando da Aeronáutica, mais proativa e menos dependente de um único órgão, pela qual se descentraliza parte das tarefas, focando a responsabilidade do Centro de Computação da Aeronáutica de Brasília em monitorar o estado de proteção dos ativos da instituição e tomar decisões estratégicas acerca da área na organização como um todo, sendo essa otimização da gestão de segurança cibernética a principal contribuição do presente trabalho.
Palavras-chave: Otimização. Política de segurança cibernética. Teste de intrusão.

1 Introdução

A crescente dependência do mundo atual com relação aos dispositivos eletrônicos ocorre em um ritmo cada vez mais acelerado e abrangente, aumentando gradativamente a importância que a segurança cibernética deve assumir no contexto de uma sociedade imersa em tecnologias da informação. Alguns exemplos disso foram a utilização do *worm*[6] Stuxnet para atrasar a operação nuclear iraniana (KASPERSKY, 2014), o ataque de negação de serviço

[6] De acordo com a Cartilha de Segurança para a Internet (BRASIL, 2012a, p. 25), "worm é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador".

distribuído (DDoS)[7] capaz de afetar mais de 80 grandes sites através da *botnet*[8] Mirai (KOCHETKOVA, 2016) e a utilização de *ransomwares*[9] para extorquir dinheiro de hospitais que não percebem outra opção ao se deparar com pacientes em estados críticos de saúde perante a inoperabilidade de sistemas inteiramente encriptados por criminosos, além da vulnerabilidade dos dados pessoais de seus clientes nessas situações (BREWSTER, 2016). É interessante perceber que, em apenas três exemplos, já se pode notar a diversidade de meios e de objetivos possíveis de serem explorados por indivíduos mal intencionados.

A maior parte dos países já vem trabalhando para elaborar doutrinas de defesa e segurança cibernética, instituindo comandos militares, agências civis, departamentos de inteligência e legislações que facilitem a prevenção, minimização e punição de crimes cibernéticos (BRASIL, 2010). O Brasil, por sua vez, desenvolvia-se lentamente na área até 2013, quando o ex-funcionário da *National Security Agency* (NSA), Edward Snowden, publicou documentos que comprovaram ações de espionagem do governo americano sobre a presidente e outras autoridades brasileiras (BRASIL, 2014a). Desde então, o processo de elaboração e de fortalecimento da Defesa e da Segurança Cibernética ganhou velocidade e atenção no país (ARTIGO 19, 2017), dividindo-se a responsabilidade do assunto entre o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), responsável pela segurança das informações relacionadas à Administração Pública Federal, e o Comando de Defesa Cibernética (ComDCiber), responsável pelas ações defensivas, ofensivas e exploratórias que sejam de interesse da Defesa Nacional (ARTIGO 19, 2016).

Embora a criação e especialização desses órgãos seja de fundamental importância para assegurar os ativos cibernéticos brasileiros, suas atuações se dão em níveis mais altos e distantes das organizações em geral, isto é, atuam no nível estratégico de um macrossistema (BRASIL, 2014b). Uma forma de melhorar o panorama do país é aperfeiçoar o papel dos setores responsáveis pela administração de redes locais, ou seja, que atuam em microssistemas. Muitos são os aspectos possíveis de serem abordados, melhorados e implementados nesse contexto, como por exemplo os testes de intrusão.

---

[7] "são caracterizados pelo envio de pacotes e requisições a um determinado alvo, visando degradar a qualidade ou tornar completamente indisponíveis os serviços oferecidos pela vítima" (OLIVEIRA *et al.*, 2007).

[8] "Botnets são redes de computadores que foram infectadas e estão sob o controle de um hacker" (SACCHETIN, 2008 *apud* MUZZI, 2010, p. 25).

[9] "ransomware é um código malicioso que tem a finalidade de sequestrar os dados do usuário e, posteriormente, solicitar um valor de resgate por esses dados" (ZAGHETTO *et al.*, 2017, p. 1).

Diante desse contexto, muitas empresas atualmente realizam testes de intrusão em suas redes e sistemas, seja por consultoria externa seja por realização própria (CCM TECNOLOGIA, 2018). No âmbito militar, essa prática também tem grande potencial de fortalecer a segurança da rede tanto global quanto localmente e já é utilizada dentro da Força Aérea pelo Centro de Computação da Aeronáutica de Brasília (CCA-BR), único órgão autorizado a realizar tais procedimentos em escopo operacional. Como forma de melhorar o uso dessa ferramenta, é necessário que se adote uma doutrina de valorização do *pentest* entre os responsáveis pela segurança da informação nas organizações como um todo e também que se autorize a realização desse procedimento por administradores das redes locais para que possam desenvolver tal processo entre determinados intervalos de tempo.

Mas qual é exatamente o impacto que isso é capaz de trazer para a segurança da infraestrutura de Tecnologia da Informação da FAB? Tomando como base um teste de intrusão de pequeno porte realizado pelos autores em uma aplicação *web* interna da Academia da Força Aérea (AFA), este trabalho analisa os benefícios dessa ferramenta aplicados em microescala dentro das redes da instituição. Com isso em mente, este trabalho objetivou formular uma política de segurança que fortaleça o acompanhamento e a proteção desses ativos por meio da utilização de testes de intrusão realizados regularmente em cada rede local por seus próprios administradores, invertendo o fluxo de informação atual, em que a identificação de vulnerabilidades parte do órgão central para os órgãos secundários, com base no princípio de que pequenos esforços conjuntos geram grande impacto no sistema como um todo.

2 Revisão bibliográfica

2.1 A Cibernética na Defesa

Buscando cumprir as concepções apresentadas na Política Nacional de Defesa (BRASIL, 2016a), em que se afirma a importância de se dedicar especial atenção à defesa e à segurança do ambiente cibernético, a Estratégia Nacional de Defesa (BRASIL, 2016b) atribui a responsabilidade pelo desenvolvimento de tal setor ao Exército Brasileiro. Apesar disso, ao tratar do setor aeroespacial, esse mesmo documento reconhece a relevância desse campo para a Força Aérea Brasileira (FAB) e a responsabiliza por manter seus sistemas protegidos.

> Considerando que a Força Aérea se configura como uma organização altamente tecnológica, imprescindível se faz utilizar-se das capacidades de proteção dos Sistemas de Comando e Controle e das Estruturas Estratégicas do País,

> principalmente daquelas que envolvam o espaço cibernético. Deve, portanto, manter em elevado grau o nível de segurança e de defesa dos seus sistemas computacionais. (BRASIL, 2016b).

Conforme conceituado na Doutrina Militar de Defesa Cibernética (DMDC) (BRASIL, 2014b), o espaço cibernético é o "espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas".

Uma visão ainda mais interessante, para as Forças Armadas (FA) e outros órgãos de defesa, sobre o espaço cibernético pode ser encontrada no documento doutrinário norte-americano *Operações no ciberespaço,* no qual se define que

> *Cyberspace is a man-made domain, and is therefore unlike the natural domains of air, land, maritime, and space. It requires continued attention from humans to persist and encompass the features of specificity, global scope, and emphasis on the electromagnetic spectrum. Cyberspace nodes physically reside in all domains. Activities in cyberspace can enable freedom of action for activities in the other domains, and activities in the other domains can create effects in and through cyberspace.* (UNITED STATES, 2010).

2.2 O *pentest* no âmbito militar

O profissional de *pentesting* busca explorar vulnerabilidades e relatar ao seu contratante os danos que poderiam ser causados por um invasor real, relatando com detalhes todas as brechas encontradas e sugerindo ou não maneiras de realizar suas correções. Entretanto, tendo em vista a sensibilidade dos dados e da própria infraestrutura de informação da Defesa, é preferível que os realizadores de testes de intrusão no âmbito das Forças Armadas sejam militares da ativa.

Para que isso seja possível, o apoio da Escola Nacional de Defesa Cibernética (ENaDCiber) e do Comando de Defesa Cibernética (ComDCiber) é imprescindível, pois torna possível capacitar militares de todas as Forças para atuarem na área de segurança cibernética[10]. Utilizando-se dessa capacidade de qualificação de recursos humanos, a capacitação de militares das seções responsáveis por administração de redes locais nas diversas organizações possibilitaria a realização de testes de intrusão com certa regularidade, proporcionando a descoberta de vulnerabilidades e suas consecutivas correções também regularmente, dificultando que ataques bem sucedidos sejam lançados sobre os sistemas militares.

[10] BRASIL. Comando do Exército. Escola Nacional de Defesa Cibernética. Pedido de Cooperação de Instrução: Atividades Cibernéticas. *Ciclo de palestras apresentadas aos cadetes da AFA*. Brasília, 2019.

Destaca-se que uma área bastante importante da realização de testes de intrusão - e da segurança da informação em geral - diz respeito à ética e à legalidade das ações. Novamente, como definido no Manual de Campanha do Exército Brasileiro sobre o assunto (BRASIL, 2017), uma das características da Guerra Cibernética é a dualidade, pois

> na guerra cibernética, as mesmas ferramentas podem ser usadas por atacantes e administradores de sistemas com finalidades distintas: uma ferramenta que busque as vulnerabilidades do sistema, por exemplo, pode ser usada por atacantes para encontrar pontos que representem oportunidades de ataque em seus sistemas-alvo e, por administradores, para descobrir as vulnerabilidades de equipamentos e de redes. (BRASIL, 2017).

Os testes de intrusão estão intimamente ligados às legislações que, dentre outras características, tipificam criminalmente o acesso não autorizado a dispositivos alheios e o uso indevido de dados de terceiros. As principais leis sobre o assunto no Brasil são: Marco Civil da Internet – Lei n° 12.965/2014 (BRASIL, 2014c), Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei n° 13.709/2018 (BRASIL, 2018b) e Lei n° 12.737/2012 (BRASIL, 2012c).

Além disso, existem normas internas da FAB, em especial a NSCA 7-13 – Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica (BRASIL, 2013), que apresentam a visão da instituição sobre o tema e normatiza a atuação dos usuários, administradores de rede e órgãos de TI que atuam no âmbito da FAB.

Buscando respeitar toda essa legislação em vigor no Brasil sobre o tema, o teste de intrusão que serviu de base a este trabalho foi realizado mediante autorização formal da autoridade competente.

3 Materiais e métodos

Conforme a legislação já citada anteriormente no tópico 2.2, "O *pentest* no âmbito militar", cujo conteúdo prevê que testes de intrusão só podem ser realizados mediante autorização legal prévia, submeteu-se inicialmente um projeto de Iniciação Científica a um Corpo de Pareceristas da própria AFA para análise e aprovação, a qual foi obtida por meio da publicação da Portaria AFA nº 20/DE_SPPC, de 18 de outubro de 2019, assinada pelo Comandante da Academia da Força Aérea. Na sequência, foi solicitada, por meio de ofício ao Chefe da ASTIC-GAP-YS, a autorização para realizar os testes de intrusão delineados e delimitados nos projetos da Iniciação Científica e do Trabalho de Conclusão de Curso, cuja autorização veio por meio do Ofício nº 3/ASTIC/9805, de 1º de novembro de 2019, assinado pelo Chefe do GAP-YS. Os resultados obtidos, análises e conclusões dessas publicações,

associados ao debate, novas análises e conclusões efetuadas durante e após a banca julgadora do Trabalho de Conclusão de Curso (TCC), culminaram no presente artigo científico.

A realização dos testes cibernéticos ocorreu de duas formas distintas: um atacante com pouco conhecimento e um atacante com conhecimento intermediário sobre segurança cibernética, mas com uma metodologia bem definida. A fim de evitar que este artigo funcione como um guia para violação da rede da GUARNAER-YS por eventuais pessoas mal intencionadas, foram suprimidos todos os detalhes que possibilitar-lhes-iam um ataque cibernético, constando exclusivamente no relatório técnico entregue à ASTIC-GAP-YS. As etapas realizadas foram: preparação, coleta de informações, modelagem de ameaças, análise de vulnerabilidades, exploração de falhas, elaboração do relatório técnico, do relatório da Iniciação Científica, do TCC e o presente artigo.

Na fase de preparação foram acertados os termos e as condições do teste, tais como escopo, formalização do pedido de autorização para realização do teste em tela, contendo o compromisso de sigilo dos participantes e outros aspectos julgados necessários pelo orientador e pelo chefe da ASTIC-GAP-YS. Dessa forma, ficou definido que os testes poderiam ocorrer de qualquer local com acesso a rede cabeada administrativa da AFA, a partir de computador pessoal ou do laboratório de informática. Entretanto, a atuação do autor estava restrita apenas ao servidor disponibilizado para os testes.

Na fase de coleta de informações, o autor reuniu dados e informações acerca dos sistemas e da instituição interessantes para o teste. As técnicas utilizadas foram desde a coleta manual de *open source intelligence* (OSINT) dentro da aplicação, por meio da análise de códigos fonte e navegação pelo site, até a utilização de ferramentas que automatizam essas buscas de forma agressiva.

Na fase de modelagem de ameaças, as informações obtidas na etapa anterior foram analisadas a fim traçar o plano de ação dos autores, isto é, raciocinar e listar possíveis meios de obter acesso ao sistema e classificá-los quanto à ordem de realização de experimentos, desenvolvendo estratégias de invasão. Assim, apesar de haver informações expostas indevidamente na aplicação e da maioria de seus softwares estarem desatualizados em algumas versões, não se identificou boas oportunidades de invasão por meio de *exploits* – técnicas ou códigos utilizados para a violação de um serviço – públicos voltados aos componentes do servidor. Apesar disso, foram encontradas duas formas de se aproveitar da

aplicação para ganhar acesso à máquina hospedeira através do banco de dados e para furtar ou alterar informações de usuários autenticados.

Com os resultados anteriores, o objetivo da fase de análise de vulnerabilidades foi identificar especificamente os meios de conseguir acesso ao sistema, baseado nas estratégias elaboradas na última etapa, de forma manual e por meio de *scanners* de vulnerabilidades. Dessa forma, foi percebido que o melhor caminho para conquistar o acesso ao sistema era por meio do seu banco de dados, após encontrar uma página do site na qual se conseguia executar códigos diretamente na consulta ao banco de dados, isto é, sem passá-lo por algum tipo de filtro ou parametrização. Além disso, foi percebida a possibilidade de explorar outro tipo de falha, no qual se conseguiria lançar ataques ao usuário, autenticado no site, através da criação e do envio de uma URL (endereço eletrônico) maliciosa.

Na fase de exploração de falhas, a meta era obter acesso ao sistema alvo por meio da aplicação das estratégias desenvolvidas anteriormente e das vulnerabilidades já identificadas, utilizando desde técnicas manuais e *scripts* simples até ferramentas automáticas mais agressivas, caso necessário. Após identificados os pontos de acesso descritos no parágrafo anterior, foi realizada a exploração de ambas as vulnerabilidades: na primeira e mais crítica, buscou-se primeiramente conseguir acesso por modo manual e, após algum tempo com resultados pouco efetivos, utilizou-se a aplicação *SQLmap* para atacar o alvo e conseguir acesso; já no segundo caso, obteve-se sucesso por meio de exploração manual, baseado em tentativa e erro, para criar uma prova de conceito (*Proof of Concept - PoC)*.

A fase de elaboração de relatórios consistiu em confeccionar documento detalhado sobre os testes, no qual se descreveu a sequência e o raciocínio de todos os passos realizados, em ambas as metodologias adotadas, além de contar com um sumário executivo visando a facilitar o entendimento do conteúdo por autoridades que não pertencem à área trabalhada, abordando as descobertas com exemplos de ataques e seus impactos sobre a instituição. Já a seção técnica do relatório possuiu a finalidade de expor ao setor de TI da organização todo o processo de realização do teste, em todas as suas fases, de forma a contribuir com a consciência situacional dos administradores de rede e facilitar a correção das falhas encontradas.

Finalizando, cada um em seu devido período, elaborou-se o relatório da Iniciação Científica, na sequência, o TCC e, posteriormente, este artigo científico, sumarizando tudo o que foi obtido, analisado e concluído.

4 Resultados e discussões

4.1 Vulnerabilidades

Conforme descrito anteriormente, foram encontradas três vulnerabilidades durante os testes, considerando-se um número significativo para o nível superficial no qual se trabalhou.

A primeira, considerada de mais baixo risco pelos próprios mecanismos de busca de vulnerabilidades, é a exposição de informações identificada pela possibilidade de acesso a dados, páginas e arquivos que não são necessários a um usuário não autenticado, essas informações constam apenas no Relatório Técnico entregue à ASTIC-GAP-YS. Essas informações, nas mãos de um indivíduo mal intencionado e que possua os conhecimentos necessários, são suficientes, ou no mínimo contribuem bastante, para a elaboração de estratégias de ataque e descobrimento de caminhos que o levem ao acesso não autorizado da máquina alvo. Para essa vulnerabilidade, foram sugeridas ações como adoção de mascaramento e obscurecimento da identidade do servidor, restrição de acesso aos arquivos e diretórios que não possuem utilidade ao usuário comum e revisão do código-fonte das páginas a fim de evitar atributos que apontem as ferramentas utilizadas na construção da aplicação.

A segunda vulnerabilidade encontrada, considerada de médio risco, foi a execução de script através do site (*cross-site scripting* ou XSS). Por meio desse ataque, é possível furtar dados de outros usuários, alterar suas senhas ou até mesmo excluir suas contas e informações da aplicação, considerando-se um usuário com nível de acesso normal, além de permitir alterações diretamente no servidor ou na conta do administrador, caso a vítima possua privilégios mais elevados. Esse tipo de vulnerabilidade é normalmente aliado à engenharia social e se deve, principalmente, à sanitização inadequada ou inexistente do *input* de usuários, sendo esta a principal sugestão para sua correção. Para evitar isso, além da sugestão descrita anteriormente a respeito da sanitização de dados, faz-se necessário também uma grande campanha de conscientização do efetivo sobre a segurança cibernética, com foco em evitar ataques de *phishing*.

A terceira e última vulnerabilidade foi também considerada de médio risco com base no ponto até onde se avançou nos testes, porém é importante ressaltar seu potencial de se tornar uma brecha de alto risco para a rede caso ela possibilite a escalação de privilégios para

um usuário administrador da rede. Essa falha existe por ser permitida, em determinadas páginas, a inserção de códigos SQL (*Structured Query Language*) que são executados no *back-end* da aplicação, sem necessidade de autenticação ou privilégios especiais. Essa falha se deve à inadequada sanitização de dados recebidos pela aplicação, o que geralmente ocorre pelo fato de o programador não considerar a possibilidade de o usuário utilizar os serviços do site de forma diferente daquela para a qual foi projetada. As sugestões para correção dessa vulnerabilidade consistem, portanto, em implantar mecanismos que filtrem o input gerado pelo usuário e, se possível, parametrizar os argumentos utilizados na consulta ao banco de dados (isto é, não permitir que os dados inseridos pelo usuário sejam diretamente executados no código SQL, mas sim passá-los à consulta através de uma variável).

4.2 Discussão dos resultados

Com base nesses resultados, é possível perceber que algumas vulnerabilidades foram encontradas com relativa facilidade perante um teste cuja metodologia está disponível publicamente e cuja aplicação não depende de conhecimentos técnicos avançados.

Isso é preocupante na medida em que se vê a crescente disponibilização de conteúdos e cursos, tanto gratuitos quanto pagos, sobre segurança cibernética na internet, tornando possível que qualquer pessoa com interesse suficiente seja capaz de aprender ataques simples e poderosos, conheça ferramentas automatizadas de grande risco para grandes instituições e até mesmo tenha acesso a códigos maliciosos, prontos para o uso, que se encontram disponíveis ou publicamente ou em fóruns reservados. Assim, a segurança de qualquer ativo de informação não pode ser negligenciada.

No início deste século, quando se utilizou o espaço cibernético pela primeira para lançar um vetor de ataque militar, o *Stuxnet* foi apenas o projeto-piloto para demonstrar o grande potencial do ciberespaço para a guerra. A partir do desenvolvimento dessa arma cibernética, vislumbrou-se em todo o mundo a possibilidade de uso do espaço cibernético para um novo tipo de guerra, a cibernética, como um novo teatro de operações militares (BISPO, 2017). Com o passar dos anos, incontáveis casos de ações cibernéticas conflituosas foram sendo vistas pelo mundo e, com isso, sua importância primordial no cenário global contemporâneo foi se tornando inegável. Engana-se, porém, aquele cujo pensamento reside na ultrapassada ideia de que os ataques de grande porte e complexidade são os únicos que merecem atenção e prevenção.

Pelo contrário, as superfícies de ataque se tornam cada vez mais amplas para um mesmo alvo e, por isso, sua proteção se torna cada vez mais complexa. Atualmente, o mais indicado não é mais buscar uma blindagem contra ataques e explorações, mas sim uma resiliência tal que permita uma rápida recuperação após sofrer intervenções externas. Isso, porém, só se aplica após se atingir um nível de proteção alto o suficiente para evitar a maior parte dos ataques. O mais importante é perceber que, quanto a segurança digital, não se deve haver economia de esforços e sim uma interconexão e trabalho conjunto entre eles.

É imprescindível que a mentalidade de todos os integrantes da instituição se volte ao mesmo objetivo: eliminar ou, pelo menos, diminuir as brechas de segurança ao menor nível possível. Não significa que esse deve ser o único objetivo, pois a Força Aérea deve estar preparada e aprimorando constantemente também suas capacidades de ataque e de exploração. Porém, percebendo-se a interconectividade dos sistemas e dos ativos de informação, torna-se nítida a necessidade de resguardar sua porção do ciberespaço desde o componente mais complexo até o mais simples, pois uma falha presente em algum serviço de execução em segundo plano em um sistema de menor importância operacional para a instituição pode ser justamente a porta de entrada de um atacante na rede, a partir da qual ele consegue a capacidade de se espalhar e realizar ataques mais significativos.

Considerando ser necessário o fortalecimento da Força Aérea Brasileira em todas as três ações da Guerra Cibernética, o modo mais eficiente de se agir para melhorar a defesa de perímetro da rede consiste em dividir o esforço da proteção cibernética entre os altos escalões e as redes locais administradas por seções menores em cada OM. Quando se trata de ações de defesa e de exploração defensiva, é necessário adotar a descentralização dos esforços de acordo com cada objetivo. Isso significa que, para realizar uma defesa contra um ataque de grandes proporções ou um gerenciamento de crises eficiente, é mais efetivo atribuir tais responsabilidades aos órgãos centrais responsáveis pelo setor cibernético da Força, enquanto que para explorações defensivas – tais como testes de intrusão e avaliação de vulnerabilidades –, bem como defesas de ataques pontuais ou de menor escala, podem e devem ser atribuídos aos setores locais de cada rede.

A decisão de deixar as explorações defensivas também a cargo dos administradores de redes locais traz como principal benefício uma quantidade maior de redes regularmente avaliadas e manutenidas quanto a sua segurança e por isso, todos os nós da rede passariam por esse processo, pois ao invés do órgão máximo responsável pela segurança dos ativos

cibernéticos, no caso o CCA-BR, necessitar de despender tempo e atenção com a realização de avaliações de vulnerabilidades em cada ponto de acesso à rede da Aeronáutica, em adição a todas as suas outras atribuições, seu trabalho seria facilitado por focar em avaliar os relatórios de avaliações já feitas pelos administradores locais.

Por meio da divisão de esforços entre os administradores de redes menos complexas, é possível elevar a quantidade de testes executados e substituir a sistemática de testes sob demanda pela realização planejada em uma política de segurança de nível institucional, na qual é possível diluir o trabalho de análise e distribuir a quantidade de organizações a realizarem as avaliações de suas redes ao longo do ano, buscando viabilizar operacionalmente essa operação. Apesar dos gastos acrescentados em função da capacitação de mais militares na área de cibernética, deve-se perceber a contrapartida da diminuição da necessidade de visitas de assessoria técnica em segurança, uma vez que a maioria das avaliações seriam feitas localmente pelo próprio efetivo da localidade e o imenso ganho de especialização em um campo fundamentalmente estratégico para a Força no cenário contemporâneo.

Certamente é um processo trabalhoso, mas com um sistema de informação adequado às necessidades desse cenário, seria possível até mesmo filtrar os resultados para facilitar a consulta e gerar estatísticas sobre os problemas que os próprios administradores encontraram em suas redes, identificando pontos a serem revisados na política de segurança ou a receberem maior atenção nas próximas avaliações. É importante ressaltar que, nessa linha de raciocínio, o órgão central não se sobrecarrega com a responsabilidade de resolver os problemas, limitando-se usualmente ao assessoramento das seções de cada OM responsáveis pelas redes testadas, fornecendo ajuda direta na solução de falhas somente quando o administrador da própria rede não for capaz de solucioná-las.

Esse sistema obviamente demanda uma ampla preparação de recursos humanos, visto que cada rede deve possuir um assessor técnico com conhecimentos de segurança. Isso, porém, não é um problema impeditivo, pois a ENaDCiber tem justamente a missão de capacitar pessoal das Forças Armadas e da Administração Pública Federal para o exercício de funções na área cibernética, com plenas condições de realizar essa preparação dos militares da FAB ao longo dos anos. Além disso, seguindo uma ideia bem parecida com o previsto no Programa de Defesa Cibernética do Exército – em parte por haver um comando militar conjunto, que facilita a comunicação entre as Forças –, o Comando da Aeronáutica

recentemente deu início ao processo de mapeamento de talentos no setor cibernético, como é possível observar no Ofício nº 57/1SC1/34410, de 30 de julho de 2020.

Por fim, é necessário também que se autorize as seções responsáveis por cada rede local a realizar os testes, isto é, fornecer às ASTICs o respaldo legal para que atuem dentro do proposto neste artigo. Apesar de decisões complexas e de mudanças necessárias no sistema atual, é possível perceber o ganho potencial para a instituição através dessa proposta.

5 Conclusões

A partir da realização do teste de invasão no âmbito da Academia da Força Aérea, foi demonstrado o grande potencial de atividades desse tipo contribuírem positivamente para a segurança cibernética institucional e, com isso, pôde-se analisar os benefícios que sua aplicação traz para a FAB.

Para isso, foi elaborado um novo modo de realizar e gerir a segurança dos diversos ativos de informação espalhados pela Força, partindo-se do princípio de que é mais eficiente e mais fácil circular as informações do nível mais baixo para o nível mais alto.

Baseando-se, portanto, no sentido que o fluxo de informações e de atribuições deve seguir entre os níveis de trabalho da instituição para que haja uma maior eficiência, analisou-se qualitativamente os ganhos que a descentralização de ações de defesa ativa, especialmente testes de intrusão, pode trazer para a FAB tanto no sentido de melhorar consideravelmente a segurança do ciberespaço institucional quanto no sentido de permitir a órgãos, como o CCA-BR, uma maior liberdade para atuação em outros projetos por meio da redução e concentração de carga de trabalho relativa à segurança geral da rede interna da Aeronáutica.

Com os resultados dessa análise, concluiu-se que é possível otimizar o sistema de avaliação de segurança da instituição e garantir uma menor vulnerabilidade a ataques que venham a ser lançados, principalmente, em pontos periféricos da rede.

Referências

ARTIGO 19. Da cibersegurança à ciberguerra: o desenvolvimento de políticas de vigilância no Brasil. *Artigo 19*, 2016. Disponível em: https://artigo19.org/wp-content/blogs.dir/24/files/2016/03/Da-Cibersegurança-à-Ciberguerra-WEB.pdf. Acesso em: 18 set. 2019.

ARTIGO 19. Desenvolvimento de políticas de cibersegurança e ciberdefesa na América do Sul: estudo de caso sobre a atuação governamental brasileira. *Artigo 19*, 2017. Disponível em: https://artigo19.org/wp-content/blogs.dir/24/files/2017/12/Desenvolvimento-de-políticas-de-cibersegurança-e-ciberdefesa-na-América-do-Sul-Estudo-de-caso-sobre-a-atuação-governamental-brasileira".pdf. Acesso em: 18 set. 2019.

BISPO, C. A. F. Avaliação dos malwares criados por Estados-Nação. SEMINÁRIO DE SEGURANÇA E DEFESA CIBERNÉTICA, I. Rio de Janeiro, Universidade da Força Aérea, Anais, 2017.

BRASIL. CERT.br. *Cartilha de Segurança para Internet*. Versão 4.0. São Paulo, 2012a.

BRASIL. Comando da Aeronáutica. *NSCA 7-13*: Segurança da Informação e Defesa Cibernética nas organizações do Comando da Aeronáutica. Brasília, DF: COMAER, 2013.

BRASIL. Comando do Exército. *EB70-MC-10.232 – Manual de Campanha do Exército Brasileiro*: Guerra Cibernética. Brasília, DF, EB: 2017. Disponível em: http://bdex.eb.mil.br/jspui/bitstream/1/631/3/EB70MC10232.pdf. Acesso em: 05 out. 2019

BRASIL. Comando do Exército. *Pedido de cooperação de instrução*: atividades cibernéticas. Brasília, DF: Escola Nacional de Defesa Cibernética, 2019.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. *Livro Verde*: Segurança Cibernética no Brasil. Brasília, DF: GSI, 2010.

BRASIL. *Lei n° 12.737, de 30 de novembro de 2012.* Brasília, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 14 out. 2019. 2012c.

BRASIL. *Lei n° 12.965, de 23 de abril de 2014.* Brasília, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 14 out. 2019. 2014c.

BRASIL. *Lei n° 13.709, de 14 de agosto de 2018.* Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 14 out. 2019. 2018b.

BRASIL. Ministério da Defesa. *Doutrina Militar de Defesa Cibernética*. Brasília, DF: Ministério da Defesa, 2014. Disponível em: https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf. Acesso em: 05 out. 2019. 2014b.

BRASIL. Ministério da Defesa. *Estratégia Nacional de Defesa*. Brasília, DF, 2016b, *minuta.* Disponível em: https://www.defesa.gov.br/arquivos/2017/mes03/pnd_end.pdf. Acesso em: 12 out. 2019.

BRASIL. Ministério da Defesa. Política Nacional de Defesa. Brasília, DF, 2016a, *minuta.* Disponível em: https://www.defesa.gov.br/arquivos/2017/mes03/pnd_end.pdf. Acesso em: 12 out. 2019.

BRASIL. Senado Federal. Denúncias de Snowden revelam amplo monitoramento. *Em Discussão*, Brasília, n. 21, jul. 2014. Disponível em: https://www12.senado.leg.br/emdiscussao/edicoes/espionagem-cibernetica/@@images/arquivo_pdf/. Acesso em: 18 set. 2019. 2014a.

BREWSTER, T. As Ransomware Crisis Explodes, Hollywood Hospital Coughs Up $17,000 In Bitcoin. *Forbes*, 18 fev. 2016. Disponível em: https://www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/#2dd6d544408f. Acesso em: 18 set. 2019.

CCM TECNOLOGIA. Testes de intrusão: entenda como funciona. *Blog de Cibersegurança*, 2018. Disponível em: https://blogdeciberseguranca.com.br/post/testes-de-intrusao-entenda-como-funciona. Acesso em: 18 out. 2019.

KASPERSKY DAILY. Stuxnet: Victims Zero. Kaspersky, 2014. Disponível em: https://www.kaspersky.com/blog/stuxnet-victims-zero/6775/. Acesso em: 18 set. 2019.

KOCHETKOVA, K. How to not break the Internet. Kaspersky. 2016. Disponível em: https://www.kaspersky.com/blog/attack-on-dyn-explained/13325/. Acesso em: 18 set. 2019.

MUZZI, F. A. G. *Análise de botnet utilizando plataforma de simulação com máquinas virtuais visando detecção e contenção.* Tese (Doutorado em Engenharia Elétrica) - Escola Politécnica da Universidade de São Paulo. São Paulo, 2010. Disponível em: https://www.teses.usp.br/teses/disponiveis/3/3142/tde-01032011-130343/publico/Tese_Fernando_Augusto_Garcia_Muzzi.pdf. Acesso em: 16 out. 2019.

OLIVEIRA, Luiz *et al.* Avaliação de proteção contra ataques de negação de serviço distribuídos (DDoS) utilizando Lista de IPs Confiáveis. SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, 7. Rio de Janeiro, 2007. Disponível em: https://www.researchgate.net/publication/257697651_Avaliacao_de_Protecao_contra_Ataques_de_Negacao_de_Servico_Distribuidos_DDoS_utilizando_Lista_de_IPs_Confiaveis. Acesso em: 17 out. 2019.

UNITED STATES. AIR FORCE. *AFDD 3-12*: cyberspace operations. 2010. Disponível em: https://fas.org/irp/doddir/usaf/afdd3-12.pdf. Acesso em: 13 out. 2019.

ZAGHETTO, Cauê *et al.* Ransomware: este problema também pode ser seu. *Revista Tecnologias em projeção*, v. 8, n. 2, 2017. Disponível em: http://revista.faculdadeprojecao.edu.br/index.php/Projecao4/article/view/791/829. Acesso em: 16 out. 2019.

Metodologia de classificação e priorização de ativos de tecnologia da informação para a Segurança Cibernética

Silvio Roberto Assunção de Oliveira Filho

Resumo: Este trabalho propõe uma metodologia de Classificação e Priorização de Ativos Críticos, com base na proposta de valor, para a Gestão Estratégica de Segurança Cibernética. Com a crescente informatização dos processos e das atividades da empresa, há uma grande preocupação da alta gestão das organizações com as infraestruturas que devem ser protegidas, visto que, com os recursos financeiros e de pessoal limitados, não se pode proteger todos os ativos da informação com o mesmo nível de segurança. Assim, uma metodologia para classificar o que é mais crítico e quais ativos estão em maior risco é de vital importância para a operação da organização. Utilizam-se as metodologias de estruturação de problemas complexos, o *Value-focused Thinking* (VFT), que oferece uma visão ampla da organização e dos processos críticos. Após a análise da atividade de valor do negócio, foi proposta uma adaptação de dois guias internacionais que tratam de segurança cibernética de infraestruturas críticas, de forma a generalizar esses modelos para qualquer tipo de empresas, públicas ou privadas. Um dos guias provém do NIST, entidade de padronização da área de TI do governo americano e o outro brasileiro, o guia do GSI, entidade responsável legal pela Segurança Cibernética nacional. Esses dois guias fornecem uma abordagem sobre o conteúdo das políticas e das ferramentas para implementação dessas políticas nas organizações em geral. Assim, propõe-se uma integração que abranja a classificação dos ativos como críticos e um processo de priorizá-los, com foco na Segurança Cibernética, a ser utilizado, como ferramenta inicial, na criação e aplicação de um Plano de Gestão de Riscos e Gestão Estratégica da Segurança da Informação.
Palavras-chave: Ativos críticos. Políticas de segurança. Segurança Cibernética. *Value-focused Thinking*.

1 Introdução

Os ataques cibernéticos estão cada vez mais frequentes no dia a dia das pessoas e das organizações. Por isso, a segurança cibernética (SC) se torna a cada dia mais relevante para a saúde das organizações públicas e privadas à medida que os sistemas e processos dessas instituições estão cada vez mais automatizados, interligados e, portanto, dependentes das infraestruturas de tecnologia da informação (TI).

Essa interligação faz com que as falhas nos sistemas de TI sejam catastróficas para as atividades cruciais das organizações. Assim como ataques que ocasionem o vazamento de informações – chamados de *Data Breach* –, tanto dos clientes quanto da própria operação da empresa, pode acarretar diversos problemas jurídicos, operacionais, financeiros e, ainda,

abalar a confiança pública e imagem da organização, acarretando grandes perdas ou até o próprio fechamento da empresa, no caso da privada, ou então prejudicar a sociedade afetando os sistemas de governos e instituições públicas.

Em 2019, o *Ponemon Institute* conduziu um estudo sobre os *Data Breach* em 16 países e regiões que quantificam os custos médio associados aos vazamentos de dados na ordem de US$ 3,94 milhões, um aumento de 1,5% em relação ao estudo do ano anterior (PONEMON, 2019). Além dessa perda financeira, o estudo mostrou como é difícil para as empresas se recuperarem do abalo à sua imagem.

Como forma de mitigar esse risco, as empresas, instituições e governos buscam cada vez mais aumentar a resiliência. Capacidade definida de continuar o cumprimento da missão da organização frente aos ataques cibernéticos e dificultar os ataques e os vazamentos de dados, aumentando os investimentos na SC e definindo políticas restritivas no tratamento de dados e na infraestrutura de TI. Custos esses que se tornam exponencialmente maiores a cada aumento no nível de segurança a ser implementada.

Apesar do ideal ser a proteção total, é economicamente impraticável fazer a proteção e a segurança plena de todos os ativos e sistemas com todos os níveis máximos de segurança, pois essas restrições, além de custosas, afetam negativamente a disponibilidade e a qualidade do serviço, conforme Sharifi (2008).

Dessa forma, a implantação viável e eficiente dos recursos na SC depende da correta identificação dos sistemas, equipamentos ou pessoas críticas para a missão principal ou processo vital, os quais são denominados “ativos críticos” para a organização. O sistema interligado que engloba esses ativos críticos, os equipamentos de TI, servidores de serviços, banco de dados, equipamentos de comunicação e acesso a serviços, é chamado de Infraestrutura Crítica da Informação (SEDGEWICK, 2014).

Essas infraestruturas da informação de uma organização suportam os sistemas cruciais do negócio, além de outras infraestruturas de suporte interligadas, e é um óbice a correta identificação e o detalhamento desses ativos, bem como da relação entre elas. Esse problema de detalhamento se torna complexo quanto maior a interação dos diversos setores e processos e da relação de influências das diversas infraestruturas críticas umas com as outras, como exemplo a energética sobre a tecnologia da informação.

Ao considerarmos a complexidade de identificação do problema, Checkland (2000) propõe uma observação holística do negócio, considerando o pensamento sistêmico, escopo

dos métodos de estruturação de problemas complexos (PSM, do inglês *Problem Structuring Methods*). Assim como Rosenhead (1996), o foco do estudo preliminar para problemas complexos deve ser inicialmente na identificação e estruturação do problema, antes de solucioná-lo.

Para essa estruturação ou caracterização do problema de identificação do que é crucial para a SC de uma organização, a metodologia *Value-Focused Thinking* (VFT), proposta por Keeney (1996), descreve os processos que apoiam a correta identificação dos ativos que geram valor à organização, para então, descendo ao nível tático, classificar quais ativos críticos suportam a operação principal e entender como priorizar a segurança dos ativos e, consequentemente, fazer a gestão de riscos de todas as infraestruturas críticas de TI da organização (ABNT, 2008).

Este trabalho é uma proposta de desenvolvimento de uma metodologia (*framework*) de classificação de ativos críticos a ser aplicada em uma organização, seja ela privada ou pública, com foco na segurança cibernética, como saída para uma posterior priorização das ações a serem implementadas de SC.

Em consequência ao problema identificado, este trabalho tem como objetivo geral propor uma metodologia de priorização de ativos críticos e de priorização de riscos para a Segurança Cibernética.

Os objetivos específicos são:

- Identificar os principais *frameworks* para a classificação de ativos críticos.
- Identificar as metodologias de priorização de riscos dos ativos críticos.
- Identificar os quesitos relevantes das etapas anteriores com foco na Segurança Cibernética.
- Propor uma metodologia de forma a sequenciar os resultados dos objetivos anteriores e realizar a classificação de ativos críticos para que, como próximo passo fora do escopo desse trabalho, seja realizada a posterior priorização dos riscos dos ativos para a Segurança Cibernética.

Com a crescente integração dos sistemas e dos processos nas organizações pelos meios de TI, aumenta a preocupação da alta gestão com essas infraestruturas, bem como a preocupação com a priorização da segurança, visto que, com os recursos financeiros e de pessoal limitados, não se pode proteger todos os sistemas da empresa com o mesmo nível de segurança. Assim, é crucial um processo de classificação e priorização do que realmente é

ativo crítico e quais ativos críticos estão em maior risco, já que um vazamento de informações dos clientes, bem como das informações operacionais do negócio, pode condenar a empresa a severas multas ou até à própria falência ou extinção. Ressalta Ponemon (2019) haver o consenso de que a classificação de ativos ou de riscos dos ativos é uma tarefa de grande importância para qualquer organização, porém ela não deve ser feita apenas pela gestão de TI.

Para alcançar os objetivos gerais e específicos para a essa seleção e o detalhamento dos ativos críticos, foram então descritos os principais conceitos e metodologias aplicáveis ao problema.

Ao tratar de problemas complexos, ou seja, de inter-relacionamentos, interdependências e conflitos de interesses dentro e fora da organização, é necessário utilizar metodologias para facilitar o entendimento dos conceitos e das ideias de maior relevância para o negócio da empresa ou organização pública, bem como há necessidade de formular o problema, no caso de classificação dos ativos de importância, de maneira mais organizada (ROSENHEAD, 1996) para, então, serem aplicados métodos de resolução do problema.

Para o tratamento do problema, os PSM são abordagens para tratar de níveis de incerteza, complexidade, conflitos, riscos para a definição e resolução dos problemas que não se limitam aos métodos quantitativos de tomada de decisão (ROSENHEAD, 1996), identificando o problema, mas não se limitando apenas ao descrito inicialmente, buscando fatores ou aspectos não detalhados inicialmente.

Entre os diversos PSM, os mais utilizados (MINGERS; ROSENHEAD, 2004) são: *Strategic Options Development and Analysis* (SODA), *Soft System Methodology* (SSM), *Strategic Choice Aproach* (SCA), e, além desses, o VFT. Ao contrário dos três primeiros métodos, que focalizam a definição do problema nas alternativas disponíveis (AFT, do inglês *Alternative-Focused Thinking*), o VFT, segundo Keeney (1996), primeiro aborda o pensamento orientado ao valor do negócio e em seguida nas alternativas para a resolução que possuem importância em relação aos valores trazidos por elas.

2 *Value-Focused Thinking* (VFT)

Os valores são fundamentais para o que fazemos, devendo ser a base para a tomada de decisão (KEENEY, 1996). No VFT os valores dos decisores são definidos anteriormente às alternativas, definidos como objetivos, o que segundo Keeney (1996) é a declaração de algo

que se busca alcançar. Devem ser orientados a três conceitos: um contexto de decisão, um objeto e uma direção de preferência. No caso desse estudo, o objetivo é: definir e priorizar os ativos críticos – no contexto de gestão de riscos de segurança cibernética – e o objeto: a atividade de gestão de riscos de ativos críticos.

A aplicação do VFT propõe-se a entender os sistemas, pessoas e infraestruturas da organização, com foco nos objetivos institucionais, ou seja, no valor (KEENEY, 1996), e dessa forma identificar quais são os ativos críticos e quais devem ser priorizados de forma a proteger a organização no quesito de segurança cibernética.

O VFT propõe inicialmente o esboço dos valores, objetivos, missão e a visão estratégica da organização, *top-down*, de forma macro, até os processos mais simples que suportam o atingimento dos objetivos. Havendo a comparação dos processos e das atividades dos diversos setores e o impacto diante da missão da organização, listando os objetivos e os atributos – características, recursos, entradas e saídas. Em seguida, é feita a classificação dos objetivos fundamentais, meios e fins, de forma a identificar os mais específicos.

Os objetivos fundamentais caracterizam uma razão essencial na situação-problema. Os objetivos meios são de interesse no contexto de decisão da alternativa a ser escolhida, são os meios para serem alcançados os fundamentais.

Então, é feita a definição dos indicadores para cada objetivo, de maneira a possibilitar a medição dos objetivos para quantificar o valor desses objetivos, utilizando o modelo de valor e a comparação das alternativas, com a finalidade de visualizarem-se os significados dos objetivos utilizando a *Strategic Utility Function* (KEENEY, 1992), conforme o Quadro abaixo.

Quadro 4 – Técnica de questionários

Técnica	Questões
Lista de desejos	O que você quer? O que você valoriza? O que você deveria querer?
Alternativas	O que é uma alternativa perfeita, uma alternativa terrível, alternativa razoável? O que é bom ou ruim sobre cada uma?
Problemas e deficiências	O que está certo ou errado com a sua organização? O que precisa de conserto?
Consequências	O que tem ocorrido? Foi bom ou ruim? O que poderia ocorrer que preocupa você?
Metas, restrições e orientações	Quais são suas aspirações? Quais são suas limitações?
Objetivos estratégicos	Quais são os seus objetivos finais? Que valores são absolutamente fundamentais a você?
Objetivos genéricos	Quais objetivos você tem para os seus clientes, seus funcionários, seus acionistas, e si mesmo? Quais objetivos ambientais, sociais, econômicos, ou saúde e segurança são importantes?
Objetivos estruturantes	Siga as relações meios-fins: por que aquele objetivo é importante? Como você pode alcançá-lo?

	Use especificação: o que você quer dizer com este objetivo?
Quantificar objetivos	Como você mede a realização deste objetivo? Por que o objetivo A é três vezes mais importante que o objetivo B?

Fonte: o autor.

Essa técnica de questionário é utilizada para se esclarecer quais os objetivos fundamentais e os meios. As ideias iniciais passarão por uma reflexão do que é objetivo, restrição ou mesmo critérios para as alternativas. No primeiro momento, as alternativas óbvias são as mais frequentes, porém é importante, segundo Keeney (1996), que se busque a melhor alternativa, descobrindo os objetivos ocultos, melhorar a comunicação, facilitar o envolvimento dos múltiplos *stakeholders*, interconectar as decisões, criar alternativas e identificar oportunidades de decisão.

No ambiente de uma organização, é previsível que cada setor procure priorizar as proteções que envolvam o seu setor, pois a visão é limitada de cada setor. Em contraposição a essa tendência, com uma análise holística o VFT tem como benefício a abordagem de uma decisão coletiva do que é mais importante para os objetivos estratégicos do negócio da instituição, seja ela uma empresa privada, pública ou híbrida, pois todas possuem a razão de existir.

3 *Framework for improving critical infrastructure cybersecurity*

Seguindo a pesquisa documental, foi encontrado o guia de aperfeiçoamento da segurança cibernética para infraestruturas críticas do *National Institute of Standards and Technology* (NIST), uma agência governamental regulatória de tecnologia dos EUA, que trata da segurança cibernética, especificamente, das infraestruturas críticas, porém define uma metodologia que possui relevantes ações e definições a serem observadas na classificação, não só dessas infraestruturas, mas também dos ativos críticos a que se propõe esse estudo. Assim define-se o próprio guia:

> Embora o Guia tenha sido desenvolvido para aperfeiçoar o gerenciamento do risco de segurança cibernética, uma vez que ele se relaciona com a infraestrutura crítica, ele pode ser utilizado por organizações em qualquer setor da economia ou da sociedade. Seu objetivo é ser útil para empresas, agências governamentais e organizações sem fins lucrativos, independentemente de sua área de atuação ou tamanho. (NIST, 2018).

O guia de aperfeiçoamento foi lançado pelo NIST com intuito de aprimorar a segurança das instalações críticas (IC). O Instituto descreve que os EUA dependem do funcionamento confiável das infraestruturas críticas e que, a cada dia, as ameaças exploram o aumento da

complexidade e da conectividade de sistemas e das IC, afetando as finanças e o resultado de uma organização. Segundo a entidade, a segurança cibernética é um elo importante do gerenciamento dos riscos da organização (NIST, 2018).

O guia utiliza uma abordagem baseada em riscos e focaliza os indicadores para orientar as atividades de segurança cibernética na gestão de riscos de TI, como parte do processo de gestão de riscos. Esse guia ajuda a priorizar as atividades de segurança da informação de acordo com os requisitos do negócio e ainda ajuda a lidar com a segurança cibernética, pois ela afeta a privacidade dos clientes e dos funcionários, bem como o funcionamento do próprio negócio.

O guia destaca que, para gerenciar os riscos de segurança cibernética, é necessário o entendimento claro dos indicadores do negócio da organização, assim como define a metodologia do VFT, que corrobora com a análise da missão da organização para a correta definição dos sistemas críticos.

A referência ainda reconhece a lei de proteção de dados e das liberdades civis (ambas em referência às legislações americanas) como instrumento de desenvolvimento da confiança da organização.

Os passos definidos pelo guia são:

- descrever as situações atuais no que tange à segurança cibernética (SC);
- descrever os objetivos no que tange à SC;
- identificar e priorizar oportunidades de aperfeiçoamento;
- avaliar os progressos frente aos objetivos; e
- comunicar aos *stakeholders* internos e externos os riscos apresentados na atual SC.

A metodologia relaciona os indicadores do negócio e as atividades de segurança cibernética. São elas: identificar, proteger, detectar, responder e recuperar (NIST, 2018). Essas funções, de maneira geral, definem o ciclo de vida da gestão de incidente de segurança.

Em seguida, descreve a importância de identificar como são os processos e como a instituição gerencia os riscos de segurança. Esse passo é importante para a classificação de ativos críticos, pois identifica se é ou não crítico, dependendo de fatores como *backup*, políticas de continuidade do serviço pela condição de reposição do equipamento ou de alternativas de continuidade do serviço por outros sistemas. Em outras palavras, a criticidade de um equipamento ou processo, mesmo que de baixo custo ou de pequena relevância, pode

ser definida por não haver equipamento reserva em relação a outro de grande importância, como um grande banco de dados, mas que já possua política e processos de recuperação já implantados na política de segurança da organização.

Finalmente, o guia encerra definindo o "como deve ser", propondo oportunidades de melhorias com base na situação atual e o estado desejado e possível.

4 Guia de Referência para a Segurança das Infraestruturas Críticas da Informação

Ainda sobre o assunto específico das infraestruturas críticas, porém na documentação nacional, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), órgão do Governo Federal responsável pela segurança cibernética das infraestruturas críticas nacionais, desenvolveu o guia de referência para a segurança das infraestruturas críticas da informação. Manual que define uma metodologia para assistir o GSIPR na missão de proteger as IC da informação (GSIPR, 2010).

Esse guia, assim como o anterior do NIST, também relaciona a segurança cibernética como uma atividade de gerenciamento de riscos. E ainda, em relação às outras duas referências anteriores, VFT e NIST, a função de todos os procedimentos sugeridos é diminuir os riscos da instituição no que diz respeito a atingir seus objetivos – relação do valor no caso do VFT – diminuindo a incerteza e aumentando a resiliência da organização, ou seja, sua capacidade de continuidade do negócio frente aos acontecimentos perturbadores e não desejados (ABNT, 2018).

Em relação a esse estudo, esse guia define macroprocessos para as ações de segurança cibernética das IC. Divididos em três processos, em que o primeiro é a identificação e classificação de ativos de informação; o segundo, a identificação de potenciais ameaças e vulnerabilidades; e o terceiro, a avaliação dos riscos.

O primeiro macroprocesso do guia tem grande similaridade com o problema de pesquisa deste estudo, ou seja, como identificar o que são os ativos críticos da informação para a organização e ainda como realizar a priorização dos riscos dos ativos, o que, no caso do guia, são das infraestruturas críticas, podendo ser relacionado e generalizado para a classificação dos ativos críticos.

Os macroprocessos seguintes, 2 e 3, são os possíveis trabalhos futuros a este estudo, pois descreve que a saída – *output* – do primeiro macroprocesso é a entrada – *input* – do

segundo, a identificação de potenciais ameaças e vulnerabilidades, e o terceiro, o gerenciamento do risco.

Ainda no primeiro processo, o guia define que o processo de identificação e a classificação de ativos de informação possui objetivos de prover à organização o entendimento comum das fronteiras, dos proprietários, de como o ativo é processado e transportado, e o consequente valor que os ativos representam para o negócio, como forma de finalizar o terceiro macroprocesso, que é desenvolver e aplicar os planos de gerenciamento de riscos.

Após essas referências, onde foram identificados diferentes metodologias e procedimentos de diferentes autorias, mas que se complementam no método proposto para a resolução do problema de estudo desse trabalho. Destaca-se a importância e a inovação desse trabalho para a integração de métodos para a completa identificação e priorização dos ativos de qualquer organização, não se limitando apenas às IC, conforme a metodologia desenvolvida e detalhada a seguir.

5 Metodologia de pesquisa

O trabalho foi realizado primeiramente propondo-se uma metodologia que iniciou com uma pesquisa bibliográfica e documental, com o intuito de identificar teorias, métodos, manuais e referências, de forma a definir como deve ser abordada a gestão estratégica da organização no âmbito de segurança cibernética. Analisando-se os processos principais do negócio com o intuito de listar as atividades e os ativos da informação que são críticos e que suportam o negócio.

Em seguida, haverá a busca e a adequação das metodologias de referência – VFT e guias do NIST e do GSI/PR – das metodologias e documentos nas referências que se aplicam ao tema de classificação de ativos críticos que, de acordo com uma pesquisa inicial, não foi encontrado especificamente sobre o tema, e sim a classificação de ativos críticos nas metodologias apenas de infraestruturas críticas, o que ressalta a inovação e a relevância de um estudo abrangente a ser aplicado à todas as organizações.

Nessa fase, são analisados os critérios, a aplicabilidade dos métodos, que se baseiam em formulários e pesquisas nas IC, e ainda a adequação das metodologias, das infraestruturas críticas de governo, com vistas a uma aplicação mais genérica nas organizações públicas e privadas.

A proposta então, fruto dessas pesquisas, é de uma metodologia inovadora que apoie a classificação dos ativos de forma a realizar a categorização como um ativo crítico da informação para os objetivos da organização. Com o intuito de, como atividade futura, realizar a priorização geral dos ativos e da gestão de risco de segurança cibernética para a organização. Descrevendo as limitações, a aplicabilidade e os resultados esperados dessa classificação.

Trata-se de pesquisa exploratória, bibliográfica e documental, pois busca coletar informação que ainda não é de conhecimento antecipado. Após uma breve pesquisa, observou-se uma lacuna nessa área, visto que, apesar de a proteção ser um assunto de grande importância nas empresas e de todos os decisores terem consciência de que deve ser feita a gestão de riscos dos ativos, a priorização do que se deve ser protegido e o como é uma tarefa árdua e de extrema importância, embora que de difícil definição para a organização, que não deve ser desenvolvida somente pelos gerentes de TI, mas por toda a organização, em um trabalho colaborativo.

É, portanto, uma pesquisa bibliográfica e documental de metodologias de identificação dos valores e da bibliografia segurança da informação para infraestruturas críticas existentes. Finalizando com uma proposta de uma integração dos métodos identificados em uma nova metodologia mais genérica para as organizações. Cumpridos os objetivos parciais de identificar os principais *frameworks* para a classificação de ativos críticos e identificar as metodologias de priorização de riscos dos ativos críticos.

As infraestruturas críticas da informação são os ativos: equipamentos, processo, sistemas e pessoas que, caso sejam danificados ou sejam indisponibilizados, prejudicam ou podem prejudicar de forma catastrófica a organização. Assim, a classificação dos ativos críticos da informação com foco na segurança da informação é uma tarefa preliminar de grande relevância para a gestão de risco de segurança cibernética na organização.

Os primeiros passos da metodologia proposta neste estudo começam com a utilização do VFT, que deve, inicialmente, ser realizada por uma coleta de dados, por meio de pesquisa documental e entrevistas aos gerentes e altos decisores do negócio, questionando-se os objetivos estratégicos da organização.

Os valores fundamentais são a força motriz da instituição, sua função social. Primeiramente, devem-se identificar os objetivos fundamentais, por diversas técnicas, como lista de desejos, alternativas, fraquezas da organização (KEENEY, 1996). Haverá nessa lista inicial diversos objetivos, restrições e alternativas que devem ser analisados e convertidos em

objetivos fundamentais e meios. Os objetivos meios são os necessários para se atingir os fundamentais.

As primeiras alternativas de solução dos problemas são geralmente as mais óbvias e utilizadas em situações análogas (KEENEY, 1996). Segundo Keeney (1996), alternativas verdadeiramente diferentes permanecem escondidas, necessitando de persistência para que se as encontre. No caso dos objetivos do negócio, deve-se entender a razão de ser da organização, quem são os clientes e, então, que processos suportam os objetivos estratégicos e os objetivos meios. Mas, geralmente, os finais são confundidos com os meios (KEENEY, 1996).

Uma empresa de *e-commerce* serve para satisfazer as necessidades dos clientes e, então, obter lucro com isso. Logo, os processos de venda, distribuição, catálogo de clientes e fornecedores são os principais processos e, consequentemente, os ativos, processos, sistemas e banco de dados diretamente ligados a essas atividades, os ativos críticos. Porém, além desses processos e ativos tangíveis, há ainda outros intangíveis como os próprios decisores que realizam esses processos.

Além dos ativos explícitos, como bancos de dados e tabela de clientes, há ainda os intangíveis, como os vendedores, que também são considerados ativos críticos, devido ao seu conhecimento tácito desses atores, que geram valor ao negócio e que, por produzirem valor, também se tornam ativos a serem protegidos, na visão do negócio.

Como primeiro passo, os objetivos fundamentais devem ser divididos em categorias e devem ser completos no sentido de descreverem o propósito da organização, sem haver intercalação ou sobreposição de objetivos.

Os objetivos meios devem ser completos e abranger todos os processos, sistemas, relacionamentos da instituição. Assim, como forma de delimitação do problema deste trabalho, devem ser listados os processos e os ativos ligados à informação. Esses ativos devem ser categorizados como ativos críticos. Em seguida, deverão ser descritos os indicadores de cada objetivo, por meio da definição de métricas e medidores de execução ou atingimento do objetivo. Indicador é uma ferramenta que permite a obtenção de informações sobre uma atividade (MITCHELL, 2008) e serve para medir o grau de sucesso da implantação de uma estratégia em relação ao objetivo pretendido (CORAL, 2002).

Na segunda fase, utilizando-se das metodologias do NIST, são aplicados os formulários de segurança, para identificar as atividades de segurança cibernéticas e os resultados

esperados frente aos objetivos e processos listados na primeira parte. Nessa fase, serão listadas as políticas, regras, legislações e a maneira de permitir a comunicação das atividades. Estas atividades de identificar, proteger, detectar, responder e recuperar listam todas as tarefas a serem implementadas.

O nível de maturidade demonstra o estado de aplicação de cada atividade. Podendo-se analisar, então, os riscos conhecidos e esperados, e os desconhecidos, bem como seus impactos na atividade do negócio. Finaliza-se o processo com uma avaliação que pode identificar oportunidades, deficiências e comparar a situação atual com a desejada (NIST, 2018), detalhando o processo de gestão da segurança como a diferença entre essas situações.

No questionário de segurança cibernética apresentado pelo NIST, propõe-se que se conheça o nível de maturidade, perguntando-se sobre atividades, políticas implementadas, além de classificar as organizações em níveis de maturidade, conforme o seguinte quadro.

Quadro 5 – Níveis de maturidade em Segurança Cibernética

Nível	Processo de Gerenciamento de Risco	Programa Integrado de Gerenciamento de Risco	Participação Externa
1 - Parcial	*Práticas de gerenciamento de risco de segurança cibernética organizacional não são formalizadas*, e o risco é gerenciado de maneira ad hoc e às vezes reativa.	Consciência limitada do risco de segurança cibernética no nível organizacional. A organização implementa o gerenciamento de riscos de segurança cibernética de maneira irregular, caso a caso, devido à experiência variada ou a informações obtidas de fontes externas.	A organização não colabora com ou recebe informações (por exemplo, inteligência de ameaças, melhores práticas, tecnologias) de outras entidades (por exemplo, compradores, fornecedores, dependências, dependentes, pesquisadores, governos), nem compartilha informações.
2 - Risco Informado	Práticas aprovadas A priorização das atividades de segurança cibernética e as necessidades de proteção são permeadas diretamente pelos objetivos de risco organizacionais.	Há uma conscientização do risco de segurança cibernética no nível organizacional, mas não foi estabelecida uma abordagem válida para toda a organização para gerenciar o risco de segurança cibernética. Informações de segurança cibernética são compartilhadas informalmente dentro da organização.	A organização colabora e recebe algumas informações de outras entidades e gera algumas de suas próprias informações, mas pode não compartilhar informações com outras pessoas.
3 - Reproduzível	As práticas de gerenciamento de risco da organização são formalmente aprovadas e expressas como política. Práticas organizacionais de segurança cibernética	Existe uma abordagem para toda a organização para gerenciar o risco de segurança cibernética. Políticas, processos e procedimentos de conhecimento de riscos são definidos, implementados conforme pretendido e revisados.	Colabora e recebe regularmente informações de outras entidades que complementam informações geradas internamente, e compartilha informações com outras entidades.

	são atualizadas regularmente com base na aplicação dos processos de gerenciamento de riscos às mudanças nos requisitos de negócios/missão.	Existem métodos consistentes para responder de forma eficaz às mudanças no risco.	
4 - Adaptável	A organização adapta suas práticas de segurança cibernética com base em atividades de segurança cibernética anteriores e atuais, incluindo lições aprendidas e indicadores preditivos.	Existe uma abordagem para toda a organização para o gerenciamento do risco de segurança cibernética que usa políticas, processos e procedimentos de conhecimento de risco para tratar possíveis ocorrências de segurança cibernética. A relação entre o risco de segurança cibernética e os objetivos organizacionais é claramente entendida e analisada durante o processo de tomada de decisões.	Ela recebe, gera e analisa informações priorizadas que informam a análise contínua de seus riscos à medida que os cenários de ameaças e tecnologia evoluem. A organização compartilha essas informações internamente e externamente com outros colaboradores. A organização usa informações em tempo real

Fonte: NIST, 2018 (com adaptações).

Em relação ao processo de gerenciamento de risco, primeira coluna, são identificados os níveis de implementação dos processos da organização, desde as práticas não formalizadas até a implementação adaptável dos processos, com acompanhamento em tempo real.

Na segunda coluna, em relação ao programa integrado de gerenciamento de risco, são identificados os objetivos parciais de como as atividades de segurança cibernética permeiam as políticas da organização e o alinhamento dessas atividades de segurança aos objetivos do negócio. Essa coluna, onde há a comparação das práticas de cibernéticas com os objetivos organizacionais, está diretamente alinhada aos objetivos propostos deste trabalho. Podendo-se observar os níveis de aplicação, desde a inicial - ter uma consciência limitada do risco de um vazamento de dados, por exemplo - até a aplicação plena, de acordo com a tabela: "*A relação entre o risco de segurança cibernética e os objetivos organizacionais é claramente entendida e analisada durante o processo de tomada de decisões*" (NIST, 2018, grifo nosso, tradução nossa).

Resumidamente, o guia define as etapas que podem ser facilmente aplicadas ao escopo da metodologia proposta neste estudo:

1. Priorize e determine o escopo. A organização identifica seus objetivos de negócios/missão e prioridades organizacionais de alto nível;

2. Oriente. Uma vez que o escopo do programa de segurança cibernética tenha sido determinado para a linha de negócios ou processo;
3. Crie uma avaliação atual. A organização desenvolve uma avaliação atual, indicando que resultados de categoria e subcategoria da estrutura básica estão sendo alcançados no momento;
4. Realize uma avaliação de risco. Esta avaliação pode ser guiada pelo processo geral de gerenciamento de riscos da organização ou atividades anteriores de avaliação de risco;
5. Criar uma avaliação desejada. A organização cria uma avaliação desejada que enfoca a avaliação das categorias e subcategorias do guia;
6. Determinar, analisar e priorizar as falhas. A organização compara a avaliação atual e a avaliação desejada para determinar as lacunas; e
7. Implementar o plano de ação. A organização determina que ações devem ser tomadas para tratar as lacunas, se houver, identificadas na etapa anterior e, em seguida, ajusta suas práticas atuais de segurança cibernética para alcançar a avaliação desejada.

Assim, ao implementar essas atividades, tem-se uma clara visualização da maturidade atual e da situação futura a ser atingida para toda a organização, porém, em relação ao escopo deste estudo, esse guia é ainda muito amplo. Assim, de forma a continuar a análise do VFT e dos relacionamentos apenas com os sistemas de TI, de segurança de informação, com os objetivos do negócio.

Relacionado ainda aos objetivos desta pesquisa, apesar de o guia não detalhar como realizar a tarefa, descreve a atividade dentro da categoria “Gerenciamento dos Ativos” na primeira função, “identificar” a atividade proposta por essa metodologia de classificar e priorizar os ativos críticos. Detalhando a atividade como:

> Gerenciamento de Ativos (ID.AM): Os dados, pessoal, dispositivos, sistemas e instalações que permitem que a organização atinja objetivos de negócio são identificados e gerenciados de maneira consistente com sua importância relativa para os objetivos organizacionais e a estratégia de risco da organização. (NIST, 2018).

O guia do NIST detalha, portanto, muito bem as tarefas que devem ser feitas em relação à segurança cibernética, sem descrever o “como fazer”.

Como forma de encontrar-se um método de análise, de como classificar e priorizar, foi identificado o guia de referência para a segurança das infraestruturas críticas da informação do Gabinete de Segurança Institucional (GSIPR, 2010), que será detalhado a seguir.

Segundo esse outro guia do GSI/PR, com a finalidade de identificar se o ambiente é ou não seguro, do ponto de vista da segurança da informação, considerando-se os critérios de disponibilidade, integridade, confidencialidade e autenticidade (DICA) são aplicados formulários e entrevistas com os diversos setores da organização.

O guia do GSI/PR, apesar de também estar focado nas infraestruturas críticas, como a referência anterior, inicia o questionário com perguntas relacionadas a qual grande área, energética, hídrica, defesa etc. está relacionada a IC. Apresenta uma boa referência de "o que" perguntar, ou "o que" se deve saber em relação aos serviços, ainda apresenta o processo macro a ser implementado, para uma plena ação de gerenciamento do risco para a organização: Mapeamento dos Ativos de Informação.

De forma relevante para a metodologia e as propostas deste trabalho, o manual define que a gestão de risco, quando implementada, possibilita aumentar a probabilidade de atingir seus objetivos; identificar e tratar os riscos de toda a organização; melhorar os controles; minimizar perdas; entre outros.

Dentro desse macroprocesso, são definidas as atividades para o aperfeiçoamento da segurança cibernética, no caso, para infraestruturas críticas, mas que podem ser facilmente aplicadas a qualquer organização. Divididos em três processos, são eles:

1. identificação e classificação de ativos de informação;
2. identificação de potenciais ameaças e vulnerabilidades; e
3. avaliação de riscos.

A identificação e classificação de ativos utilizam-se como entrada à listagem dos equipamentos, *software*, interfaces, dados e informações, pessoas e locais físicos, além de legislações e regulamentos da organização. Após a identificação e classificação, as saídas são as fronteiras dos sistemas, onde estão as bordas e os limites para outros sistemas, e a outra saída, alinhada a este estudo é a relação de sistemas, locais, pessoas, dados e o valor do ativo da informação.

As saídas desse macroprocesso são as entradas para a próxima etapa, que identifica as potenciais ameaças e vulnerabilidades. Resumidamente, busca coletar, internamente e externamente, histórico de ocorrências, auditorias, testes de segurança, quantidades de

ataques pela experiência dos gestores, os relatos de falhas em *softwares* e vazamentos nos sistemas, em procura nos bancos de dados públicos de órgãos especializados, baseados nas listas de equipamentos, *softwares* etc., do inventário da organização (primeira etapa).

Na terceira, é feita a gestão de risco propriamente dita, onde são observados os ativos críticos (fase 1), o histórico de ataques e vulnerabilidades (fase 2) e o plano de gestão de risco com a classificação das ações, de forma a minimizar o risco de segurança da informação para a organização. Essa etapa é finalizada com a criação das listas de riscos priorizadas, lista de ativos de informação priorizadas por necessidade de proteção, resultados das avaliações dos controles utilizados e da lista de novos controles recomendados.

Detalhando um pouco mais a primeira etapa, por ser a mais relevante para este estudo, o guia divide a classificação em seis atividades: (1) coletar informações gerais; (2) definir as informações dos ativos; (3) identificar o(s) responsável(is); (4) identificar os contêineres dos ativos; e (5) definir os requisitos de segurança; e (6) estabelecer o valor do ativo de informação.

E, então, dessa forma identificam-se os históricos dos ativos com informações da alta gestão e dos proprietários dos recursos de informação. Identificar os contêineres da informação, onde estão armazenadas, é uma etapa de grande relevância, pois, como define o guia,

> Os ativos de informação são protegidos a partir dos controles implementados nos seus respectivos contêineres, ou seja, o nível de proteção fornecido pelos controles relaciona-se diretamente com a efetividade ao atendimento dos requisitos de segurança do ativo de informação. (GSIPR, 2010).

De maneira geral, os ativos são divididos em: sistemas e aplicações; *hardwares* e pessoas, para então definir os requisitos de segurança e finalizar com o estabelecimento do valor do ativo.

Assim, a integração das referências utilizadas neste estudo torna-o inovador ao integrar a estruturação de problemas complexos e as metodologias de segurança para infraestruturas críticas de qualquer organização, detalhando de forma resumida os passos no quadro abaixo.

Quadro 6 – Integração da estruturação de problemas complexos com as metodologias de segurança para infraestruturas críticas

Etapa	Entrada/ Metodologia	Processo	Atividades	Saída	Referência
1	Entrevista e pesquisa documental	Identificação do valor negócio.	• Identificação dos Processos críticos. • Identificação das informações críticas.	Lista de processos críticos. Classificação dos ativos que suportam os processos críticos.	VFT
2	Pesquisas documental, entrevistas e formulários	Identificação do nível de maturidade e de controles.	• Identificação dos níveis de implementação da segurança. • Classificação da maturidade dos diversos setores da organização.	Planilha de maturidade das atividades de segurança da organização.	GUIA NIST
3	Pesquisa documental, entrevistas e análise quantitativa e qualitativa	Identificação e classificação dos ativos críticos.	• Identificação dos equipamentos, contêineres, pessoas e bordas dos sistemas. • Análise quantitativa dos valores dos ativos. • Análise qualitativa dos controles dos ativos de segurança. • Classificação dos ativos críticos. • Priorização dos ativos conforme a necessidade de controles.	Planilha de classificação e priorização de ativos críticos. Esboço do plano de gestão estratégica de Segurança da informação.	GUIA GSIPR

Fonte: o autor.

6 Conclusões

A tarefa de proteger os ativos da informação de uma organização se torna uma tarefa complexa, devido ao custo elevado e à grande quantidade de ativos a serem protegidos. Como forma de aplicação a esse problema, a classificação e a priorização foram o objeto de estudo deste trabalho, considerado o escopo da segurança cibernética e identificados os processos e ativos de valor para a organização.

O resultado é uma proposta preliminar, mas inovadora de integração de métodos aplicados à classificação dos ativos como críticos e um processo seguinte de priorizá-los para a gestão da segurança cibernética e para ser utilizado como ferramenta inicial na criação e aplicação de um Plano de Gestão de Riscos e Gestão Estratégica da Segurança da Informação.

Para isso, o VFT contribuiu com o foco na visão geral da organização, buscando os processos críticos que agregam mais valor à organização, ou seja, uma análise macro dos

processos mais relevantes para o negócio principal da organização. E, ainda, com a lista dos ativos críticos que suportam esses processos.

Em seguida, foram analisados dois guias, primeiramente do NIST, que proveu uma clara identificação das atividades de segurança e dos métodos de identificação dos níveis de maturidade da organização no quesito da segurança dos ativos críticos.

Finalmente, o guia do GSIPR, de forma mais prática, demonstrou as atividades, os processos, as entradas e saídas para a classificação dos ativos críticos da informação para a infraestrutura crítica, porém aplicável a qualquer organização após algumas modificações e considerações propostas neste estudo.

Então, como próximas ações após a metodologia inovadora proposta neste trabalho, poderão ser feitos estudos relacionados à implementação de políticas de controles automatizados que analisam e identificam alteração nas políticas de segurança e atualizam os estados de maturidade, como forma de propor um plano de criação e acompanhamento para a Gestão Estratégica de Segurança Cibernética.

Referências

ABNT – Associação Brasileira de Normas Técnicas. *NBR ISO/IEC 27005–Tecnologia da Informação–Técnicas de Segurança–Gestão de Riscos de Segurança da Informação*. Rio de Janeiro: ABNT, 2008.

ABNT - Associação Brasileira de Normas Técnicas. *NBR ISO 31000:2018-Gestão de Riscos - Diretrizes*. Rio de Janeiro, RJ. ABNT, 2018.

BRASIL. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. *Guia de Referência para a Segurança das Infraestruturas Críticas da Informação*. Versão 1. Brasília. nov. 2010. Disponível em: http://dsic.planalto.gov.br/legislacao/2_Guia_SICI.pdf. Acesso em: 28 out. 2019.

CANONGIA, Claudia; GONÇALVES JÚNIOR, Admilson; MANDARINO JUNIOR, Raphael. *Guia de Referência para a Segurança das Infraestruturas Críticas da Informação*. Brasília, DF: GSIPR/SE/DSIC 2010.

CHECKLAND, Peter. Soft systems methodology: a thirty year retrospective. *Systems research and behavioral science*, v. 17, n. S1, p. S11-S58, 2000.

CORAL, Eliza *et al*. *Modelo de planejamento estratégico para a sustentabilidade empresarial*. 2002.

KEENEY, R. L.; Value focused thinking: a path to creative decision making. Cambridge, MA: Harvard University Press, 1992.

KEENEY, Ralph L. *Value-focused thinking*. Harvard University Press, 1996.

MINGERS, John; ROSENHEAD, Jonathan. Problem structuring methods in action. *European journal of operational research*, v. 152, n. 3, p. 530-554, 2004.

MITCHELL, Gordon. Problems and fundamentals of sustainable development indicators. *Sustainable development*, v. 4, n. 1, p. 1-11, 1996.

NIST – National Institute of Standards and Technology. *Framework for improving critical infrastructure cybersecurity*. Gaithersburg: NIST, 2018. Disponível em: https://doi.org/10.6028/NIST.CSWP.04162018. Acesso em: 10 out. 2020.

PONEMON INSTITUTE. *2019 Cost of Data Breach Study*. 2019. Disponível em: https://www.ibm.com/security/data-breach. Acesso em: 10 out. 2019.

ROSENHEAD, Jonathan. What's the problem? An introduction to problem structuring methods. *Interfaces*, v. 26, n. 6, p. 117-131, 1996.

SEDGEWICK, Adam. *Framework for improving critical infrastructure cybersecurity, version 1.0*. 2014.

SHARIFI, Mohammad *et al*. Lessons learned in ITIL implementation failure. *In*: INTERNATIONAL SYMPOSIUM ON INFORMATION TECHNOLOGY. IEEE, 2008. p. 1-4.

O conceito de dissuasão cibernética: relevância e possibilidades

Cícero Araújo Lisboa

Guilherme Ziebell

Resumo: Este trabalho tem como objetivo discutir o conceito de dissuasão cibernética. Diante de sua crescente importância na vida das sociedades, o ciberespaço passou a ocupar dimensão central também nas preocupações estratégicas de qualquer nação. Frente à possibilidade de existência de conflitos de natureza cibernética, a reflexão a respeito do conceito de dissuasão cibernética, bem como de sua viabilidade e relevância, impõe-se. Nesse contexto, o trabalho tem por objetivo discutir a noção de dissuasão cibernética, considerando suas possíveis aplicações e limitações, bem como suas características principais, avaliando suas similaridades e diferenças em relação ao conceito de dissuasão convencional. A pesquisa tem natureza aplicada, caráter exploratório e abordagem qualitativa, apoiando-se em revisão bibliográfica e documental. Após uma discussão sobre o conceito de dissuasão e suas particularidades, o trabalho apresenta uma análise da segurança cibernética, dando especial atenção à discussão das ameaças cibernéticas - sobretudo aquelas pertinentes ao setor aeroespacial. Por fim, realiza-se uma discussão sobre a aplicação do conceito de dissuasão no âmbito da segurança cibernética, demonstrando sua aplicabilidade e ressaltando suas principais potencialidades e limitações. O trabalho demonstra que o conceito de dissuasão cibernética, a despeito de apresentar limitações, desafios e peculiaridades, tem grande relevância e operacionalidade nas discussões sobre segurança cibernética contemporânea, tratando-se, portanto, de um tema que exige atenção especial dos responsáveis pela defesa nacional.
Palavras-chave: dissuasão cibernética, segurança cibernética, segurança espacial.

1 Introdução

Em maio de 2019, em mais um capítulo de violência entre Israel e Palestina, na faixa de Gaza, 25 palestinos e 4 israelenses foram mortos em um final de semana, durante um bombardeio. Após décadas de conflito, isso não seria uma surpresa. Entretanto um aspecto chamou atenção dos especialistas em segurança cibernética: pela primeira vez as Forças Armadas de Israel haviam bombardeado um prédio que supostamente serviria de base para um grupo de *hackers* do Hamas (NEWMAN, 2019). Por meio de seu perfil na rede social Twitter, as Forças Armadas de Israel (IDF) afirmaram que haviam frustrado "uma tentativa de ofensiva cibernética do Hamas contra alvos israelenses. Após nossa operação de defesa cibernética bem-sucedida, visamos um prédio onde o Hamas operava no ciberespaço. HamasCyberHQ.exe foi removido" (IDF, 2019, tradução nossa).

Considerado por especialistas em segurança cibernética como o primeiro ataque físico disparado como resposta a ataques digitais, tal fato, contudo, não é inesperado (DOFFMAN, 2019). Desde 2011, a estratégia nacional de segurança cibernética dos Estados Unidos considera a possibilidade de uma resposta cinética contra ataques realizados por meio do ciberespaço (THE WHITE HOUSE, 2011; 2018). Tal questão se mostra de grande relevância para o país, não apenas porque os Estados Unidos são cada vez mais dependentes do ciberespaço para o fluxo de bens e serviços, para o suporte ao controle de suas infraestruturas críticas – como eletricidade, distribuição de água, sistema financeiro, transporte e comunicação –, e para o comando e controle de sistemas militares, mas também porque tal dependência é acompanhada por um aumento simultâneo da quantidade e da capacidade de atividades maliciosas no ciberespaço desenvolvidas por outros atores – estatais ou não estatais (NYE, 2016).

Por meio do ciberespaço, hoje é possível, além de oferecer entretenimento (como filmes, músicas, redes sociais, etc.), controlar infraestruturas críticas, gerir os sistemas financeiros, armazenar propriedade intelectual, prover serviços de governo eletrônico, entre outros. Todas essas possibilidades de uso transformaram o ciberespaço em um ambiente estratégico para os governos, os negócios e as sociedades (TEN; MANIMARAN; LIU, 2010). Entretanto existem, também, muitas ameaças no ciberespaço. Em 2019, o Fórum Econômico Mundial elencou os ataques cibernéticos entre os cinco maiores riscos que a humanidade enfrentaria naquele ano (MYERS; WHITING, 2019). De acordo com o Relatório Anual Oficial de Crimes Cibernéticos de 2019 da *Cybersecurity Ventures*, o crime cibernético é a maior ameaça para todas as empresas no mundo e um dos maiores problemas que a humanidade enfrenta. O relatório estima que o cibercrime custará ao mundo mais de US$ 6 trilhões por ano até 2021, ante US$ 3 trilhões em 2015 (VENTURES, 2020).

Casos de ataque à soberania dos países também representam uma ameaça no ciberespaço. Um dos eventos mais conhecidos foi o da sabotagem das instalações nucleares do Irã, em 2010, pelo *worm*[11] de computador *Stuxnet*, que causou a destruição de grande parte da planta de enriquecimento de urânio daquele país (SINGER; FRIEDMAN, 2014). Outro caso importante ocorreu em 2007, na Estônia, quando, após divergências entre o governo do país e o governo da Rússia sobre a remoção de um memorial da Segunda Guerra, a Estônia

[11] *Worm* é semelhante a um vírus de computador, podendo prejudicar usuários e sistemas de diversas formas, porém, possui a capacidade de se autorreplicar.

passou a receber ataques cibernéticos em massa, que eram destinados ao governo, aos bancos e à imprensa. Para fazer frente aos ataques, o governo estoniano precisou desativar o acesso de endereços IP[12] externos, e o país levou meses para se recuperar totalmente (CLARKE; KNAKE, 2011).

Há, ainda, outros casos que podem ser citados. Especula-se que em 2007 Israel tenha utilizado armas cibernéticas para impedir que a Força Aérea Síria percebesse o avanço de aviões israelenses, que passaram sem ser detectados pelos radares sírios no ataque aéreo realizado ao país árabe em setembro daquele ano (SINGER; FRIEDMAN, 2014). Em 2008, a Geórgia, durante o conflito que se desenrolou com a Rússia, sofreu ataques de negação de serviço[13] que paralisaram sua *internet*, limitando a capacidade do governo de comunicar-se com a população e o mundo, ao mesmo tempo em que as forças russas cruzavam sua fronteira (CLARKE; KNAKE, 2011). Também pode-se citar o Brasil, que foi alvo de um programa de vigilância mantido pelos Estados Unidos, que monitorava *e-mails* e ligações telefônicas do governo brasileiro. Esse fato foi revelado por Edward Snowden, em 2013, e provocou mal-estar diplomático entre os dois governos (FERRAÇO, 2014).

Com os países cada vez mais incorporando capacidades de segurança e defesa cibernéticas, torna-se necessário capacitar suas organizações para promover a proteção de seus ativos de informação mais valiosos e de suas infraestruturas críticas. Dessa forma, a partir do momento em que dispositivos de controle, sejam industriais ou militares, começam a utilizar funcionalidades definidas por *software*[14], tornam-se vulneráveis às ameaças do ciberespaço. Assim, medidas de segurança cibernética tornaram-se necessárias para a proteção destes e, até mesmo, para desenvolver ações de planejamento militar contra ataques, conforme o nível de criticidade dos ativos envolvidos.

Em 2017, Jeanette Hanna-Ruiz, diretora de segurança da informação da Agência Espacial Americana (NASA), responsável por proteger os dados enviados do espaço para o planeta Terra contra ataques cibernéticos, disse em entrevista que "[é] uma questão de

[12] Do inglês *Internet Protocol address* (*IP address*), é um rótulo numérico atribuído a cada dispositivo (computador, impressora, smartphone etc.) conectado a uma rede de computadores que utiliza o Protocolo de *Internet* para comunicação. Um endereço IP serve a duas funções principais: identificação de interface de hospedeiro ou de rede e endereçamento de localização.

[13] A Negação de Serviço ocorre quando sites são repentinamente submetidos a uma grande quantidade de acessos, assim sobrecarregando os recursos computacionais (rede, memória, capacidade de processamento) dos servidores alvo.

[14] *Software* é um programa, rotina ou conjunto de instruções que controla o funcionamento de um computador.

tempo até alguém invadir algo no espaço" (SYEED, 2017, tradução nossa). Em 2018, a empresa de segurança cibernética *Symantec* denunciou uma sofisticada campanha de *hackers* que seria supostamente lançada por computadores chineses contra operadores de satélites, empresas de defesa e de telecomunicações nos Estados Unidos e no sudeste da Ásia. A empresa sugere que o ataque pode ter sido impulsionado por metas de espionagem e a interceptação de comunicações militares e civis (G1 ECONOMIA, 2018).

Essa capacidade de interceptação não é inédita. Além dela, outra grande ameaça é a de que os *hackers* possam alterar as posições dos dispositivos em órbita. Um dos casos mais conhecidos aconteceu em 1998, quando *hackers* assumiram o controle do telescópio alemão ROSAT e modificaram o posicionamento dos painéis solares do telescópio, o que acabou danificando as baterias do equipamento. Outro caso importante foi o sequestro dos satélites britânicos SkyNet, em 1999, no qual os criminosos pediram um resgate em dinheiro para devolver o controle sobre eles (AKOTO, 2020).

Tais acontecimentos, que misturam ações militares e de inteligência, são fundamentais para que muitos pesquisadores considerem que nos aproximamos, cada vez mais, de um cenário de potencial eclosão de guerras cibernéticas em nível global (NYE, 2016). É justamente frente à possibilidade de existência de conflitos dessa natureza que a reflexão a respeito do conceito de dissuasão cibernética, bem como de sua viabilidade e relevância, impõe-se e traz a seguinte questão: pode um país dissuadir outros Estados ou grupos não estatais no âmbito do ciberespaço? Diante disso, o presente trabalho busca discutir a noção de dissuasão cibernética, considerando suas possíveis aplicações e limitações, bem como suas características principais, avaliando suas similaridades e diferenças em relação ao conceito de dissuasão convencional.

Para alguns pesquisadores, o conceito de dissuasão é inseparável da ideia de ameaça de punição retaliatória - ou seja, a teoria de dissuasão clássica repousa em dois mecanismos principais, uma ameaça crível de punição por uma ação e a negação de ganhos de uma dada ação. No livro *Arms and Influence*, Schelling (1966) refere-se ao poder de ferir como um dos atributos mais impressionantes da força militar, visto que a expectativa de sofrimento pode motivar as vítimas a quererem evitar a dor ou a tentarem evitar perder algo. No entanto existem muitas dúvidas se uma dissuasão cibernética poderia imprimir nos adversários a mesma linguagem utilizada na dissuasão convencional.

Esse trabalho tem natureza aplicada e caráter exploratório, adotando uma abordagem qualitativa e apoiando-se em revisão bibliográfica (de artigos e de livros) e documental. Sendo assim, e de forma a atingir os objetivos propostos, está estruturado em três seções, além desta introdução e da seção de conclusão. A primeira seção apresenta uma contextualização dos diversos elementos que compõem a dissuasão convencional, sua definição e características. A segunda seção apresenta uma discussão a respeito do conceito de segurança cibernética, fazendo uma análise em relação à segurança da informação e da segurança dos ativos de tecnologia de informação e comunicação. Por fim, na terceira parte é realizada a análise da aplicação do conceito de dissuasão no âmbito da segurança cibernética, bem como algumas considerações a respeito de como ela pode ser aplicada para enfrentar os desafios da defesa cibernética na projeção espacial brasileira.

2 O conceito de dissuasão

O conceito de dissuasão, em sua essência, pode ser entendido como a decisão de um ator de não realizar uma determinada ação contra um segundo ator, a partir da percepção de que os potenciais custos e riscos envolvidos em tal ação não compensam os eventuais benefícios esperados (MEARSHEIMER, 1981). Ainda que as discussões sobre a questão remontem ao menos ao século V a.C., no contexto da Guerra do Peloponeso[15], sua relevância contemporânea para as Relações Internacionais começou a desenhar-se nos anos iniciais do século XX (JERVIS, 1979). Os desenvolvimentos tecnológicos do período, especialmente a possibilidade de realização de ataques aéreos, foram fundamentais para que passassem a ser feitas as reflexões mais aprofundadas a respeito da ideia de dissuasão (MULLER, 2004). Foi, contudo, a partir da Segunda Guerra Mundial, marcada por um aumento significativo da capacidade destrutiva dos armamentos – especialmente a partir do emprego dos artefatos nucleares estadunidenses em Hiroshima e Nagasaki, no Japão –, que a dissuasão passou a ocupar espaço de destaque nas discussões do campo das Relações Internacionais (MORGAN, 2003).

Nesse contexto, imediatamente após o fim do conflito mundial, autores como Brodie (1946) e Wolfers (1946) passaram a elaborar discussões a respeito das implicações dos armamentos nucleares para a dissuasão. Em linhas gerais, para tais autores, a existência dos

[15] A discussão sobre a ameaça do uso da violência em resposta às ações adversárias aparece na célebre obra de Tucídides sobre Guerra do Peloponeso (THUCYDIDES, 2009).

artefatos nucleares havia alterado fundamentalmente a natureza da guerra, impondo, assim, uma revolução estratégica, uma vez que, se antes o objetivo era vencer os conflitos, com base no então o objetivo passava a ser evitar que eles ocorressem (PUTTEN; MEIJNDERS; ROOD, 2015). Tal transformação resultaria justamente da possibilidade de destruição total representada pelo eventual uso dos artefatos nucleares, bem como da incapacidade de defesa daqueles Estados que não detivessem tais armamentos (BRODIE, 1946; JERVIS, 1979).

A partir da década de 1950, uma nova onda de estudos sobre dissuasão começou a tomar forma. Buscando incorporar maior "rigor científico" e capacidade de abstração às reflexões, diversos autores passaram a incorporar elementos de Teoria dos Jogos às suas discussões, especialmente o chamado "*Chicken game*"[16] (BRANTLY, 2018). Nesse sentido, autores como Brodie (1959), Wholstetter (1959), Schelling (1960; 1966) e Snyder (1961) procuraram demonstrar a importância da noção de racionalidade dos atores para a ideia de dissuasão. A guerra, assim, passava a ser tratada como um processo de barganha, no qual os adversários buscariam, por meio de ameaças, promessas e ações, influenciar as expectativas e intenções uns dos outros. Ela seria, portanto, a arte da coerção, da intimidação e, também, da dissuasão (SCHELLING, 1966).

A despeito de tais contribuições aportadas pelas reflexões dessa segunda onda, muitas foram as críticas ao seu desenvolvimento, o que levou ao surgimento de uma nova onda de estudos que incorporou, entre outros, elementos da psicologia cognitiva e de estudos comportamentais (KARPAVIČIŪTĖ, 2019). Autores como Allison (1971), George e Smoke (1974), Steinbruner (1976), Janis (1982) e Jervis, Lebow e Stein (1985), entre outros, por meio de diferentes perspectivas e abordagens, elaboraram discussões que questionavam não apenas a falta de evidências empíricas e o forte recurso à dedução nas análises de dissuasão, mas também os próprios pressupostos de racionalidade e sua fragilidade nos processos de tomada de decisão. Os estudos elaborados nesse contexto, os quais buscavam maior suporte em evidências empíricas, demonstraram a necessidade de revisão das Teorias de Dissuasão em certos elementos (como definição de riscos, recompensas, probabilidades, erros de percepção e burocracia e política doméstica), procurando desenvolver novas soluções para todos eles (JERVIS, 1979; WALT, 1991).

[16] Trata-se de um jogo simétrico, em que os dois competidores, ao se confrontarem, têm como opções continuar ou desistir. Se nenhum dos dois desistir, ambos perdem tudo. Se apenas um desistir, este sai como o único perdedor – ainda que sem uma derrota total.

Autores como Knopf (2010), Lupovici (2010), Putten, Meijnders e Rood (2015) e Karpavičiūtė (2019)[17] identificam ainda a existência de uma quarta onda de estudos de dissuasão. Enquanto as três primeiras tinham como motivador principal e elemento central das discussões a questão dos armamentos nucleares – e as inúmeras possíveis consequências de sua existência –, a nova linha teria sido estruturada a partir do fim da Guerra Fria, sobretudo diante da noção de emergência de "novas" ameaças, tendo ganhado força especialmente com os atentados de 11 de setembro de 2001 aos Estados Unidos (KNOPF, 2010).

Assim, a nova onda distinguir-se-ia das anteriores principalmente por duas características. Primeiro, por seu enfoque, não mais centrado exclusivamente nos armamentos nucleares e em ameaças tradicionais, mas incorporando discussões a respeito de uma gama muito mais ampla de ameaças, como violência perpetrada por atores não estatais e guerras assimétricas (PUTTEN; MEIJNDERS; ROOD, 2015). Segundo, por seu caráter, que teria natureza interpretativa, dedicando grande relevância para o contexto intersubjetivo da dissuasão, entendido como sendo fundamental para a construção da compreensão dos atores nela envolvidos a respeito de seu significado (LUPOVICI, 2010). Nesse sentido, como destacado por Gray (1990; 1999), a dissuasão estabelecer-se-ia não necessariamente (e tampouco de forma exclusiva) pelas capacidades concretas do Estado dissuasor, mas sim pela percepção do Estado dissuadido a respeito dessa capacidade e de suas implicações.

A despeito da existência de inúmeras (e relevantes) distinções entre as quatro ondas de estudos de dissuasão – especialmente no que diz respeito aos diferentes enfoques por elas adotados –, em linhas gerais é possível identificar a existência de sete componentes que atuam de forma conjunta e inter-relacionada e que são fundamentais para a dissuasão - independente do enfoque adotado (GOODMAN, 2010; WILNER, 2017; McKENZIE, 2017). O primeiro é a existência de um determinado interesse, o qual o agente dissuasor busca proteger. O segundo componente é a declaração dissuasória, que tem por objetivo apresentar, de forma clara, o interesse que o ator busca proteger e as consequências a serem impostas aos demais atores caso ataquem tal interesse – as ações de dissuasão.

[17] Karpavičiūtė (2019) ainda identifica uma quinta onda, que teria início a partir dos anos 2010, centrando-se, a partir da compatibilização de elementos teóricos das quatro primeiras ondas, em discussões sobre dissuasão multidimensional e sobre os impactos tecnológicos e o papel da inteligência artificial na dissuasão. A despeito da segmentação proposta pela autora, para este estudo consideramos que tais discussões, dadas suas naturezas, são pertinentes, ainda, a uma quarta onda de estudos sobre dissuasão.

As ações de dissuasão são o terceiro componente e podem ser de dois tipos: medidas de punição ou de negação. Medidas de punição compõem o aspecto ofensivo da dissuasão, sendo aquelas em que o ator dissuasor ameaça retaliar um eventual agressor caso ele realize uma ação indesejada – ou seja, a tentativa de dissuasão se constrói a partir da ameaça de impor custos ao eventual agressor. Por outro lado, as medidas de negação são o aspecto defensivo da dissuasão e dizem respeito à capacidade de demover um potencial agressor de sua intenção de atacar por meio da redução dos eventuais benefícios a serem conquistados com tal ataque. Esse tipo de dissuasão ocorreria em casos em que o ator dissuasor demonstrasse resiliência – sendo esta entendida como a capacidade de mitigar efeitos de um eventual ataque (dissuasão por prevenção) e/ou de recuperar-se rapidamente após ser atingido (dissuasão por futilidade). Assim, como destaca Wilner (2017, p.310, tradução nossa) "[e]m suma, dissuasão por punição [...] ameaça causar danos, adicionando custos a determinados comportamentos; a dissuasão por negação [...] ameaça o fracasso, subtraindo benefícios de determinado comportamento".

O quarto componente é a credibilidade (entendida como a plausibilidade das eventuais ações de dissuasão, expressas na declaração dissuasória), o quinto é a confiança (a garantia de que não haverá punições caso não haja atentados contra o interesse que está sendo protegido) e o sexto é o medo (do ator dissuadido em relação às ações de dissuasão). Por fim, o sétimo componente é o cálculo de custo-benefício, que envolve todos os componentes anteriores e que, em última instância, é o que determina o comportamento do ator que se busca dissuadir.

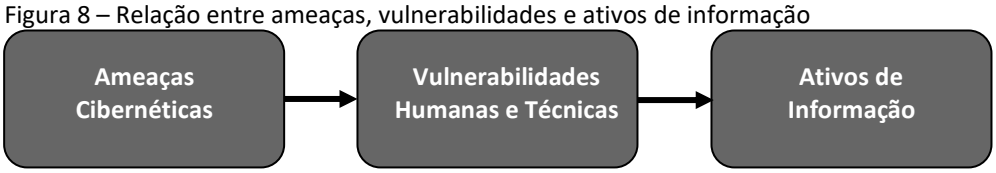
3 Segurança e Defesa Cibernéticas

Para falar de segurança cibernética é necessário conhecer o conceito de segurança da informação, que é definido pela norma internacional ISO/IEC 27000:2018 como a preservação da confidencialidade, integridade e disponibilidade da informação (CID) (ISO, 2018). Diante disso, a informação pode ter muitas formas, armazenada em papel ou meio eletrônico, e podendo ser transmitida através da voz, do papel e eletronicamente pelos meios digitais - como filmes, músicas, entre outros (ISO/IEC 27000:2018). Em uma visão mais ampla, pode-se definir a segurança da informação como uma área do conhecimento que estuda a proteção

dos ativos[18] de informação contra acessos não autorizados, alterações indevidas e sua indisponibilidade. Dessa forma, a área de conhecimento trata de criar regras que devem incidir sobre todo o ciclo de vida de informação (manuseio, armazenamento, transporte e descarte), buscando identificar ameaças, vulnerabilidades e os seus possíveis controles (SÊMOLA, 2014).

As ameaças são agentes ou condições que afetam as informações e seus ativos por meio da exploração de vulnerabilidades, causando a perda dos atributos de confidencialidade, integridade e disponibilidade, e acarretando impactos aos negócios/processos de uma organização. As vulnerabilidades, por outro lado, são fragilidades presentes em ativos de informação que, ao serem exploradas por ameaças, permitem a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação. Vulnerabilidades por si só não provocam incidentes, pois são elementos passivos, ou seja, precisam de um agente causador, que são as ameaças (SÊMOLA, 2014). Um exemplo disso são os erros de codificação ou a configuração incorreta de sistemas, aplicativos ou equipamentos que, consequentemente, podem levar a ameaças, como acessos indevidos e vazamentos de dados, entre outros. A figura abaixo sintetiza as relações existentes entre ameaças, vulnerabilidades e ativos de informação.

Figura 8 – Relação entre ameaças, vulnerabilidades e ativos de informação



Fonte: os autores.

A segurança cibernética se destina à proteção do ciberespaço, e os recursos que mantêm esse ambiente são oriundos de ativos das tecnologias de informação e comunicação (TIC), formados por um ambiente de natureza híbrida – *hardware*[19] e *software* - e interligados por inúmeras redes de computadores. A Associação Brasileira de Normas Técnicas (ABNT) define o ciberespaço como o "[a]mbiente complexo resultante da interação de pessoas, *software* e serviços na *Internet,* suportado por instrumentos físicos de tecnologia da

[18] Considera-se um ativo tudo aquilo que tem valor para um indivíduo, uma organização ou um governo.
[19] *Hardware* é a parte física de um computador, formada por componentes eletrônicos necessários para fazer com que o computador funcione.

informação e comunicação (TIC) e redes conectadas e distribuídas pelo mundo inteiro" (ABNT, 2015, p. 9).

No entanto, quando se fala do ciberespaço, existem questões de segurança não atendidas pela atual segurança da informação, como a de *internet*, a de redes e as melhores práticas recomendadas de segurança de TIC, bem como os vácuos entre esses domínios e a falha de comunicação entre organizações e provedores no ciberespaço. Isso pode ser explicado porque os ativos e as redes conectadas que suportam o ciberespaço possuem diferentes proprietários, cada um com suas convicções de segurança e suas próprias preocupações comerciais, operacionais e legais, fazendo com que cada organização apresente um foco diferente no ciberespaço, e resultando em uma segurança fragmentada para esse ambiente (ABNT, 2015).

Nesse sentido, a proteção dos ativos de TIC é realizada por meio de contramedidas que vão além das propriedades da confidencialidade, integridade e disponibilidade, incorporando outros aspectos, como não repúdio[20], responsabilidade[21], autenticidade[22] e confiabilidade[23] dos ativos de informação e das redes (ISO, 2015). A adoção dessas contramedidas serve para a proteção dos recursos de TIC contra ameaças e vulnerabilidades, sendo procedimentos e mecanismos que podem impedir que ameaças explorem vulnerabilidades e, assim, limitando o impacto ou a probabilidade de sua exploração, acarretem a mitigação do risco ou mesmo evitá-lo (SÊMOLA, 2014). Essas medidas de segurança podem ser preventivas, detectivas e/ou corretivas.

Dessa forma, a segurança cibernética se baseia na segurança da informação, na segurança de *internet* e na segurança de TIC, como blocos de construção fundamentais. A ABNT 27032 define a segurança cibernética como a preservação da confidencialidade, integridade e disponibilidade das informações no Espaço Cibernético (ABNT, 2015). No entanto a mesma definição considera que a proteção do ciberespaço deve levar em conta aspectos físicos, sociais, financeiros, políticos, emocionais, profissionais, psicológicos, educacionais ou outros tipos ou consequências de falhas, danos, erros, acidentes, prejuízos

[20] Não repúdio, também chamado de irretratabilidade, é o princípio de jamais ser possível ocultar o autor de uma ação no ciberespaço, como no caso do envio de um e-mail com assinatura digital, por exemplo.
[21] Responsabilidade, definição das obrigações usuários, administradores de sistemas, redes e banco de dados em relação à propriedade dos ativos de informação.
[22] Autenticidade, propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.
[23] Confiabilidade é a propriedade que garante a informação fidedigna.

ou quaisquer eventos considerados indesejáveis nesse ambiente (ABNT, 2015). Os desafios da segurança cibernética ultrapassam a proteção das informações e de seus ativos. Suas ações visam proteger a sociedade, os governos e as empresas dos novos desafios do ciberespaço, tais como: o *cyberbullying*[24], a espionagem cibernética, o ciberterrorismo, a proteção das infraestruturas críticas e o ataque cibernético entre países (VON SOLMS; VAN NIEKERK, 2013).

Nesse contexto, no cenário da exploração espacial, a ameaça cibernética recebe destaque nas estratégias para o espaço de alguns países e em publicações como o relatório *Global Counterspace Capabilities: an open source assessment* (SAMSON; WEEDEN, 2020), que avalia como os países implementam suas infraestruturas (tipos de satélites, bases de controle etc.), bem como os riscos envolvidos. Essa preocupação decorre do receio (e à expectativa) de que vulnerabilidades em *softwares* comerciais, utilizados em sistemas espaciais, possam ser explorados por Estados ou atores não estatais para roubar dados ou causar danos em satélites e bases de controle.

Assim, sabe-se que os ativos de informação precisam ser protegidos porque apresentam vulnerabilidades que podem ser exploradas por ameaças. Entretanto a segurança cibernética tem uma dimensão que vai além da preservação dos atributos da segurança da informação (CID), podendo, também, apresentar uma dimensão ética. É o caso do problema do *cyberbullying*, que precisa ser enfrentado pela sociedade, mas cujos desafios vão além das questões técnicas. Outro caso relevante é o roubo de ciclos de processamento de um computador para uso em *botnets*.[25] Ainda que não comprometa os atributos da CID, caso tal *botnet* seja usada para cometer um crime, o proprietário do computador em questão pode ser um cúmplice desconhecido.

Esses exemplos mostram como são heterogêneas as ameaças do ciberespaço. Devido a isso, alguns países, como Austrália, Colômbia, Espanha e Estados Unidos desenvolveram estratégias de segurança cibernética, alinhadas a suas estratégias nacionais de segurança, para promoverem a proteção da privacidade, da sociedade, dos negócios, da propriedade intelectual e das suas infraestruturas críticas. Essas estratégias propõem uma série de ações, como conscientização da população, educação de profissionais, políticas de desenvolvimento

[24] Cyberbullying é a violência praticada através da internet ou de outras tecnologias relacionadas ao mundo virtual, com o objetivo de agredir, perseguir, ridicularizar e/ou assediar.

[25] Botnet é uma rede de computadores que foram infectados por *softwares* maliciosos e podem ser controlados remotamente, obrigando-os a enviar *spam*, espalhar vírus ou executar ataques de negação de serviço (*Denial of Service - DDoS*) sem o conhecimento ou o consentimento dos seus donos.

de uma indústria *ciber* e o estabelecimento de órgãos responsáveis - em suma, estabelecem os objetivos para que uma nação tenha um ciberespaço mais seguro.

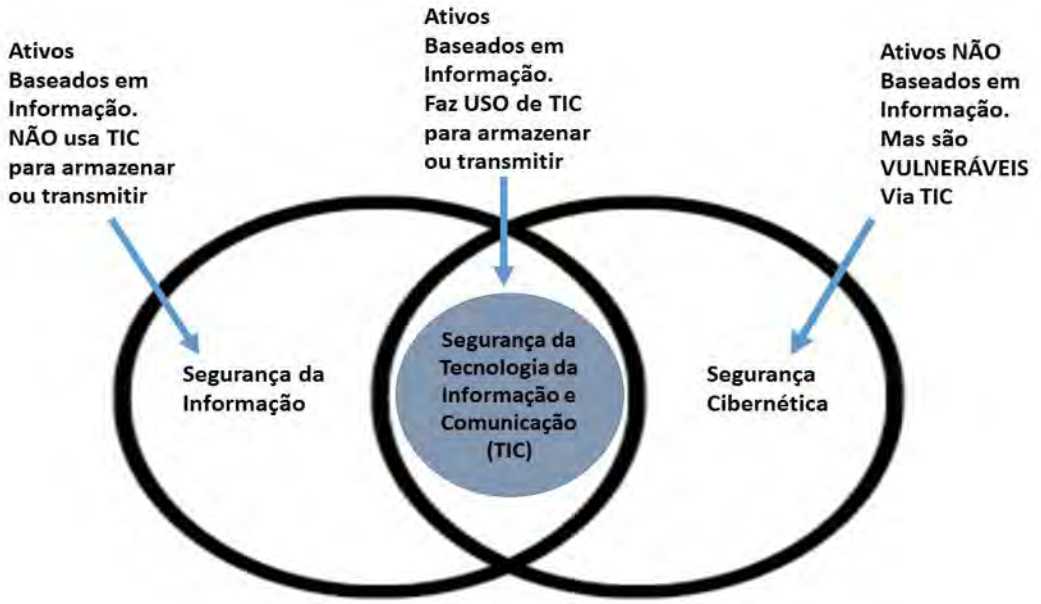
Isso posto, torna-se difícil enquadrar as ações de interrupção, sabotagem e crime cibernético na mesma categoria de ações previstas em uma estratégia de segurança cibernética, como o que ocorreu contra a Estônia, por exemplo. Essas ações ofensivas recaem sobre a responsabilidade das forças armadas, compreendendo, assim, a defesa cibernética. A Doutrina Militar de Defesa Cibernética (DMDC) do Brasil a define assim:

> Conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente (BRASIL, 2014, p. 18).

Segundo Villa e Reis (2006), o conceito de segurança cibernética está mais ligado a questões defensivas, fazendo referência ao combate e à prevenção dos chamados crimes cibernéticos na esfera pública - ou seja, no nível político. Já as ações defensivas, ofensivas e exploratórias, realizadas no ciberespaço dentro de um contexto de planejamento militar, são coordenadas por um órgão militar. Assim, considerando-se os aspectos táticos e operacionais do ciberespaço, são as forças armadas que têm a responsabilidade de aplicar a estratégia, com a finalidade de prevenirem ou responderem em caso de ataques cibernéticos contra a soberania nacional. Muitos países já possuem sua força ciber formalizada, como o Brasil (CDCiber) e os Estados Unidos (USCYBERCOM).

Por fim, com base no tipo de ativo e na necessidade do uso, ou não, de TIC, é possível dizer que a segurança da informação é baseada em qualquer tipo de ativo de informação, não precisando, necessariamente, estar armazenado em ativos de TIC. No caso da segurança de TIC, os ativos de informação são baseados em TIC para transmissão e armazenamento (computadores, redes, *pendrives*, *smartphones* etc.). Na segurança cibernética, por outro lado, os ativos não precisam ser baseados em informação, sendo, contudo, vulneráveis por recursos de TIC (pessoas, infraestruturas críticas, etc). A figura abaixo demonstra, de forma sintetizada, a interseção e/ou correlação da segurança da informação com a segurança de TIC e a segurança cibernética, e suas dependências em relação aos ativos de informação.

Figura 9 – Correlação entre Segurança da Informação, Segurança de TIC e Segurança Cibernética



Fonte: VON SOLMS; VAN NIEKERK, 2013, p. 101 (com adaptações)

4 Aplicação do conceito de dissuasão no âmbito da Segurança Cibernética

A dissuasão, conforme apresentado anteriormente, em sua essência, significa convencer um oponente a não iniciar uma ação específica, porque os benefícios percebidos não justificam os custos e riscos potenciais. Embora seu livro *The Theory and Practice of Conventional Deterrence* tivesse como foco de estudo a prevenção da guerra, Mearsheimer (1981) aponta que não apenas considerações militares contribuem para a dissuasão, mas também outros elementos, como as ações de aliados, o direito internacional e fatores econômicos, exercem uma influência sobre uma nação que pretende empreender uma ação militar.

Em seu livro *Cyberdeterrence and Cyberwar*, Libicki (2009) descreve as opções de dissuasão por negação (capacidade de resistir aos/frustrar os ataques) e dissuasão por punição (a ameaça de retaliar). Com base nessas nomenclaturas, o autor estabelece uma distinção, do ponto de vista cibernético, entre dissuasão cibernética passiva (negação) e ativa (punição). A dissuasão passiva é responsável por implementar as ações de segurança da informação e de segurança de TIC para desenvolver sistemas seguros e, também, para construir redes resilientes que minimizem os riscos e efeitos de um ataque. Na dissuasão ativa existe a ameaça de retaliação ou algum tipo de resposta indesejável, que pode, em nível de beligerância, ir desde negociações diplomáticas até um ataque cinético e força nuclear, passando por sanções econômicas e contra-ataques cibernéticos.

Quando o Irã sofreu o ataque do vírus Stuxnet, que destruiu suas centrífugas nucleares, especialistas em segurança acreditaram que os Estados Unidos poderiam estar envolvidos, dada a complexidade do ataque (CLARKE; KNAKE, 2011). Esse ataque poderia ser considerado um caso de dissuasão preventiva punitiva dos EUA contra o Irã, uma vez que o país continuava com seus procedimentos de enriquecimento de urânio (IASIELLO, 2014).

Já para Nye (2016), existem quatro métodos de dissuasão para reduzir e prevenir ações adversas no ciberespaço: punição, negação, emaranhamento[26] e tabus normativos. Em relação à punição, Nye ratifica o que Libicki afirma sobre esse tipo de dissuasão. No caso da negação, assevera que, no caso dos Estados Unidos, esse tipo de dissuasão é o que concentra os maiores esforços estratégicos do Pentágono. Em suma, boas defesas cibernéticas podem construir resiliência e boa capacidade de recuperação, e o aumento dos custos pode reduzir o incentivo para alguns ataques potenciais, principalmente daqueles usuários ou grupos que não são tão sofisticados.

Ancorado na definição de Snyder (1960), que teoriza a dissuasão como um conceito mais amplo e que não precisa contar apenas com a força militar (ou seja, um agressor pode ser inibido pela própria consciência ou, provavelmente, pela perspectiva de perder posição política em relação a outros países), Nye (2016) introduz os mecanismos de dissuasão por emaranhamento e tabus normativos, divergindo da ideia central da adoção da punição e negação como temas centrais para a concepção clássica de dissuasão.

A dissuasão por emaranhamento tem semelhanças com a noção da corrente liberal de Relações Internacionais de que a interdependência e o comércio seriam desincentivos ao conflito. Aqui, o interesse mútuo está no cerne desse conceito. Entretanto expande-se para incluir outros métodos que incentivem a contenção entre os atores, motivando um comportamento responsável dos países por meio de normas e princípios. Assim, Estados com amplas relações econômicas, diplomáticas e estratégicas devem calcular até que ponto o comportamento agressivo no ciberespaço poderia afetar potencialmente outros aspectos de suas relações (NYE, 2016).

A noção de dissuasão por tabus normativos foi introduzida por Joseph Nye e acabou, sucessivamente, sendo adotada por outros pesquisadores. Segundo Nye (2016), as normas são como um padrão de comportamento apropriado sobre como uma classe de atores deve

[26] O termo original, em inglês, é *entanglement*.

agir, ao longo do tempo, quando fornecem ordem, estabilidade e segurança, podendo ser codificadas como leis. Já os tabus são semelhantes às normas, no entanto têm uma conotação negativa e invertida, pois se referem às formas inapropriadas de agir ou a costumes culturais que são "fora dos limites". Um exemplo desse tipo de dissuasão foi o acordo, em 2015, entre Estados Unidos e China sobre abster-se de espionagem industrial ou de roubo de propriedade intelectual patrocinada pelo Estado. Isso ocorreu depois que *hackers* chineses roubaram 4 milhões de dados pessoais do *Office of Personnel Management* (OPM), órgão que faz a gestão dos funcionários públicos civis do governo estadunidense. Como resultado, com base no consenso sino-americano, estabeleceu-se um forte precedente para que outros países, particularmente as grandes e médias potências, não sejam vistos como indo de encontro à convenção estabelecida por um aliado ou adversário mais poderoso.

Cornish (2010), por sua vez, propôs o conceito de dissuasão por associação. Tal conceito é descrito como um mecanismo político para modificar o comportamento de um adversário, seja ele um Estado ou um outro ator, por ligação de suas atividades predatórias no ciberespaço com sua identidade real. Ao tornar possível identificar e constranger um adversário, exibindo seu comportamento "inapropriado", esse conceito de dissuasão reapresenta a dissuasão por punição, mas agora com um custo social para os Estados, que pode assumir muitas formas, seja pela perda de credibilidade na comunidade internacional, por danos à reputação para as suas empresas ou por ser ostracizado por países de sua comunidade/região.

4.1 Desafios da dissuasão cibernética

Em linhas gerais, podemos identificar três desafios principais à dissuasão cibernética. O primeiro é a noção de atribuição. Em 2010, o secretário-adjunto de Defesa, William Lynn, escreveu que "[e]nquanto um míssil vem com um endereço de retorno, um vírus de computador geralmente não" (LYNN, 2010, p. 99, tradução nossa). Isso posto, pode-se dizer que a atribuição é um dos maiores desafios da dissuasão cibernética, especialmente devido à dificuldade forense para identificar um atacante, o que pode demorar meses ou até mesmo não ser possível. Tal dinâmica é significativamente diferente da atribuição nuclear, uma vez, que em um contexto em que apenas nove países possuem armamentos de tal natureza, há mais recursos para identificar os materiais necessários para fabricar uma arma, além de

existirem diversas barreiras contra aqueles (atores não estatais) que desejam apropriar-se de armas e materiais nucleares (NYE, 2016).

No ciberespaço, tal realidade não se reproduz, pois linhas de código-fonte malicioso podem ser desenvolvidas por qualquer pessoa em seu computador ou mesmo compradas na *dark web*[27] por atores estatais ou não estatais. Determinar a atribuição no ciberespaço é extremamente difícil, pois os atacantes têm uma infinidade de técnicas de ofuscação para impedir que sejam identificados corretamente ou que identifiquem seu verdadeiro ponto de origem, seja pelo comprometimento de uma série de computadores em diferentes países para executar ataques (*botnets*), ou utilizando *proxies*[28] e anonimizadores (IASIELLO, 2014).

A atribuição é um componente necessário de qualquer estratégia de dissuasão, pois cabe ao Estado defensor atribuir positivamente um agressor antes do início de qualquer ação retaliatória. No meio militar convencional também existem dificuldades de atribuição. Em trecho do livro *Fleet Tactics and Coastal Combat* sobre o combate costeiro, Hughes e Girrier (2018, tradução nossa) destacam a confusão provocada por comunicações cruzadas nos oceanos. Segundo os autores,

> [a]s águas litorâneas podem ser definidas de forma útil como onde a confusão de comércio costeiro amigo, inimigo e neutro, barcos de pesca, plataformas de petróleo, pequenas ilhas, tráfego aéreo denso, grandes navios comerciais e um intrincado emaranhado de emissões eletrônicas criam um ambiente confuso no qual um ataque furtivo pode ocorrer de repente e quase sem aviso.

No entanto, nesse contexto do ciberespaço, Healey (2012) construiu uma ferramenta que chamou de "espectro da responsabilidade estatal", que tem como objetivo auxiliar analistas com pouco conhecimento a atribuir responsabilidades por um ataque específico ou campanha de ataques, com certa precisão e transparência. O espectro tem dez categorias e cada uma estabelece um grau diferente de responsabilidade, com base na avaliação da relação de uma nação com um ataque (se ela o ignora, apoia ou conduz). A análise do Estado-nação realizada pela ferramenta produz como resposta um nível de culpabilidade que serve como guia para o tipo e o nível de resposta adequado, que pode ir desde ignorar o ataque até revidar o agressor percebido.

[27] A *Dark Web* é uma pequena parcela da *Deep Web* composta por *sites* e redes não indexados por mecanismos de busca (como o Google) voltados, quase em sua totalidade, à prática de crimes como tráfico de drogas, exploração infantil, serviços de assassinos de aluguel, compartilhamento de imagens de pessoas sendo torturadas, etc.

[28] *Proxy* é o termo utilizado para definir os intermediários entre o usuário e seu servidor.

Uma prática de atribuição bem-sucedida no ciberespaço reúne análises técnicas, cognitivas, de inteligência e comportamentais para melhor identificar os atacantes, bem como as influências que podem estar orientando suas operações. A análise técnica não é suficiente para fins de atribuição, pois os atores hostis implementam as mesmas ferramentas, táticas, técnicas e procedimentos. Vários problemas inibem processos de atribuição rápidos e precisos, incluindo o tempo necessário para coletar e analisar o método de ataque empregado e a identificação de motivos, comportamentos e influências externas do ator. No entanto, a fim de evitar constrangimentos públicos e reduzir o volume e a probabilidade de danos colaterais, um nível aceitável de atribuição deve ser realizado antes do início de qualquer ação retaliatória (MCKENZIE, 2017).

O segundo desafio para a dissuasão cibernética é a comunicação. No livro *Arms and Influence*, Schelling (1966) observa que uma dissuasão bem-sucedida, com métodos de punição e negação, depende da comunicação efetiva entre um Estado e o ator que deseja dissuadir. Ou seja, deve ser capaz de comunicar efetivamente à comunidade internacional e, em particular, aos adversários o que é ou não aceitável e quais serão as consequências caso esse limite seja ultrapassado. Assim, um Estado deve não apenas se pronunciar sobre as atividades que considera que transgridem os limites por ele estabelecidos, mas também estar preparado para agir em resposta a tais ações, sob risco de perder (ou fragilizar) sua credibilidade caso não o faça.

Nesse sentido, a comunicação no ciberespaço assume uma função importante, exigindo esforço para obter-se consenso para as normas de comportamento nesse ambiente. Tentando identificar uma linguagem comum, em 2013, os Estados Unidos estabeleceram com a China o chamado Diálogo Estratégico e Econômico, para tratar de uma agenda sobre diversos assuntos de economia e segurança e, inclusive, de questões sobre ataques cibernéticos chineses contra empresas americanas. Nesse campo, entretanto, os diálogos não evoluíram significativamente, sobretudo devido à forma de cada nação abordar o tema. Enquanto os Estados Unidos preferem o termo segurança cibernética para análise dos ativos e ameaças, a China utiliza o termo segurança da informação que, como visto anteriormente, é mais amplo (GERTZ, 2013). Sem um léxico comum entre ambos, as probabilidades de que a comunicação permaneça em desacordo são expressivas, dificultando que haja um consenso entre ambos sobre como a internet deve ser usada adequadamente.

Outra forma de buscar-se atingir um acordo sobre normas foi a Convenção Europeia sobre Crimes Cibernéticos de 2001, que fornece um bom quadro de terminologias sobre crimes no ciberespaço. Até o momento, houve sessenta e duas adesões à convenção. A China não se juntou à convenção, relatando sua relutância em aceitar uma terminologia acordada pelos Estados Ocidentais (GILES; HAGESTAD, 2013; COUNCIL OF EUROPE, 2014).

O terceiro desafio à dissuasão cibernética é a proporcionalidade que, baseada nos princípios expressos nas Convenções de Genebra, de 1949, sobre conflito armado, bem como no Manual de Tallinn (SCHMITT, 2016), defende a assimilação da guerra cibernética na guerra convencional. Nesse sentido, é estabelecido que uma ação no ciberespaço precisa ser proporcional, principalmente quando essas ações são supostamente provocadas pelos próprios Estados ou por atores patrocinados por eles - ou seja, deve ser comparável e não provocar uma escalada (JENSEN, 2012). Por uma série de razões, contudo, é difícil alcançar a proporcionalidade no ciberespaço - isso porque qualquer resposta deve refletir a quantidade (proporcional) do dano causado a um alvo que foi atingido. Portanto, antes da retaliação, que pode ser cinética ou não, um Estado deve avaliar os riscos diplomáticos e econômicos de sua resposta, e todas as suas consequências projetadas, como avaliações de danos de batalha e possíveis efeitos políticos (IASIELLO, 2014).

Além dos desafios descritos, também devem ser considerados os desafios e as possibilidades dos sete componentes inerentes à dissuasão apresentados anteriormente. No quadro apresentado na próxima seção, sintetiza-se a adequação desses componentes à noção de dissuasão cibernética, bem como os eventuais desafios à sua aplicação. Os sete componentes elencados se mostram compatíveis com a ideia de dissuasão cibernética.

No que diz respeito à apresentação, pelos atores, de um interesse específico a ser protegido, não há qualquer diferença em relação a outras formas de dissuasão - porquanto a tendência seja de que haja uma grande quantidade de interesses simultâneos, dada a existência, no âmbito cibernético, de um número expressivo de ativos que podem, potencialmente, ser alvos de ataques.

O segundo componente, a declaração dissuasória no âmbito cibernético, por sua vez, consubstancia-se, em linhas gerais, nas estratégias de segurança cibernética dos países, as quais expressam os limites e as possíveis ações retaliatórias em casos de ataque.

O terceiro componente, as ações de dissuasão, ainda que operem em lógica semelhante a qualquer outra forma de dissuasão, apresentam diferenças no que diz respeito

às estratégias punitivas e de negação no âmbito cibernético, devido às dificuldades de identificar os agressores e na proporcionalidade da resposta.

O quarto componente, a credibilidade, por sua vez, apresenta peculiaridades relevantes no âmbito cibernético, uma vez que, diferente da dissuasão em outros contextos, a demonstração de capacidades – sistemas e equipamentos – pode mais do que evidenciar a credibilidade das eventuais ameaças, expor eventuais vulnerabilidades do dissuasor.

O quinto componente, a confiança, que trata da punição somente quando o país tiver seus interesses violados, também se expressa de forma distinta no âmbito do ciberespaço, visto que os ataques são furtivos e podem ser disparados por atores estatais ou não estatais, o que pode contribuir para que uma agressão possa levar a uma escalada de ataques cibernéticos como resposta.

Em relação ao medo, percebe-se que, no contexto do ciberespaço, ele se caracteriza não necessariamente pelo receio de uma eventual retaliação cinética, mas sobretudo pelo temor de consequências com um maior custo social, atingindo os países em seus laços comerciais e diplomáticos e, consequentemente, impactando também os atores não estatais.

Por fim, o sétimo componente, o cálculo de custo-benefício, que está na essência da eficácia da dissuasão, é realizado por todos os atores (sejam eles estatais, ou não) na consideração da viabilidade (e dos potenciais ganhos auferidos com) eventuais ataques, cibernéticos ou não.

5 A dissuasão e os desafios da Defesa Cibernética na projeção espacial brasileira

Segundo relatório da *Secure World Fundation* (2020), países como Estados Unidos, China e Rússia têm buscado implementar capacidades militares em seus programas espaciais para degradarem ou negarem as capacidades dos seus adversários. Atualmente, já seriam capazes de coletar informações em satélites estrangeiros, ter o poder de bloquear sinais de GPS (inclusive de serviços civis de localização global), bem como realizar a defesa de mísseis no espaço.

Nesse contexto, vários países detêm capacidades cibernéticas que poderiam ser usadas contra sistemas espaciais, ao passo que um número crescente de atores não estatais está sondando ativamente sistemas de satélites comerciais e descobrindo que existem vulnerabilidades cibernéticas semelhantes às encontradas em sistemas de computação convencional (SAMSON; WEEDEN, 2020).

Quadro 7 – Aplicações e desafios dos componentes da dissuasão convencional na dissuasão cibernética

Componente	Adequação	Observações
Interesse	Apresenta desafios	Em suas estratégias, os Estados definem a prioridade de proteção para seus ativos mais críticos, o que se torna difícil no ciberespaço, pois esse ambiente permite que muitos ativos possam ser alvos de ataque.
Declaração dissuasória	Aplicável	Representada pelas estratégias de segurança cibernética dos países, onde expressam os limites e ações retaliatórias em casos de ataque.
Ações de dissuasão	Apresenta desafios	Enquanto a punição sofre com os problemas de atribuição e proporcionalidade, a negação apresenta as maiores chances de sucesso na dissuasão cibernética.
Credibilidade	Apresenta desafios	As ações de dissuasão precisam ser comunicadas à comunidade internacional, particularmente aos adversários, sobre os limites aceitáveis, assim a credibilidade age em conjunto com a comunicação.
Confiança	Apresenta desafios	Os diversos casos de ataques cibernéticos relatados, bem como os casos de espionagem cibernética, revelam que ainda não é possível garantir que não haverá punições se um interesse/ativo for desrespeitado no ciberespaço.
Medo	Apresenta desafios	Os Estados, devido aos custos sociais, estão suscetíveis ao medo, por conseguinte, pode atingir os atores não estatais que precisam do patrocínio de Estados.
Custo-benefício	Aplicável	O interesse mútuo e a interdependência no comércio são importantes para países com múltiplos laços comerciais e políticos, podendo não afetar aqueles com poucos laços no cenário internacional.

Fonte: Os autores.

Essa dependência de sistemas comerciais, relativamente inseguros, em sistemas espaciais, possibilita que atores não estatais tenham capacidade para realizar ações no ambiente espacial sem a necessidade da assistência do Estado. Embora essa questão mereça atenção e, provavelmente, cresça em relevância nos próximos anos, ainda existe uma grande diferença entre as capacidades de ataques cibernéticos dos principais países e dos demais atores (SAMSON; WEEDEN, 2020).

Os conceitos de dissuasão por negação são importantes, nesse sentido, porque promovem a resiliência de toda a infraestrutura técnica do projeto espacial do Brasil. Nesse sentido, parece-nos fundamental ao projeto desenvolver um rigoroso processo de avaliação de riscos e de gestão de vulnerabilidades, envolvendo processos, ativos de informação e cadeias de suprimentos e de fornecedores. Medidas de segurança de perímetro tradicionais, como controle de acesso às instalações e aos ativos de informação, fortalecimento do monitoramento, inspeção de pacotes, segregação de redes, entre outras, devem ser

implementadas. Além disso, considerando que é mais fácil atacar que defender no domínio cibernético (RYAN, 2017), mostra-se fundamental a adoção de medidas que contribuam para o constante incremento da sofisticação no monitoramento e inspeção de pacotes por meio de técnicas de inteligência artificial, com o objetivo de garantir o constante aprimoramento das capacidades defensivas do projeto.

Com o intuito de criar medidas que contemplem a dissuasão por associação e emaranhamento, que, basicamente, focam na visão de um Estado com "boa conduta" no ciberespaço, em que suas ações respeitam as normas estabelecidas entre os países, reveste-se de importância a criação de uma estratégia de defesa para o espaço nos moldes do Livro Branco de Defesa Nacional, de forma a demonstrar à comunidade internacional os interesses e compromissos do Brasil na exploração do espaço.

Além disso, seria promissor, no contexto da proteção do ciberespaço, a participação do Brasil como signatário da Convenção Europeia[29] de Crimes Cibernéticos de 2001, com o intuito de demonstrar alinhamento às demais nações sobre o tratamento desse tipo de crime. Por fim, embora a dissuasão por punição ainda possa representar um desafio, o uso de medidas de custo social - como a exposição dos atores maliciosos na comunidade internacional - e o uso de ações diplomáticas e econômicas em caso de ataques cibernéticos disparados contra seus ativos do projeto espacial (satélites, radares, bases de controle), apresenta-se, igualmente, como uma importante estratégia a ser seguida.

6 Considerações finais

O ciberespaço tem-se tornado cada vez mais necessário à vida das sociedades, ocupando espaço nas comunicações, nos negócios, nos estudos, no entretenimento, nos serviços de governo digital e no controle de infraestruturas críticas. Devido aos múltiplos ataques cibernéticos disparados contra organizações civis ou militares, sua proteção passou, nesse contexto, a ser estratégica. Na busca de alternativas para tal questão, este trabalho apresentou uma análise do conceito da dissuasão cibernética, demonstrando que ele pode ser aplicado nas estratégias de segurança e defesa cibernética das nações. Embora esse conceito encontre similaridade com a teoria da dissuasão convencional, sendo composto por

[29] Em julho de 2019, o Brasil foi convidado a aderir à Convenção de Budapeste, tendo iniciado os trâmites para formalizar sua adesão (BRASIL, 2020).

elementos como punição, negação, atribuição e comunicação – os quais estruturam o modelo convencional –, precisa de algumas adaptações para garantir sua efetividade.

O conceito de dissuasão cibernética por negação é o que mais apresenta chances de sucesso, pois se adapta melhor às necessidades de segurança cibernética por meio da construção de defesas eficientes que possam tornar os sistemas menos vulneráveis e as redes mais resilientes. No entanto exige a integração de capacidades e tecnologias inovadoras para monitoramento de novas ameaças, como o uso de inteligência artificial, por exemplo. Ao exigir maiores recursos e tempo dos atacantes, a negação no ciberespaço estabelece o modelo de custo-benefício que desestimula um atacante. Uma boa defesa cibernética pode eliminar a maioria dos ataques potenciais de atacantes não sofisticados e de atores não estatais, contudo ela pode não ser suficiente para deter ameaças avançadas persistentes[30] (APT), disparadas por Estados e inteligências governamentais, pois estas são elaboradas de forma específica para um determinado alvo.

A atribuição rápida e eficaz de um atacante, bem como a proporcionalidade de uma resposta, constituem grandes desafios para a dissuasão cibernética. Consequentemente, isso diminui a possibilidade da dissuasão cibernética por punição por Estados - ou seja, a punição no ciberespaço acaba tendo um papel menos estratégico que no caso das armas nucleares. Entretanto as diferenças nos instrumentos clássicos de punição e de negação no ciberespaço abrem espaço para as formas de dissuasão cibernética de emaranhamento, de associação e de tabus normativos que se utilizam do custo social como punição aos adversários.

A dissuasão cibernética por emaranhamento utiliza o interesse mútuo e a interdependência no comércio para construir esse conceito, todavia o cálculo de custo-benefício pode ser importante para um país com múltiplos laços comerciais e políticos, mas, provavelmente, não afete um país que tenha laços políticos e, sobretudo, comerciais mais limitados. O emaranhamento pode, também, afetar atores não estatais, pois, ainda que desvinculados dos Estados, alguns precisam do seu patrocínio para desenvolver suas ações. Na dissuasão cibernética por associação, a punição assume um custo social ao apresentar as

[30] Um Ataque Persistente Avançado usa técnicas de invasão contínuas, clandestinas e sofisticadas para obter acesso a um sistema e permanecer dentro dele por um período prolongado, com consequências potencialmente destrutivas. Geralmente são direcionadas a alvos de grande valor, como países e grandes corporações, com o objetivo final de roubar informações durante um longo período, em vez de simplesmente adentrar e sair rapidamente, como muitos hackers mal-intencionados fazem durante ataques cibernéticos de nível inferior (KASPERSKY, 2018).

ações negativas de um Estado ou outro ator no ciberespaço, causando a estes a perda de credibilidade no cenário internacional. Na dissuasão por tabus normativos, as grandes potências estabelecem comportamentos entre si, que, pela importância dos objetivos e das ações firmadas, acabam chegando aos seus aliados e adversários como se fossem normas a serem seguidas.

Essas formas de dissuasão cibernética ocorrem de maneiras relativamente diferentes, mas todas buscam punir e coibir os comportamentos criminosos no ciberespaço. Assim, é importante que as nações construam estratégias de segurança e defesa cibernéticas que estabeleçam, de forma clara, seus limites e quais serão suas ações retaliatórias (cinéticas, não cinéticas, diplomáticas e econômicas) caso sejam alvo de ataques. Essa postura dos Estados não deve apenas estar focada nas ações de revide aos adversários, pois necessita, também, de que as nações avaliem, de forma constante, suas posturas de segurança no atual ciberespaço, bem como suas formas de produzir conhecimento, experiência e aprimoramento de suas táticas, técnicas e procedimentos para a gestão da segurança e defesa cibernética.

Diante do exposto e dada, atualmente, a maior possibilidade de um ataque cibernético frente a um ataque físico contra satélites, por exemplo, conclui-se, pelo exposto neste trabalho, que a segurança cibernética não é uma solução estática - ou seja, precisa evoluir constantemente à medida que os atacantes ganham mais conhecimento, experiência e que suas táticas, técnicas e procedimentos se transformem ao longo do tempo.

Assim, estratégias de segurança que funcionam hoje poderão não ter o mesmo sucesso no futuro (mesmo que próximo), devido ao cenário de rápidas mudanças inerente à questão. Sendo assim, as organizações responsáveis por esses ativos precisam implementar estratégias de segurança cibernética que estabeleçam rígidos programas de atualização de *softwares* e correção de vulnerabilidades, periódicos testes de invasão, conscientização em segurança e o estabelecimento de um firme programa de padrões e controles de segurança a ser seguido por toda a organização, que incluam marcos e medidas de desempenho para garantir que metas sejam cumpridas.

Como medidas mais estratégicas, este trabalho sugere que os países que desenvolverem estratégias de segurança no espaço, integradas às demais estratégias que a nação adote, tornem claros e evidentes para seus parceiros e para a comunidade internacional seus planos de exploração no espaço. Assim sendo, parece-nos que, a despeito de apresentar limitações, desafios e particularidades em relação ao modelo convencional, a dissuasão

cibernética tem um relevante papel no âmbito da segurança cibernética atual. Suas contribuições podem auxiliar, por conseguinte, os tomadores de decisão da defesa nacional, pois vão desde a preocupação com segurança da informação, em todas as fases de projeto e sua operacionalização, até a necessidade de formulação de respostas para os casos de ataques cibernéticos, sejam elas em todas as formas.

Referências

ABNT. *ABNT NBR ISO/IEC 27032. Tecnologia da Informação - Técnicas de segurança - Diretrizes para segurança cibernética*. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2015.

AKOTO, William. Hackers could shut down satellites – or turn them into weapons. *The Conversation*, [*s. l.*], 2020. Disponível em: https://theconversation.com/hackers-could-shut-down-satellites-or-turn-them-into-weapons-130932. Acesso em: 28 out. 2020.

ALLISON, Graham T. *Essence of decision*: explaining the Cuban missile crisis. Boston: Little, Brown, 1971.

BRANTLY, Aaron. The Cyber Deterrence Problem. *In*: MINÁRIK, T; JAKSCHIS, R; LINDSTRÖM, L (org.). *2018 10th International Conference on Cyber Conflict CyCon X: Maximising Effects*. Tallinn: Nato Cooperative Cyber Defence Centre Of Excellence, 2018. p. 31-54.

BRASIL. *Doutrina Militar de Defesa Cibernética*. Brasília: Ministério da Defesa, 2014. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf. Acesso em: 27 out. 2020.

BRASIL. *Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública*. [*S. l.*], 2020. Disponível em: http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica. Acesso em: 2 nov. 2020.

BRODIE, Bernard. *Strategy in the Missile Age*. Santa Monica: Rand, 1959.

BRODIE, Bernard (org.). *The Absolute Weapon: Atomic Power and World Order*. New York: Harcourt, Brace and Co, 1946.

CLARKE, Richard A; KNAKE, Robert K. *Cyber War*: the next threat to national security and what to do about it. Nova Iorque: HarperCollins, 2011.

CORNISH, Paul. Arms control tomorrow: the challenge of nuclear weapons in the twenty-first century. *In*: NIBLETT, Robin. *America and a Changed World*: A Question of Leadership. London: The Royal Institute of International Affairs, 2010. cap. 12, p. 223-237.

COUNCIL OF EUROPE. *Convention on Cybercrime*. [*S. l.*], 2014. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures. Acesso em: 31 out. 2020.

DHILLON, Gurpreet. *Principles of information systems security*: text and cases. Hoboken: Wiley, 2007.

DOFFMAN, Zak. *Israel responds to cyber attack with air strike on cyber attackers in world first*. [*S. l.*], 2019. Disponível em: https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/?sh=6a5bfcc7afb5. Acesso em: 2 nov. 2020.

FERRAÇO, Ricardo. *CPI DA ESPIONAGEM RELATÓRIO FINAL*. [Brasília, DF*:* Senado Federal], 2014. Disponível em: https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco. Acesso em: 23 set. 2020.

G1 ECONOMIA. *Ataque hacker lançado da China invadiu satélites e empresas de defesa dos EUA, diz Symantec*. [*S. l.*], 2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/ataque-hacker-lancado-da-china-invadiu-satelites-e-empresas-de-defesa-dos-eua-diz-symantec.ghtml. Acesso em: 28 out. 2020.

GEORGE, Alexander L; SMOKE, Richard. *Deterrence in American foreign policy: theory and practice*. New York: Columbia University Press, 1974.

GERTZ, Bill. *U.S., China Conclude Strategic and Economic Dialogue Talks*. [*S. l.*], 2013. Disponível em: https://freebeacon.com/national-security/u-s-china-conclude-strategic-and-economic-dialogue-talks/. Acesso em: 31 out. 2020.

GILES, K.; HAGESTAD, W. *Divided by a common language: Cyber definitions in Chinese, Russian and English*. [*S. l.*], 2013. Disponível em: https://ieeexplore.ieee.org/abstract/document/6568390. Acesso em: 4 nov. 2020.

GOODMAN, Will. Cyber Deterrence: Tougher in Theory than in Practice? *Strategic Studies Quarterly*, [*s. l.*], v. 4, n. 3, p. 102–135, 2010.

GRAY, Colin S. The definitions and assumptions of deterrence: Questions of theory and practice. *Journal of Strategic Studies*, [*s. l.*], v. 13, n. 4, p. 1-18, 1990.

GRAY, Colin S. *The second nuclear age*. Boulder: Lynne Rienner, 1999.

HEALEY, Jason. *Beyond Attribution: Seeking National Responsibility in Cyberspace*. [*S. l.*], 2012. Disponível em: https://www.atlanticcouncil.org/in-depth-research-reports/issue-

brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/. Acesso em: 30 out. 2020.

HUGHES, Wayne P; GIRRIER, Robert. *Fleet tactics and naval operations*. Annapolis: Naval Institute Press, 2018.

IASIELLO, Emilio. Is Cyber Deterrence an Illusory Course of Action? *Journal of Strategic Security*, [*s. l.*], v. 7, n. 1, p. 54–67, 2014.

IDF, Israel Defense Forces. *Cleared for Release*. [*S. l.*], 2019. Disponível em: https://twitter.com/IDF/status/1125066395010699264?s=20. Acesso em: 17 out. 2020.

ISO, International Organization for Standardization. *ISO/IEC 27000. Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*. ISO - International Organization for Standardization, 2018.

ISO. *ISO/IEC 27033-1. Information technology — Security techniques — Network security — Part 1: Overview and concepts*. ISO - International Organization for Standardization, 2015.
JANIS, Irving Lester. *Groupthink*: psychological studies of policy decisions and fiascoes. Boston: Houghton Mifflin, 1982.

JENSEN, Eric. Cyber Deterrence. *Emory International Law Review*, [*s. l.*], v. 26, p. 773–824, 2012.

JERVIS, Robert. Deterrence Theory Revisited. *World Politics*, [*s. l.*], v. 31, n. 2, p. 289–324, 1979.

JERVIS, Robert; LEBOW, Richard Ned; STEIN, Janice Gross. *Psychology and deterrence*. Baltimore: Johns Hopkins University Press, 1985.

KARPAVIČIŪTĖ, Ieva. Strategic Stability: It Takes Two to Tango? *Lithuanian Annual Strategic Review*, [*s. l.*], v. 17, n. 1, p. 97–121, 2019.

KASPERSKY. *O que é uma ameaça persistente avançada (APT)?*. [*S. l.*], 2018. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/advanced-persistent-threats. Acesso em: 1 nov. 2020.

KLIMBURG, Alexander (org.). *National cyber security framework manual*. Tallinn: Nato Cooperative Cyber Defence Centre Of Excellence, 2012.

KNOPF, Jeffrey W. The Fourth Wave in Deterrence Research. *Contemporary Security Policy*, [*s. l.*], v. 31, n. 1, p. 1-33, 2010.

LIBICKI, Martin C. *Cyberdeterrence and cyberwar*. Santa Monica: Rand, 2009.
LONG, Austin G. *Deterrence-From Cold War to long war*: lessons from six decades of RAND research. Santa Monica: RAND, 2008.

LUPOVICI, Amir. The Emerging Fourth Wave of Deterrence Theory: Toward a New Research Agenda. *International Studies Quarterly*, [*s. l.*], v. 54, n. 3, p. 705-732, 2010.

LYNN, William. Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, [*s. l.*], v. 89, n. 5, p. 97-108, 2010.

MCKENZIE, Timothy M. *Is cyber deterrence possible?* Alabama: Air University Press, Air Force Research Institute, 2017.

MEARSHEIMER, John J. *The theory and practice of conventional deterrence*. Tese (Doutorado em Filosofia). Cornell University, 1981.

MORGAN, Patrick M. *Deterrence now*. Cambridge: Cambridge University Press, 2003.

MULLER, Richard. The Origins of MAD: A Short History of City-Busting. *In*: SOKOLSKI, Henry D (org.). *Getting MAD*: Nuclear mutual assured destruction, its origins and practice. Carlisle: Strategic Studies Institute, 2004, p. 15–50.

MYERS, Joe; WHITING, Kate. *These are the biggest risks facing our world in 2019*. [*S. l.*], 2019. Disponível em: https://www.weforum.org/agenda/2019/01/these-are-the-biggest-risks-facing-our-world-in-2019/. Acesso em: 27 out. 2020.

NEWMAN, Lily Hay. What Israel's Strike on Hamas Hackers Means For Cyberwar. *Wired*, [*s. l.*], 2019. Disponível em: https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/. Acesso em: 17 out. 2020.

NYE, Joseph. Deterrence and Dissuasion in Cyberspace. *Journal of Cyber Policy*, [*s. l.*], v. 1, n. 2, p. 44–71, 2016.

PUTTEN, Frans-Paul Van Der; MEIJNDERS, Minke; ROOD, Jan. *Deterrence as a security concept against non-traditional threats*. The Hague: Clingendael Institute, 2015.

RYAN, N. J. Five Kinds of Cyber Deterrence. *Philosophy & Technology*, [s. l.], v. 31, n. 3, p. 331–338, 2017. Disponível em: https://doi.org/10.1007/s13347-016-0251-1. Acesso em: 4 nov. 2020.

SAMSON, Victoria; WEEDEN, Brian (org.). *Global Counterspace Capabilities*: An Open Source Assessment. Washington: Secure World Foundation, 2020. Disponível em: https://swfound.org/media/206970/swf_counterspace2020_electronic_final.pdf. Acesso em: 31 out. 2020.

SCHELLING, Thomas C. *Arms and Influence*. New Haven: Yale University Press, 1966.

SCHELLING, Thomas C. *The strategy of conflict*. Cambridge: Harvard University Press, 1960.
SÊMOLA, Marcos. *Gestão da Segurança da Informação*: uma visão executiva. Rio de Janeiro: Elsevier, 2014.

SINGER, P W; FRIEDMAN, Allan. *Cybersecurity and cyberwar: what everyone needs to know*. Oxford: Oxford University Press, 2014.

SNYDER, Glenn. *Deterrence or Defense*. Princeton: Princeton University Press, 1961.

SNYDER, Glenn H. Deterrence and power. *Journal of Conflict Resolution*, [*s. l.*], v. 4, n. 2, p. 163–178, 1960.

STEINBRUNER, John. Beyond Rational Deterrence: The Struggle for New Conceptions. *World Politics*, [*s. l.*], v. 28, n. 2, p. 223–245, 1976.

SYEED, Nafeesa. Outer-Space Hacking a Top Concern for NASA's Cybersecurity Chief. *Bloomberg.com*, [*s. l.*], 12 Apr. 2017. Disponível em: https://www.bloomberg.com/news/articles/2017-04-12/outer-space-hacking-a-top-concern-for-nasa-s-cybersecurity-chief. Acesso em: 28 out. 2020.

TEN, Chee-Wooi; MANIMARAN, Govindarasu; LIU, Chen-Ching. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, [*s. l.*], v. 40, n. 4, p. 853–865, 2010.

THE WHITE HOUSE. *International Strategy for Cyberspace*. Washington: White House, 2011. Disponível em: https://assets.documentcloud.org/documents/2700127/Document-46.pdf. Acesso em: 23 set. 2020.

THE WHITE HOUSE. *National Cyber Strategy*. Washington: White House, 2018. Disponível em: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. Acesso em: 23 set. 2020.

THUCYDIDES. *The Peloponnesian War*. Tradução: Martin Hammond. Oxford: Oxford University Press, 2009.

VENTURES, Cybersecurity. *2019 Official Annual Cybercrime Report*. [*S. l.*]: Herjavec Group, 2020. Disponível em: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf. Acesso em: 27 out. 2020.

VILLA, Rafael Antonio Duarte. A segurança internacional no pós-Guerra Fria: um balanço da teoria tradicional e das novas agendas de pesquisa. *Bib: Revista Brasileira de Informação Bibliográfica em Ciências Sociais*, [*s. l.*], v. 62, n. 2, p. 19–31, 2006.

VON SOLMS, Rossouw; VAN NIEKERK, Johan. From information security to cyber security. *Computers & Security*, [*s. l.*], v. 38, n. 1, p. 97–102, 2013.

WALT, Stephen M. The Renaissance of Security Studies. *International Studies Quarterly*, [*s. l.*], v. 35, n. 2, p. 211–239, 1991.

WILNER, Alex. Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation. *Comparative Strategy*, [*s. l.*], v. 36, n. 4, p. 309–318, 2017.

WOHLSTETTER, Albert. The Delicate Balance of Terror. *Foreign Affairs*, [*s. l.*], v. 37, n. 2, p. 211–234, 1959.

WOLFERS, Arnold. The Atomic Bomb and Soviet-American relation. *In*: BRODIE, Bernard (org.). *The Absolute Weapon: Atomic Power and World Order*. New York: Harcourt, Brace and Co, 1946. p. 90-123.

Principais ameaças cibernéticas aos sistemas espaciais

André Lucas Alcântara da Silva

Resumo: Os setores cibernético e espacial são considerados, individualmente, estratégicos pela Estratégia Nacional de Defesa. No entanto é nítida a relevância e influência do primeiro sobre o segundo. Sistemas espaciais contam com elementos de alta tecnologia em todos os seus segmentos (espacial, terrestre e de usuário) e, portanto, estão susceptíveis a ataques cibernéticos de diferentes níveis. O objetivo deste trabalho é identificar as principais ameaças cibernéticas em sistemas espaciais. Para tanto, utiliza-se um estudo descritivo, baseado em levantamento e revisão bibliográfica e documental. Por meio da revisão bibliográfica, tendo como fonte livros e artigos científicos que abordam o tema, busca-se identificar a estrutura básica de sistemas espaciais, bem como os componentes cibernéticos dos mesmos e as principais ameaças existentes. O levantamento documental, por sua vez, está baseado em registros de ataques cibernéticos que tiveram ativos espaciais como principal alvo. Em seguida, o trabalho analisa as informações levantadas, descrevendo e classificando as ameaças cibernéticas mais relevantes em sistemas espaciais e os desafios da Tecnologia da Informação no tratamento de tais ameaças. A partir dessa análise é possível identificar que, atualmente, o segmento terrestre recebe a maior quantidade de ações de proteção cibernética, visto que o mesmo, à priori, está mais exposto se comparado aos demais segmentos. As principais ameaças cibernéticas para o segmento terrestre envolvem comprometimento dos ativos de rede e sistemas legados ou desatualizados. No caso do segmento espacial, as ameaças se concentram em vulnerabilidades de *hardware* e *software* embarcado. Quanto ao meio de comunicação, as ameaças mais relevantes se referem à utilização de sinais de rádio frequência para a incidência de *jamming*. No estudo conclui-se que existem diferentes tipos de ameaças cibernéticas para cada segmento do projeto espacial, portanto necessitam de tratamentos distintos. Por fim, recomenda-se o envolvimento dos setores de Tecnologia da Informação em todas as fases de um projeto espacial, desde a concepção até o encerramento de sua operação.
Palavras-chave: Ameaça cibernética. Sistemas espaciais. Tecnologia da Informação.

1 Introdução

A indústria tecnológica permanece em franca expansão desde a década de 1950 (HUTCHINS, 2016), as soluções providas por esses recursos são cada vez mais populares e de ampla utilização na sociedade. Nessa evolução, as tecnologias espaciais deixaram de ser exclusividade de grandes empresas e nações poderosas. Novos *players* foram inseridos nesse mercado bilionário, seja por motivos econômicos ou de ordem política-estratégica (HUTCHINS, 2016; MANULIS *et al.,* 2020; UNAL, ZATTI, 2020).

Serviços baseados em soluções espaciais tornaram-se comuns ou até mesmo essenciais, sejam eles de aplicação militar ou civil.

Naturalmente, devido ao nível de dependência tecnológica dos sistemas espaciais, os mesmos são expostos a possíveis vulnerabilidades técnicas, as quais podem ser exploradas e viabilizarem ataques cibernéticos, capazes de gerar danos de inúmeros tipos e intensidade (UNAL, 2019).

A importância dos sistemas espaciais no processo de controle e monitoramento de infraestruturas críticas, comunicação, posicionamento e navegação, bem como agricultura e defesa nacional, fizeram com que países estabelecessem os setores espacial e cibernético como estratégicos para a nação. Do ponto de vista militar, organizações internacionais como a Organização do Tratado do Atlântico Norte (OTAN) reconheceram esses setores como novos domínios operacionais de combate (GREST *et al*., 2020).

Diante desse cenário, torna-se relevante compreender a relação dos setores citados, bem como a influência cibernética no âmbito espacial. Assim, o objetivo do presente trabalho é identificar as ameaças cibernéticas em sistemas espaciais. Para isso, são analisados desde a importância estratégica de tais setores até o histórico de ataques cibernéticos voltados a ativos espaciais.

2 A importância estratégica dos setores cibernético e espacial

Os Objetivos Nacionais de Defesa (OND) do Brasil estão descritos na Política Nacional de Defesa (PND), documento de mais alto nível para o planejamento de ações destinadas à defesa do País (BRASIL, 2020). Tal documento é acompanhado da Estratégia Nacional de Defesa (END) que, por sua vez, descreve as Estratégias de Defesa (ED) e orientam as Ações Estratégicas de Defesa (AED), as quais são necessárias para o alcance dos OND. Tanto a PND quanto a END são revisadas quadrienalmente pelo Poder Executivo, por meio do Ministério da Defesa (MD), e encaminhadas ao Congresso Nacional.

Desde a primeira versão do atual formato da PND, publicada em 2012, alguns setores receberam especial atenção no intuito de reforçar a relevância dos mesmos no cenário político-estratégico de Defesa Nacional. Dois dos três setores mencionados foram o cibernético e o espacial. Enquanto o primeiro envolve a capacidade de o Estado atuar de forma eficaz no âmbito do espaço cibernético, seja com ações de defesa, monitoramento ou ataque, o segundo se refere ao desenvolvimento do setor espacial brasileiro, desde o aumento de competências associadas aos projetos de veículos lançadores de satélites até a

própria fabricação e integração de plataformas espaciais para aplicações civil e militar (BRASIL, 2020).

O destaque de tais setores em documentos como a PND e END está alinhado ao que acontece no âmbito mundial, quer do ponto de vista de grandes nações ou da perspectiva de organizações internacionais, que entendem a concepção estratégica dos setores cibernético e espacial, bem como a necessidade de proteção dos mesmos. A respeito do setor cibernético, especificamente, a Secretaria Geral da Organização das Nações Unidas (ONU), por meio do *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* é enfática ao dizer que:

> O espaço cibernético se relaciona a todos os aspectos de nossas vidas. Os benefícios são enormes, mas não vêm sem riscos. O ambiente global de tecnologia enfrenta um dramático aumento das ameaças cibernéticas praticadas por atores estatais e não estatais. O uso indevido dos recursos tecnológicos representa um risco para todos os Estados e pode comprometer a paz e a segurança internacional (ONU, 2019, tradução nossa).

Ao analisar o cenário nacional no contexto da PND, o próprio documento reconhece a relevância de possuir uma estrutura segura no espaço cibernético:

> Requerem especial atenção a segurança e a defesa do espaço cibernético brasileiro, essenciais para garantir o funcionamento dos sistemas de informações, de gerenciamento e de comunicações de interesse nacional. (BRASIL, 2020, p. 8).

O setor espacial, por sua vez, também recebe especial atenção nos dias de hoje. O uso do espaço tornou-se essencial para operar e manter as infraestruturas nacionais e internacionais, que oferecem serviços de comunicação, monitoramento ambiental, navegação e apoio a experimentos científicos (UNAL, 2019). No âmbito nacional, a PND (2020, p. 8) considera a atuação espacial ferramenta para a manutenção da soberania brasileira: “O uso do espaço exterior, [...] bem como o contínuo desenvolvimento aeroespacial são essenciais para resguardar a soberania e os interesses nacionais”.

2.1 Relação entre os setores Cibernético e Espacial

Naturalmente, por tratar-se de setores baseados em tecnologia, há considerável relação entre os mesmos. Ambos possuem importância singular em inúmeros setores, sejam eles voltados para segurança e defesa ou para a manutenção de serviços essenciais à população. Ademais, tanto o setor cibernético quanto o espacial podem ser relevantes

facilitadores no processo de desenvolvimento tecnológico de um país, proporcionando avanços em pesquisas e trabalhos científicos.

No entanto, percebe-se maior influência do setor cibernético sobre o espacial. Segundo a pesquisadora Unal (2019, p. 2, tradução nossa),

> Todos os satélites dependem de tecnologias cibernéticas incluindo *software, hardware* e outros componentes digitais. Logo, qualquer ameaça ao sistema de controle do satélite ou à sua disponibilidade, representa um desafio direto aos ativos críticos nacionais.

Assim, no âmbito de um sistema espacial, caso as vulnerabilidades cibernéticas não sejam identificadas e tratadas de forma eficaz, o mesmo pode sofrer danos severos, comprometendo a disponibilidade dos serviços por ele prestados.

3 Estrutura básica de sistemas espaciais e seus componentes cibernéticos

Sistemas espaciais são montados de acordo com a missão a ser realizada pelos mesmos, no entanto há uma arquitetura genérica aplicada a todos eles, independentemente de sua aplicação. Tal estrutura, de forma geral, é composta por três grandes segmentos: o segmento espacial; o segmento terrestre; e o segmento de usuário (NATO, 2019). Este último, inclusive, é tratado como uma extensão do segmento terrestre por inúmeros autores. Especificamente neste trabalho, o segmento de usuário será tratado de forma separada, visto que possui vulnerabilidades cibernéticas particulares que serão abordadas no capítulo quatro. Além dos três segmentos básicos, há a estrutura de comunicação entre eles. A comunicação no sentido segmento terrestre - ou segmento de usuário – para o segmento espacial é chamada de *uplink*, logo o sentido inverso da comunicação é conhecido como *downlink*.

O segmento espacial inclui um ou mais satélites em órbita, estações espaciais e veículos lançadores de satélites (VLS) (GARINO; GIBSON, 2018). O satélite, em si, possui uma carga útil (*payload*), responsável por realizar a função do satélite propriamente dita. Adicionalmente, o satélite conta com sistemas específicos, capazes de receber e enviar dados, bem como validá-los, decodificá-los e direcioná-los a outros (MANULIS *et al*., 2020). O segmento terrestre, por sua vez, refere-se a toda infraestrutura terrestre, capaz de receber e enviar sinais de Radiofrequência (RF) que possibilitam o controle e monitoramento do satélite. Os principais elementos desse segmento são estações terrestres, centros de gerenciamento de missão, além da infraestrutura de redes, capaz de interligar os sistemas e enviar os dados coletados ao segmento de usuário. O terceiro e último segmento trata da infraestrutura

disponível para que o usuário consiga receber o serviço/produto fornecido pelo satélite. Para tanto, pode comunicar-se diretamente com o satélite ou com a estrutura de controle do segmento terrestre (MANULIS *et al*., 2020).

Todos os segmentos demostram estreita dependência de componentes digitais e cibernéticos. Um exemplo é a necessidade de sistemas e subsistemas satelitais. Tais recursos são compostos por *hardwares* e *softwares* que, juntos, possuem funções específicas e vitais para o satélite, como aqueles responsáveis por possibilitarem a recepção de telemetria, os dados de rastreamento e o envio de comandos (TT&C), a manipulação de dados (C&DH) e a determinação e o controle de órbita (AOCS) (MANULIS *et al*., 2020). Além disso, há uma gama de outros elementos tão importantes quanto os anteriores e que suportam as operações espaciais, como: sensores, antenas, terminais de comunicação, sistemas, banco de dados e computadores, bem como a rede capaz de interligá-los.

4 Principais ameaças cibernéticas aos sistemas espaciais

O uso do espaço exterior e a dependência dos serviços fornecidos por satélites têm aumentado a cada ano. No âmbito militar, segundo a análise da *Chatham House*, praticamente todas as recentes operações militares executadas por países da OTAN contaram com recursos providos por sistemas espaciais. Ainda na mesma análise, os autores da pesquisa ressaltam que o componente espacial influencia diretamente em todos os demais domínios operacionais, a saber: mar; terra; ar; e cibernético (UNAL, 2019). Em uma perspectiva civil, percebe-se a utilização em massa de serviços satelitais no dia a dia da sociedade. São comunicações via satélites, transmissões de programas televisivos, telefonia celular, conexões banda-larga, informações de posicionamento e navegação, entre outros. Toda essa demanda impulsiona o mercado e a indústria de ativos espaciais. De acordo com Livingston e Lewis (2016, p. 10, tradução nossa):

> O mercado espacial, considerando a construção de satélites, foguetes e veículos espaciais, além dos serviços providos através de tecnologia espacial, está estimado em 125 bilhões de libras por ano e estará próximo a 400 bilhões de libras em 2030.

Esse cenário faz dos sistemas espaciais alvos de ofensivas cibernéticas, oriundas de inúmeros locais, praticadas por atores estatais e não estatais com diferentes motivações. De acordo com a *Consultative Commitee for Space Data Systems* (CCSDS), as ameaças cibernéticas mais comuns em sistemas espaciais são: alteração/corrupção de dados; perda do

sistema de controle (terrestre); interceptação de dados; *jamming*; negação de serviço; *spoofing*; ataques *replay*; ameaças de *software*; e acesso não autorizado (CCSDS, 2015).

Analisando o aumento da demanda por serviços satelitais, bem como sua recorrente aplicação em missões militares, os pesquisadores Zatti e Unal (2020) são claros ao reconhecerem o desafio da gestão da cadeia de suprimentos/materiais utilizados no desenvolvimento e na construção de ativos espaciais. Na visão dos pesquisadores, a busca das empresas em reduzir custos operacionais fez com que as mesmas passassem a terceirizar a construção de equipamentos e dispositivos digitais a serem incorporados nos projetos satelitais. Essa situação, somada a ausência de fiscalização e acompanhamento do processo produtivo, é crítica e pode tornar-se fonte de vulnerabilidades, caso o fabricante insira *softwares* maliciosos embarcados ao equipamento ou, até mesmo, deixe de existir, fazendo com que os dispositivos fiquem desatualizados e obsoletos. Para Manulis *et al.* (2020), essa dinâmica é típica de um novo momento da indústria espacial, conhecida como New Space. Segundo o pesquisador, tal momento evidencia o ingresso de pequenas e médias empresas no mercado espacial, fornecendo principalmente, serviços e produtos gerados por constelações de *Small Sats*, ou seja, pequenos satélites em órbita baixa, de custo reduzido, capazes de minimizar o tempo entre a concepção e o lançamento dos mesmos.

Além disso, existem ameaças que possuem maior incidência em determinados segmentos. Sendo assim, analisá-las com base no segmento afetado colabora para a compreensão geral do problema, o que é demonstrado nos tópicos a seguir.

4.1 Segmento espacial

O segmento espacial é considerado o segmento mais difícil de ser atacado. Uma vez em órbita e não acessível fisicamente danificá-lo irá requerer um considerável conhecimento de todo o sistema espacial, no entanto, o mesmo não está imune a ataques cibernéticos. Segundo o professor e pesquisador Zatti (2020), tal segmento tornou-se mais vulnerável nos últimos anos devido às múltiplas conexões de redes utilizadas. No caso, um ataque cibernético a esse segmento seria possível com a obtenção do controle de seu *link* de comunicação.

Além disso, o segmento espacial pode ser atacado devido a possíveis vulnerabilidades em seus ativos, sejam elas de *software* ou *hardware*. Satélites mais recentes têm aplicado novas tecnologias capazes de substituir um determinado equipamento. É o caso do Rádio Definido por *Software* (SDR), que utiliza sistemas capazes de prover as funcionalidades de um

rádio tradicional. O processamento equivocado dos *frames* e o envio de pacotes mal formatados podem gerar o efeito conhecido como *Buffer Overflow*, provocando situações de negação de serviço (DoS) e até mesmo o bloqueio da comunicação com o satélite (MANULIS *et al.,* 2020).

4.2 Segmento terrestre

Diferentemente do segmento espacial, o segmento terrestre está mais exposto aos ataques cibernéticos. O fato de ser acessível fisicamente, fazer uso de redes de computadores corporativas e contar com um número elevado de pessoas no ambiente ampliam as formas de ataque a este segmento. Uma vez que o segmento terrestre possui os ativos necessários para o controle e monitoramento satelital, obter o acesso a tais recursos ou inserir algum tipo de vulnerabilidade em seu parque tecnológico torna-se a maneira mais simples de afetar um sistema espacial.

Sendo assim, no âmbito do segmento terrestre, as seguintes ameaças podem ser destacadas:

a) ataques físicos: caracteriza-se quando o atacante obtém acesso não autorizado à estação de solo, bem como aos ativos de tecnologia da informação (TI), possibilitando a coleta de informações, manipulação de dados ou até mesmo o dano físico dos equipamentos existentes. Essas ações podem gerar danos de diferentes níveis de severidade, desde o simples desligamento de um ativo de TI até a obtenção do controle do satélite, propriamente dito (MANULIS *et al.,* 2020);

b) alteração/corrupção de dados: trata-se da modificação de dados em trânsito ou armazenados, o que pode ocorrer devido a falhas de *softwares*/ *hardwares* ou pela utilização de sistemas não originais, que possuem a capacidade de danificar informações por ele utilizadas. Nesse caso, um determinado comando enviado ao satélite poderia ser modificado antes de seu envio, gerando resultados/comportamentos não desejados (MANULIS *et al.,* 2020);

c) ataques do tipo *Computer Network Exploitation* (CNE): são ataques que visam comprometer a rede de computadores utilizada no segmento terrestre, desabilitando ativos de segurança de rede no intuito de deixá-la

vulnerável. Assim, o atacante teria livre acesso aos seus recursos, podendo, inclusive, influenciar nos ativos que possibilitam o controle satelital (MANULIS *et al.,* 2020); e

d) sistemas legados/desatualizados: inevitavelmente, a infraestrutura de TI disponível no segmento terrestre utiliza *softwares* corporativos amplamente conhecidos no mercado, desenvolvidos por terceiros e com vistas a uma utilização genérica. Tais sistemas são conhecidos como *Commercial Off-The-Shelf* (COTS), que precisam de atualização periódica, principalmente no que se refere à correção de vulnerabilidades. Se essas atualizações não forem realizadas ou se o fornecedor descontinuar o produto, os ativos de TI que utilizam esses recursos ficarão ainda mais expostos (MANULIS *et al.,* 2020).

4.3 Segmento de usuário

O segmento de usuário, por tratar-se de uma extensão do segmento terrestre, está susceptível aos mesmos tipos de ataques, no entanto faz-se necessário evidenciar algumas outras ameaças mais relevantes neste segmento.

a) Interceptação de informações: o segmento de usuário é composto por equipamentos capazes de receber os produtos/serviços providos pelo satélite. Nesse contexto, em algum momento, o resultado gerado pelo satélite estará disponível para acesso. Caso a infraestrutura disponível esteja vulnerável a ataques cibernéticos, as informações ali disponíveis poderão ser acessadas por pessoas não autorizadas e, consequentemente, danos de diferentes severidades poderão ser gerados (CCSDS, 2015); e

b) Engenharia Social: de forma geral, as pessoas que compõem o segmento de usuário estão mais focadas na utilização dos produtos/serviços disponibilizados pelos satélites que nos procedimentos de segurança afetos a arquitetura e controle do sistema espacial. Nesses casos, podem tornar-se vítimas de engenharia social, fornecendo informações sensíveis quanto a localização de terminais de acesso, estrutura e forma de disponibilização de dados. Tais informações podem ser utilizadas pelo atacante durante o período de preparação para atacar os segmentos espacial e terrestre (CCSDS, 2015).

4.4 Comunicação

A comunicação em sistemas espaciais pode ocorrer em três sentidos distintos. Os dois primeiros se referem a troca de informações entre o segmento espacial e o segmento terrestre (incluindo o segmento de usuário). Tal comunicação acontece via ondas de RF, possibilitando o envio de telecomandos ao satélite e o recebimento de telemetrias e dados de monitoramento. Nesse caso, os tipos de ataques mais conhecidos são:

a) *jamming*: tipo de ataque que requer uma antena, o conhecimento da frequência pela qual a comunicação está acontecendo e a capacidade de transmitir um sinal em alta potência. Ele consiste em emitir tal sinal na mesma frequência utilizada para a comunicação entre os segmentos espacial e terrestre. Dessa forma, o sinal emitido pelo atacante causará interferência na comunicação entre as partes (MANULIS *et al*., 2020);

b) *eavesdropping*: trata-se da interceptação de dados por um canal de comunicação. No caso da troca de informações entre o satélite e a estação terrestre, tal comunicação ocorre via RF, utilizando o ar como meio para trafegar o conteúdo das mensagens. Sendo assim, se a comunicação entre as partes não for criptografada, o atacante pode utilizar equipamentos específicos para interceptar os dados e ter acesso às informações (MANULIS *et al.,* 2020); e

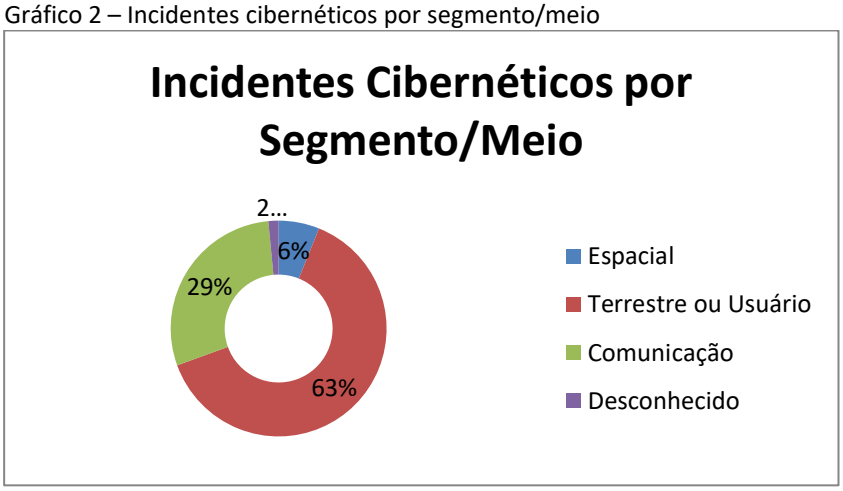
c) *spoofing*: caracteriza-se pela possibilidade de transmitir um sinal, passado por legítimo, porém com envio de dados errôneos. Este tipo de ataque pode gerar desinformação e ser bastante prejudicial ao processo de tomada de decisão, seja no aspecto civil ou militar (MANULIS *et al.,* 2020).

O terceiro e último sentido de comunicação, em um sistema espacial, refere-se à troca de informações entre as estações terrestres e os equipamentos do segmento de usuário. Ela ocorre, em sua maioria, por meio de conexões físicas via cabeamento estruturado. Nesse caso, as principais ameaças são o acesso físico não autorizado às estruturas de rede, bem como aos ativos de configuração da rede em questão, o que possibilita ao atacante interferir na comunicação entre as partes.

5 Ataques cibernéticos a ativos espaciais

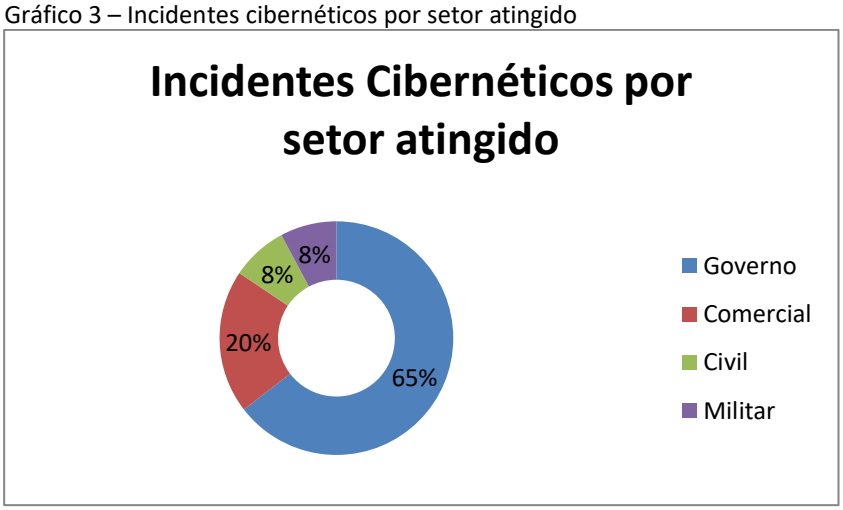
A identificação de ataques cibernéticos, independente se são aplicados contra ativos espaciais ou não, é uma tarefa complexa (HUTCHINS, 2016). Uma vez que a grande parte dos ataques possui motivações políticas e econômicas, garantir o anonimato da autoria faz parte da estratégia dos atacantes. Por outro lado, Estados e Organizações, vítimas de tais ataques, nem sempre reconhecem o fato, no intuito de não demonstrarem vulnerabilidades existentes. Pesquisadores britânicos das universidades de Surrey e Manchester, no entanto, catalogaram uma série de incidentes a ativos espaciais entre os anos de 1977 a 2019, categorizando-os de acordo com o segmento atacado, o setor atingido e o tipo de incidente ocorrido. Segundo a pesquisa, os ataques do tipo roubo/perda de dados, CNE e j*amming* representam a maior parte dos casos, 36%, 22% e 14%, respectivamente (MANULIS *et al.,* 2020). Quanto ao segmento atacado e o setor atingido, os gráficos abaixo demonstram o resultado do referido trabalho.

Gráfico 2 – Incidentes cibernéticos por segmento/meio



Fonte: MANULIS *et al.,* 2020, p. 9

Gráfico 3 – Incidentes cibernéticos por setor atingido



Fonte: MANULIS *et al.,* 2020, p. 9

Alguns desses ataques fornecem a dimensão do impacto causado nos produtos/serviços gerados por ativos espaciais. A seguir, são citados três que obtiveram uma repercussão mundial.

a) Em novembro de 2018, durante um exercício militar conjunto da OTAN no norte da Finlândia, os serviços de navegação aérea civil, tendo como base informações providas pela constelação de satélites GPS, foram afetados por interferências eletrônicas. Paralelamente, a Noruega também reportou a perda das capacidades de navegação via GPS. Identificar o autor e as motivações relativas ao ataque não é simples, no entanto, de acordo com a situação política à época e considerando que o exercício foi realizado próximo à fronteira russa, de país que já havia expressado sua insatisfação com a ocorrência de tal exercício naquela região, é possível compreender o que talvez fosse uma motivação para ataques cibernéticos (HUTCHINS, 2016; FALCO, 2018);
b) a *National Oceanic and Atmospheric Administration* (NOAA), instituição ligada ao governo norte-americano e administradora de uma constelação de satélites de observação terrestre para monitoramento climático, foi alvo de um ataque cibernético em 2014. Segundo a organização, o ataque foi executado via *internet* e atingiu quatro *sites* da NOAA, resultando na interrupção temporária do fluxo de dados de satélites para o serviço meteorológico. A instituição acionou os órgãos de investigação, que trataram o ataque de forma sigilosa (GRUSS, 2014; HUTCHINS, 2016; FALCO, 2018); e
c) em 2017, houve um registro de ataque do tipo *spoofing*. Segundo reportado pela *US Maritime Administration*, vinte navios foram impactados pela variação dos sinais de posicionamento. No caso, os equipamentos de navegação que utilizam informações providas pela constelação de satélites GPS, indicavam um posicionamento equivocado dos navios, algo em torno de 25 milhas náuticas da posição real (FALCO, 2018).

Diante de uma gama de possibilidades de ataques cibernéticos e inúmeras vulnerabilidade que podem ser exploradas, pesquisadores, organizações e instituições públicas têm dedicado esforços no intuito de reduzirem a probabilidade de sucesso dessas investidas. Medidas mitigadoras como envolver especialistas em segurança cibernética

durante todo o ciclo de vida de um sistema espacial, desde a sua concepção até a descontinuidade do mesmo, passando pelo *design* do sistema; definir processos capazes de garantir a segurança dos dispositivos digitais fabricados por terceiros (gerenciamento da cadeia de suprimentos); e avaliar/monitorar os riscos identificados, são tidas como as mais relevantes no âmbito da segurança cibernética (UNAL; ZATTI, 2020).

Da perspectiva institucional e governamental, países buscam criar padrões e orientações específicas acerca da proteção cibernética, tanto de maneira geral quanto especificamente de sistemas espaciais. Exemplo disso são os relatórios de *Security Threats Against Space Missions*, *The Consultative Committee for Space Data Systems* (CCSDS) e de boas práticas publicadas pela estadunidense *Cibersecurity & Infraestructure Security Agency*. Há também organizações não governamentais que se dedicam a pesquisar o tema em questão, como a *Chatham House* e o grupo especializado em *Space & Cyber security* da *Space Generation Advisory Council*.

6 Considerações finais

Os setores cibernético e espacial são estratégicos e essenciais nos dias de hoje. As tecnologias desenvolvidas no âmbito cibernético habilitam novas possibilidades aos sistemas espaciais, os quais podem entregar uma variedade de serviços e produtos. Indiferentemente da aplicação, soluções espaciais geram benefícios para inúmeros setores, sejam eles militar, civil, governamental ou privado.

Da perspectiva de uma arquitetura genérica de sistema espacial, é possível perceber que existem diferentes ameaças cibernéticas de acordo com cada segmento dessa estrutura. O segmento terrestre, mais susceptível a ataques cibernéticos, está exposto a ataques do tipo físico e CNE, além das possíveis vulnerabilidades existentes em *softwares* do tipo COTS. O segmento de usuário, por ser uma extensão do segmento terrestre, está sujeito aos mesmos tipos de ataques; ademais, também é exposto a ataques do tipo interceptação de informação e engenharia social. O segmento espacial, mesmo estando fisicamente inacessível, não está livre das ameaças cibernéticas.

A crescente utilização de *softwares* capazes de realizar funções que outrora eram executadas por equipamentos específicos pode ser uma vulnerabilidade para o sistema espacial. É o caso do uso de SDR em substituição a um rádio tradicional. Caso o mesmo seja mal codificado (com ou sem intenção) poderá comprometer o funcionamento do satélite. A

infraestrutura de comunicações também pode ser alvo de ataques cibernéticos do tipo j*amming*, s*poofing* e e*avesdropping*.

Historicamente, a maioria dos ataques cibernéticos, realizados contra ativos espaciais, teve como meio o segmento terrestre, justamente pela maior facilidade de acesso. Adicionalmente, é possível perceber que o principal alvo desses ataques são organizações governamentais.

Por fim, evidencia-se que o envolvimento de especialistas em TI e segurança da informação, desde a concepção do sistema espacial até o término de sua vida útil, bem como a existência de processos e legislações específicas para garantir a integridade de dispositivos digitais adquiridos por terceiros, são essenciais para que se reduzam as chances de sucesso dos ataques cibernéticos.

Referências

BRASIL. Ministério da Defesa. *Política de Defesa Naciona*. Brasília, DF, 2020.

CCSDS. *Security Threats Against Space Missions*. CCSDS, 2015. Disponível em: https://public.ccsds.org/Pubs/350x1g2.pdf. Acesso em: 10 out. 2020.

FALCO, Gregory. *Job one for space force: Space asset security*. Harvard Kennedy School, 2018. Disponível em: https://www.belfercenter.org/sites/default/files/files/publication/CSP%20Falco%20Space%20Asset%20-%20FINAL.pdf. Acesso em: 9 out. 2020.

GARINO, B.; GIBSON, J. *Space System Threats*. Aeroespace Security, 2018. Disponível em: https://aerospace.csis.org/wp-content/uploads/2018/09/Space-System-Threats.pdf. Acesso em: 5 out. 2020.

GREST, H.; VASEM, T.; HEREN, H. *Space: NATO'S Newst Operational Domain*. Joint Air Power Competence Center, 2020. Disponível em: https://www.japcc.org/wp-content/uploads/JAPCC-Flyer-on-Space-NATOs_Newest_Operational_Domain.pdf. Acesso em: 31 set. 2020.

GRUSS, Mike. *NOAA admits to cyberattack on satellite data networks*. Space News, 2014. Disponível em: https://spacenews.com/42561noaa-admits-to-cyberattack-on-satellite-data-networks/. Acesso em: 13 out. 2020.

HUTCHINS, Ryan. *Cyber defense of space assets*, 2016. Disponível em: http://www.cs.tufts.edu/comp/116/archive/fall2016/rhutchins.pdf. Acesso em: 2 out 2020.

LIVINGSTON, David; LEWIS, Patricia. *Space, the final frontier for cybersecurity*. Chatham House, September 2016. Disponível em: https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf. Acesso em: 31 out. 2020.

MANULIS, M.; BRIDGES, C.P.; HARRISON, R. *et al*. Cyber security in New Space. *Int. J. Inf. Secur*., May 2020. Disponível em: https://link.springer.com/article/10.1007/s10207-020-00503-w#citeas . Acesso em: 1 out 2020.

NATO, *space Handbook*. Chatham House, July 2019. Disponível em: https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf. Acesso em: 7 out. 2020.

ONU. *Developments in the field of information and telecommunications in the context of international security*, 2019. Disponível em: https://www.un.org/disarmament/ict-security/. Acesso em: 4 set. 2020.

UNAL, Beyza. *Cybersecurity of of NATO's Space-based strategic assets*. Chatham House, July 2019. Disponível em: https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf. Acesso em: 2 out. 2020.

UNAL, Beyza; ZATTI, Stefano. *Cybersecurity of space based weapons systems and Protecting space missions from cyber threats*. Second webinar report, April 2020. Disponível em: https://spacegeneration.org/wp-content/uploads/2020/05/Report-2nd-Webinar-SGAC-SpaceCybersecurity-PG.pdf. Acesso em: 2 out. 2020.

Defesa da propriedade intelectual contra *cyberattacks* nas infraestruturas do setor aeroespacial brasileiro

Viviane Souza da Costa

Resumo: O presente artigo objetiva retratar como o investimento na Defesa da Propriedade Intelectual das Infraestruturas do Setor Aeroespacial Brasileiro pode representar oportunidades para diversos setores da indústria de Defesa, especialmente das Empresas de Defesa e Empresas Estratégicas de Defesa na proteção dos 10 (dez) principais ataques cibernéticos à propriedade intelectual na Administração Pública, bem como realizar revisão integrativa da literatura dos processos de homologação e certificação dos produtos de natureza cibernética utilizados por Órgãos da Administração Pública Central e Forças Armadas. Os resultados desses estudos apresentados nas considerações finais, ao retratarem e sistematizarem as soluções a serem implementadas, visam contribuir para validação e avanço da pesquisa, em especial para os estudos do grupo focal de especialistas em Inovação e Propriedade Intelectual para o Setor de Defesa, bem como para o desenvolvimento de mecanismos de prevenção aos ataques cibernéticos e aperfeiçoamento legislativo no combate de tais práticas.
Palavras-chave: Propriedade Intelectual. Defesa Cibernética. Setor Aeroespacial.

1 Introdução

De acordo com a Lei 12.737 de 2012, que alterou o artigo 154-A do Código Penal Brasileiro, *cyberattack* – ataque cibernético ou ciberataque − é um tipo de crime virtual definido como invasão de dispositivos informáticos alheios, mediante violação indevida de mecanismos de segurança, e, que, sem autorização de seus titulares, por diferentes meios, busca obter vantagem ilícita. A Propriedade Intelectual (PI) de diferentes organizações vem sendo o principal alvo desse tipo de crime virtual.

Propriedade Intelectual é uma expressão genérica que pretende garantir a inventores ou responsáveis por qualquer produção do intelecto (seja nos domínios industrial, científico, literário e/ou artístico) o direito de auferir, ao menos por um determinado período de tempo, uma recompensa pela própria criação (NUNES, 2009 *apud* WIPO, 2020). Segundo as normas estabelecidas pela Organização Mundial da Propriedade Intelectual (OMPI, em inglês *WIPO: World Intellectual Property Organization*), o sistema de PI abrange duas grandes áreas: Propriedade Industrial (patentes, marcas, desenho industrial, indicações geográficas e proteção de cultivares) e Direito Autoral (obras literárias e artísticas, programas de

computador, domínios na Internet e cultura imaterial) e visa promover um ambiente em que a criatividade e a inovação possam florescer (WIPO, 2020).

Os sinais emergem de qualquer processo de interação entre dos indivíduos, incluindo ocaso específico de interações econômicas. A marca, por exemplo, que desde sua origem rapidamente ganhou impulso com a era industrial e hoje é crucial à existência de uma economia de mercado como a conhecemos, é um sinal usado nas atividades econômicas para identificar um produto ou serviço específico. Em outras palavras, é um "sinal distintivo" que permite aos consumidores distinguir entre mercadorias diferentes e reconhecer sua proveniência. Esses atributos tornam a marca registrada um dispositivo econômico extremamente poderoso (RAMELLO, 2006).

Não é sem razão que um ataque cibernético aos ativos de propriedade intelectual de uma instituição, e a marca é um exemplo desses ativos, possa causar danos de natureza imedível, com potencial de atingir não só seus sistemas computacionais, como também tem o condão de atingir a reputação institucional perante o mercado e expor suas vulnerabilidades.

As mudanças tecnológicas das últimas décadas do Século XX provocaram um impacto nas infraestruturas de produção, de segurança e de crédito com a estrutura do conhecimento. O conhecimento, o controle sobre sua produção e seu acesso a ele transformaram-se num ponto crucial da competição entre Estados. Poder e conhecimento significa poder sobre a produção, segurança e crédito (GANDELMAN, 2004).

No Brasil, corroborando o exposto, a Portaria nº 2 de 08 de fevereiro de 2008 - Gabinete de Segurança Institucional da Presidência da República (GSI/PR), publicada no Diário Oficial da União (D.O.U.) de 11 de fevereiro de 2008 instituiu Grupos Técnicos de Segurança de Infraestruturas Críticas (GTSIC) e considerou como áreas prioritárias em seu artigo 3°,incisos de I a V: Energia, Transporte, Água, Telecomunicações e Finanças, principais setores onde o controle da produção é exercido e que podem colocar em risco a segurança nacional em caso de ataques cibernéticos que interrompam o funcionamento de serviços essenciais.

A segurança das Infraestruturas Críticas (IEC), para efeitos dessa Portaria, é considerada como instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional.

Partindo das áreas prioritárias, o investimento na defesa da propriedade intelectual das infraestruturas críticas do setor aeroespacial brasileiro pode trazer possibilidades para

diversos setores da indústria de Defesa, especialmente das Empresas de Defesa (ED) e Empresas Estratégicas de Defesa (EED) na proteção dos 10 (dez) principais ataques cibernéticos à propriedade intelectual na Administração Pública*: backdoor, phishing, spoofing,* manipulação de *URLs, Denial Of Service* (DoS), *Distributed Denialof Service (DDoS), Ataque DMA (Direct Memory Access), eavesdropping, decoy e Shoulder surfing.*

As "Empresas de Defesa" e "Empresas Estratégicas de Defesa" são definidas pela Lei 12.598 de 21 de março de 2012, que também classifica um produto ou serviço como de interesse estratégico para a defesa nacional pelo conteúdo tecnológico, dificuldade de obtenção ou pela imprescindibilidade e podem ser na forma do inciso II, alíneas "a", "b" e "c" do artigo 2°,desde recursos bélicos navais, terrestres e aeroespaciais; serviços técnicos especializados na área de projetos, pesquisas e desenvolvimento científico e tecnológico, como equipamentos e serviços técnicos especializados para as áreas de informação e de inteligência.

Sendo a cibersegurança imprescindível para a proteção dos ativos da Propriedade Intelectual das Infraestruturas críticas não só da Administração Pública Federal, como do Setor Aeroespacial Brasileiro, a criação de soluções para proteção destes ativos pode representar oportunidades para diversos setores da indústria de Defesa, especialmente os regulamentados na Forma do Decreto 7.970 de 28 de março de 2013 na forma do artigo 4°, por meio dos quais os produtos de defesa serão catalogados conforme as normas e os procedimentos compatíveis com o Sistema Militar de Catalogação das Forças Armadas (SISMICAT).

Uma importante diretriz na estratégia tecnológica do governo brasileiro é a confecção de um sistema que seja capaz de homologar e certificar os produtos utilizados pelos órgãos centrais e forças armadas, de modo a garantir que não haja espionagem cibernética nos equipamentos em uso pela Administração Pública. Tais sistemas são esforços conjuntos e atuais dos Estados Unidos e países da Europa e Ásia para construírem uma sistemática de segurança cibernética similar à preocupação brasileira (BARBALHO *et al*., 2018).

Uma revisão sistemática da efetividade da Tríplice Hélice à Quíntupla Hélice no Setor Aeroespacial com aplicação no desenvolvimento de soluções desde a comunicação cibernética de aeronaves aos demais produtos de defesa com aplicação do *Privacy by Design* (PbD), visa antecipar e prevenir situações de invasão de privacidade antes de elas acontecerem (CAVOUKIAN, 2009).

Com a finalidade de contribuir com o diagnóstico da segurança cibernética e proteção das infraestruturas físicas aprovadas pela Política Nacional de Segurança das Infraestruturas Críticas Nacionais, este artigo está dividido da seguinte forma: na introdução são apresentados os conceitos gerais de *cyberattack* e PI e sua inter-relação com o Setor Cibernético e Espacial como estratégicos para a Defesa Nacional. A seção 1 aborda a proteção jurídica à Propriedade Intelectual das Estruturas Críticas no Setor Cibernético e Aeroespacial, a seção 2 aponta os Principais Riscos aos Sistemas Informacionais da Administração Pública Federal, a estrutura metodológica é apresentada na seção 3juntamente com os resultados da Recente fiscalização denominada "Levantamento de Riscos em Sistemas Informacionais da Administração Pública Federal, autorizada por meio do Acórdão 2.077/2019", realizada pelo Tribunal de Contas da União (TCU), e, por fim, na seção 4, são apresentados os desafios no tratamento e resposta aos incidentes da Segurança da Informação e as oportunidades para a Indústria de Defesa seguida das considerações finais.

O presente artigo objetiva retratar como o investimento na defesa da propriedade intelectual das infraestruturas do setor aeroespacial brasileiro pode representar oportunidades para diversos setores da indústria de Defesa, especialmente pelas ED e EED, na proteção dos 10 (dez) principais ataques cibernéticos à propriedade intelectual na Administração Pública, bem como realizar revisão integrativa da literatura dos processos de homologação e certificação dos produtos de natureza cibernética utilizados por Órgãos da Administração Pública central e Forças Armadas. Os resultados desses estudos, apresentados nas considerações finais, ao retratarem e sistematizarem as soluções a serem implementadas, visam contribuir para validação e avanço da pesquisa, em especial para os estudos, do grupo focal de especialistas em Inovação e Propriedade Intelectual para o Setor de Defesa, para o desenvolvimento de mecanismos de prevenção aos ataques cibernéticos e aperfeiçoamento legislativo no combate de tais práticas.

2 A proteção jurídica à Propriedade Intelectual das Estruturas Críticas nos Setores Cibernético e Aeroespacial

A proteção jurídica à Propriedade Intelectual e seus efeitos ambíguos, tanto incentivadores da atividade inovativa quanto restritivos da concorrência (MELLO, 2010) são os principais alvos de ciberataques para espionagem industrial e desvio de informações com potencial significativo de dano à soberania nacional.

Com base nas definições da economia do conhecimento e da sociedade, e o papel dessas tecnologias de comunicação da informação examinadas, além do estudo direcionado a verificar se as formas de proteção e controle da PI mudaram nessa nova configuração de sociedade, enfatizou-se o papel da inovação, via capital humano, com uma maior confiança nas capacidades intelectuais e com isso, no debate sobre a "economia e sociedade do conhecimento" verificou-se que o papel da PI, portanto, permanece central, mas agora é desafiado pelo surgimento de novas formas de comunicação, que dificultam sua proteção e movem grande parte da preocupação com relação à regulação para um nível global e não somente nacional e local (MACHLUP, PENROSE, 1950).

Os sistemas, projetos de *Offset*, acordos de compensação baseados em transferência de tecnologia previstos no inciso VIII do artigo 2°, da Lei 12.598/2012 e outros ativos industriais representados por direitos de propriedade industrial, podem ser alvo de ciberataque para obtenção de informação privilegiada, vantagem competitiva indevida e prática de concorrência desleal.

Para fins de implementação da Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) consideram-se no seu artigo 4º, como diretrizes, dentre outras, a integração com outras políticas de Estado, incluídos os seus sistemas de gerenciamento e monitoramento; a cooperação entre órgãos e entidades federais, estaduais, distritais e municipais nas ações necessárias à implementação e à manutenção da segurança das infraestruturas críticas, dentre eles o Instituto Nacional da Propriedade Industrial (INPI), Ministério da Economia e Ministério da Defesa, bem como o incentivo à cooperação e à realização de parcerias entre o setor público e privado, com vistas a elevar o nível de segurança das infraestruturas críticas – Empresas Estratégicas de Defesa (EED) e Instituição Científica e Tecnológica (ICT), Órgão ou Entidade da Administração Pública, definidos nos termos do inciso V do caput do art. 2º, da Lei nº 10.973, de 2 de dezembro de 2004.

Em 22 de novembro de 2018 o Decreto n. 9.573 aprovou a PNSIC e definiu como um dos seus princípios a integração entre as diferentes esferas do Poder Público, o setor empresarial e os demais segmentos da sociedade.

Sendo a Segurança Cibernética (SegCiber) a área mais crítica e atual a ser abordada pela Política Nacional de Segurança da Informação (PNSI): Decreto nº 9.637 de 26 de dezembro de 2018, e, de acordo com o Decreto 10.222 de 05 de fevereiro de 2020, que aprovou a Estratégia Nacional de Segurança Cibernética (E-Ciber) com validade no quadriênio

até 2023 e sendo o Setor Cibernético e Espacial estratégicos para a Defesa Nacional Lei Complementar n. 97 de 9 de Junho de 1999 e Lei Complementar n. 136 de 25 de agosto de 2010, uma vez que, respectivamente, abrangem desde a proteção de infraestruturas críticas através da salvaguarda de dados sensíveis até o desenvolvimento e produção de veículos aeroespaciais, passaram a integrar a lista de alvos dos cibercriminosos que diuturnamente buscam obter informações e dados sigilosos utilizando os sistemas informacionais críticos da Administração Pública Federal, tanto para espionagem industrial como para desvio de informações com potencial significativo de dano à soberania nacional.

O setor de aeroespaço e defesa (A&D) ou simplesmente aeroespacial apresenta características próprias de desenvolvimento e importância comercial capazes de atrair o interesse de vários Estados nacionais. A articulação que se verifica na cadeia produtiva aeroespacial entre diversos atores, abrangendo os setores públicos e privados em um país, também tem rebatimento entre estes e seus pares em outras nações. O mercado do setor é global e requer uma constante atenção à sua evolução. Além disso, o setor de A&D colabora para o desenvolvimento do país, posto que a aplicação de tecnologias inovadoras ocorre de forma transversal nas esferas militar e civil, e o produto final, uma aeronave, tem alto valor agregado para exportação (GOMES *et al*., 2017)

Além da aviação na esfera militar, a aviação civil também é alvo recorrente de interferências ilícitas. Nessa área, a ameaça cibernética é real e poderia resultar em episódio classificável como “cisne negro”, nos moldes dos ataques terroristas de 11 de setembro de 2001. A ameaça do ataque cibernético no Setor Aeroespacial contempla também a irrefutabilidade de possíveis falhas, os alvos potenciais, as categorias de atores e suas motivações, a capacidade de agir e os possíveis métodos de ataque (SILVA, 2019).

O Setor Cibernético, um dos três setores de importância estratégica para a Defesa do País Nacional segundo as diretrizes estabelecidas pela Estratégia Nacional de Defesa (END, 2020), foi introduzido no âmbito da Força Terrestre, tendo o Centro de Defesa Cibernética (CDCiber) como órgão encarregado de coordenar e integrar os esforços dos vetores vocacionados para esse campo de atuação (EPEX, 2017)

A Política Nacional de Defesa (PND) – aprovada originalmente pelo Decreto 5484 de 30 de junho de 2005, atualizada em 2012 e apresentada nova versão em julho de 2020 – é o principal documento de planejamento da defesa do país. Ele estabelece objetivos e diretrizes para o preparo e emprego da capacitação nacional, com o envolvimento dos setores militar e

civil, em todas as esferas de poder. A END (Decreto 6.703 de 18 de dezembro de 2008), por sua vez, pretende definir como fazer o que se determinou na PND. Já o chamado Livro Branco de Defesa Nacional (LBDN), criado pela Lei Complementar nº 136, de 25 de agosto de 2010, segundo a qual os três documentos devem ser enviados ao Legislativo a cada quatro anos, com suas respectivas atualizações, a partir de 2012, apresenta uma visão geral da defesa e das Forças Armadas, tendo como principal propósito permitir transparência, promovendo assim a confiança mútua entre os países (MD, 2020).

A END, na sua formulação sistemática no seu primeiro item informa que Estratégia nacional de defesa é inseparável de estratégia nacional de desenvolvimento (BRASIL, 2008). Ainda no item 4 deste dispositivo, assim declara: "Projeto forte de defesa favorece projeto forte de desenvolvimento." E para ser forte o Projeto deve ser guiado por princípios que incluem, dentre eles na alínea b: "Independência nacional, alcançada pela capacitação tecnológica autônoma, inclusive nos estratégicos setores espacial, cibernético e nuclear. Não é independente quem não tem o domínio das tecnologias sensíveis, tanto para a defesa como para o desenvolvimento".

Organizada em três eixos estruturantes. Ao lado da destinação constitucional, das atribuições, da cultura, dos costumes e das competências próprias de cada Força e da maneira de sistematizá-las em estratégia de defesa integrada, aborda-se na END, o papel de três setores decisivos para a defesa nacional: o espacial, o cibernético e o nuclear.

Descrevem-se na END como as três Forças devem operar em rede - entre si e em ligação com o monitoramento do território, do espaço aéreo e das águas jurisdicionais brasileiras. O primeiro deles refere-se à Forças Armadas para transformar suas diretrizes em prática a partir de capacitações operacionais e a linha de evolução tecnológica necessária, o segundo eixo estruturante refere-se à reorganização da indústria nacional de material de defesa, para assegurar que o atendimento das necessidades de equipamento das Forças Armadas apoie-se em tecnologias sob domínio nacional e por fim, o terceiro eixo estruturante versa sobre a composição dos efetivos das Forças Armadas (BRASIL, 2008).

Com a finalidade de viabilizar a implementação estratégica, a Portaria Normativa n° 86/GM-MD, de 13 de dezembro de 2018, estabelece procedimentos administrativos para o credenciamento, descredenciamento e a avaliação de ED, EED e para a classificação e desclassificação de Produtos de Defesa (PRODE), e Produtos Estratégicos de Defesa (PED).

Na década de 1990, foi desenvolvido o modelo de tripla hélice como uma metáfora para explicar a capacidade de transformar conhecimento científico em inovação tecnológica, com base na interação motivada a partir de um ator como "motor". A proposta base traz a ideia de que a inovação tecnológica só é possível no momento em que o conhecimento desenvolvido nas universidades é canalizado para atender demandas econômico-sociais que as entidades privadas e empresas analisam, gerenciam e, posteriormente comercializam, com o apoio de políticas públicas que visem coordenar o desenvolvimento do potencial de setores e regiões e gerir os modelos contratuais das parcerias entre os diferentes atores (incluindo as patentes) (ETZKOWITZ, 2008).

Nessa perspectiva, os atores (governos, indústria e universidades) precisam aumentar sua interação para criar inovações que contribuam para o desenvolvimento econômico, a competitividade e o bem-estar social. As relações entre universidade-indústria-governo são vistas como estratégicas para incentivar a dinâmica da inovação, contudo, essa tríade recebeu novos atores que fortalecem o processo de geração de inovação e conhecimento, considerados os aspectos para um desenvolvimento sustentável. A forma de relacionamento entre esses atores no cenário global expandiu ao longo do tempo. A tradicional tríade formada por universidade-indústria-governo vem sendo fortalecida com novos modelos de geração do conhecimento, incluindo-se a sociedade (Hélice Quádrupla - HQ) e o ambiente (Hélice Quíntupla) com hélices importantes na dinâmica da inovação (MINEIRO *et al*., 2018).

Exatamente essa interação, só que dessa vez, como no Sistema de Inovação, seria capitaneada pela indústria, principal interessado na proteção jurídica à PI dos ativos industriais e técnicos que coloca à disposição nos ajustes de salvaguarda das Estruturas Críticas nos Setores Cibernético e Aeroespacial, e poderia provocar uma revisão sistemática da efetividade da Tríplice à Quíntupla Hélice no Setor Aeroespacial.

A aplicação do modelo das hélices dar-se-ia no desenvolvimento de soluções, desde a comunicação cibernética de aeronaves aos demais produtos de defesa, como para o desenvolvimento de mecanismos de prevenção aos ataques cibernéticos e aperfeiçoamento legislativo no combate de tais práticas na Estratégia Nacional de Defesa – especialmente tecnologias sensíveis de uso dual.

3 Principais Riscos aos Sistemas Informacionais da Administração Pública Federal

Segundo levantamento do Serviço de Inteligência Fortiguard (2019), divulgado na 4ª edição do *Fortinet Cibersecurity Summit* (FSC19), entre março e junho de 2019 o Brasil já havia sofrido 15 bilhões de ataques cibernéticos. Entre os 10 (dez) principais ataques cibernéticos à propriedade intelectual na Administração Pública, estão: i) *o backdoor*, um tipo de cavalo de Troia para acessar máquinas por meio da infecção de sistemas e apps; ii) o *phishing,* método no interior da linha de engenharia social que se aproveita da confiança depositada por um usuário para roubar seus dados – o cibercriminoso se passa por uma pessoa ou instituição legítima para enganar o usuário, por isso, *o phishing* pode acontecer de diversas formas, seja em conversas de mensageiros instantâneos, seja em *links* de e-mails falsos; iii)o *spoofing* está relacionado com à falsificação de endereços de IP, de DNS e de *e-mails*; iv) a *manipulação de URL* de alguns *hackers* para fazer o servidor transmitir páginas às quais ele não teria autorização de acesso; v) o *ataque DoS*, traduzido como *negação de serviço*, que sobrecarrega um servidor ou um computador com um alto volume de pedidos de pacotes. Por não conseguir lidar com as requisições, o sistema não consegue mais responder, ficando indisponível, mas neste caso não há invasão; vi) o DDoS (*Distributed Denial of Service*). O ataque de negação de serviço distribuído compartilha os pedidos para várias máquinas; vii) o *Ataque DMA (Direct Memory Access),* ataque de Acesso Direto à Memória, uma função que permite ao *hardware* da máquina ter um acesso direto à memória RAM sem passar pelo processador, acelerando, assim, a taxa de transferência e o processamento do computador; viii) o *eavesdropping,* em que o *hacker* utiliza diferentes sistemas de *e-mail*, mensagens instantâneas e telefonia, além de serviços de internet, para violar a confidencialidade da vítima; ix) o *decoy,* em que o *hacker* simula um programa legítimo, em que o usuário faz o *login* e o programa armazena suas informações, que poderão ser utilizadas pelo atacante; e x) o *Shoulder surfing* é uma expressão da língua inglesa que significa "*espiar sobre os ombros*", ato de olhar a tela de um usuário enquanto ele acessa dados sigilosos (UNYLEYA, 2020).

Em maio de 2017, foi noticiada, na imprensa nacional uma onda de ataques cibernéticos iniciados em empresas europeias, que, ganhando proporções continentais teve reflexos no Brasil, pois várias empresas e órgãos públicos foram atingidos pelo vírus *WannaCry*. (MELODY *et al.*, 2017), que interrompeu as atividades regulares em diversos órgãos Públicos como o INSS e o Tribunal de Justiça de São Paulo.

O sítio da *internet* sobre o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) apresenta em seu histórico que existiam alguns grupos de resposta de

incidentes isolados dentro da Administração Pública Federal (APF), mas, face às novas necessidades decorrentes da sociedade da informação, o GSI/PR por meio da Portaria nº 12, de 27 de junho de 2003, instituiu a criação de sete grupos de trabalho para adequar os órgãos da APF à nova realidade. Mais tarde, a Portaria nº 56, de 05 de novembro de 2009, deu competência à Coordenação-Geral de Tratamento de Incidentes de Rede e denominou o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da APF de CTIR Gov.

O CTIR Gov está enquadrado na categoria "CSIRT de responsabilidade nacional de coordenação" e tem por objetivo coordenar e integrar as ações destinadas à gestão de incidentes computacionais em órgãos ou entidades de quaisquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios, bem como: prevenir, monitorar, analisar e mitigar os incidentes de segurança da informação; promover o intercâmbio científico-tecnológico; participar da articulação, para o estabelecimento de diretrizes sobre gestão de incidentes computacionais; e criar processo de inteligência de ameaças cibernéticas para subsidiar criação de políticas públicas e tomada de decisão em nível decisório (CTIR, 2020).

O Centro de Tratamento de Incidentes de Redes da Força Aérea Brasileira se chama (CTIR.FAB) e atualmente, está ativo na defesa de diversos ataques de criminosos que, aproveitando da pandemia do COVID-19, vêm aplicando golpes ou campanhas de *malwares*, principalmente em hospitais e centros de tratamento (INCAER, 2020).

Uma analogia com o Sistema de Inovação e o modelo das hélices no Setor Cibernético e Espacial poderia nascer daqui, a exemplo do Centro de Pesquisa e Inovação Sueco Brasileiro (CISB), SAAB e do *Computer Security Incident Response Team* (CSIRT).

O CISB é uma associação privada sem fins lucrativos que atua como um *hub* internacional para promover o diálogo e oferecer um ambiente propício de colaboração entre Suécia e Brasil. Seu principal objetivo é identificar e apoiar iniciativas de desenvolvimento de projetos que envolvam tecnologias avançadas para entregar soluções a uma série de setores da indústria, impactando positivamente a sociedade como um todo no modelo indústria-academia-governo (CISB, 2020).

Uma vez que o CSIRT é um grupo técnico responsável pela resolução incidentes relacionados à segurança em sistemas computacionais, e este pode ser um serviço prestado por empresas e projetos multidisciplinares, caso estes *players* se interessarem por

desenvolver soluções sob medida para prevenção de novos incidentes, poderiam inaugurar e impulsionar o modelo baseado nas hélices entre os Setores.

4 Estrutura metodológica e resultados do "Levantamento de Riscos em Sistemas Informacionais da Administração Pública Federal" – Tribunal de Contas da União (TCU)

Para desenvolvimento deste artigo foram realizadas pesquisas documentais, especialmente a Base de dados abertos do Governo Federal, com consulta à lista de produtos de Defesa do Ministério da Defesa – MD e ao Relatório de fiscalização denominado Levantamento de Riscos em Sistemas Informacionais da APF, autorizada por meio do Acórdão 2.077/2019 – TCU - Plenário no âmbito do processo administrativo TC 022.454/2019-5 ao Acórdão - TC 031.436/2019-6.

Foi realizada a revisão da literatura de Introdução à Propriedade Intelectual, Economia do Conhecimento e Inovação, Crimes Cibernéticos e à Proteção de infraestruturas críticas por meio da salvaguarda de dados sensíveis até o desenvolvimento e a comunicação cibernética na produção de veículos aeroespaciais por meio da PND e END também foi realizada, além da revisão da legislação vigente que abarcou a Lei de Inovação, Estratégia Nacional de Segurança Cibernética, com análise da Lei Geral da Proteção de Dados (LGPD) à Instrução Normativa n° 02/GSI de 24 de julho de 2020 que alterou a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal teve igualmente seu espaço.

A partir de entrevistas na Divisão de Coordenação da Indústria de Defesa do Ministério da Defesa (DIVICID) em setembro de 2020 (presencial), na divisão de cadastramento das EED e com a Vice-Presidência da Associação Brasileira das Indústrias de Materiais de Defesa e Segurança (ABIMDE), em julho de 2020 (teleconferência), foram reveladas que há muitas oportunidades ainda não aproveitadas pelas empresas da área de Defesa, especialmente as surgidas a partir das Políticas Públicas. Tendo em vista que os produtos de defesa passam pelo Centro de Catalogação das Forças Armadas (CASLOD), a Base Industrial de Defesa (BID) pode beneficiar-se, contribuindo com novas iniciativas para desenvolvimento de produtos de natureza cibernética estratégicos para o país.

Recente fiscalização denominada "Levantamento de Riscos em Sistemas Informacionais da Administração Pública Federal", autorizada por meio do Acórdão 2.077/2019", realizada pelo Tribunal de Contas da União em 58 (cinquenta e oito) órgãos de sua estrutura da Administração direta, indireta, autárquica e fundacional, participantes do

Sistema de Administração dos Recursos de Tecnologia da Informação, dentre eles, Agência Espacial Brasileira, Instituto Nacional da Propriedade Industrial, Ministério da Ciência, Tecnologia, Inovações e Comunicações; Ministério da Defesa; Ministério da Defesa – Comando da Aeronáutica, Ministério da Defesa – Comando do Exército e Ministério da Economia, apontou que, entre os 71% dos sistemas classificados como críticos, 22,2% estão nas secretarias de controle externo da Defesa (TCU, 2020).

Nesse levantamento foi desenvolvido um modelo de avaliação de criticidade de sistemas de informação, que contempla as seguintes etapas, conforme demonstrado na Figura abaixo, do Acórdão acima referenciado.

Figura 10 – Modelo de avaliação de criticidade de sistemas de informação

Fonte: TCU, 2020

Na lista de produtos de Defesa do MD, atualizada em 08 de julho de 2020, já podem ser localizados alguns exemplos de produtos cibernéticos:

Quadro 8 – Exemplos de produtos cibernéticos.

EMPRESA/PRODUTO	CLASSIFICAÇÃO	DATA
AXUR - Fiscalização da *Internet* e Reação a Ameaças Cibernéticas (CIBERPROTECTION)	EED	28/5/2014
RUSTICON - Simulador de Operações Cibernéticas (SIMOC)	EED	28/5/2014
NS PREVENTION - Hades - Plataforma de Inteligência Cibernética (PIC-NSP)	EED	19/7/2017
PIQL - Sistema PIQL de Defesa Cibernética	EED	11/1/2018

Fonte: a autora.

Esse quadro demonstra um cenário, ainda que incipiente, como oportunidades para desenvolvimento do mercado de segurança cibernética.

5 Os desafios no tratamento e resposta aos incidentes da Segurança da Informação e as oportunidades para a indústria de Defesa

Demonstrar vulnerabilidade a incidentes da Segurança da Informação não significa fragilidade, mas possibilidade de transformação.

Desde o ano de 2016, o TCU, que tem por missão aprimorar a Administração Pública em benefício da sociedade por meio do controle externo, apontou governança deficiente no setor espacial brasileiro e retrata investimento insuficiente no setor. Dos sistemas analisados pela fiscalização, 22,2% dos sistemas foram classificados como críticos e estão nas secretarias de controle externo da Defesa. Os sistemas, projetos de *offset* e outros ativos industriais representados por direitos de propriedade industrial podem ser alvo de ciberataque para obtenção de informação privilegiada, vantagem competitiva indevida e prática de concorrência desleal.

Novas oportunidades para as EED podem surgir da aplicação da metodologia PbD nos processos de homologação e certificação dos produtos de natureza cibernética também para uso na comunicação cibernética de aeronaves aos demais produtos de defesa.

Em 2019, para incrementar os níveis de segurança cibernética de equipamentos e dispositivos importantes para a segurança e a defesa nacional, o Inmetro e o Exército Brasileiro trabalharam no estabelecimento de um programa de avaliação de riscos e conformidade denominado Sistema Nacional de Certificação e Homologação de Produtos de Defesa Cibernética (SHCDCiber), em que foi assinado um Termo de Execução Descentralizada (TED) entre o Inmetro e o Departamento de Ciência e Tecnologia do Exército (INMETRO, 2019).

De acordo com a END, na parte de reorganização da indústria nacional de material de defesa nos itens 5, 6 e 7 assim diz:

> 5. O futuro das capacitações tecnológicas nacionais de defesa depende mais da formação de recursos humanos do que do desenvolvimento de aparato industrial. Daí a primazia da política de formação de cientistas, em ciência aplicada e básica, já abordada no tratamento dos setores espacial, cibernético e nuclear.
> 6. No esforço de reorganizar a indústria nacional de material de defesa, buscar-se-á parcerias com outros países, com o objetivo de desenvolver a capacitação tecnológica nacional, de modo a reduzir progressivamente a compra de serviços e de produtos acabados no exterior. A esses interlocutores estrangeiros, o Brasil deixará sempre claro que pretende ser parceiro, não cliente ou comprador. O País está mais interessado em parcerias que fortaleçam suas capacitações independentes do que na compra de produtos e serviços acabados. Tais parcerias devem contemplar, em princípio, que parte substancial da pesquisa e da fabricação seja desenvolvida no Brasil e ganharão relevo maior quando forem expressão de associações estratégicas abrangentes.

> 7. Estabelecer-se-á, no Ministério da Defesa, uma Secretaria de Produtos de Defesa. O Secretário será nomeado pelo Presidente da República, por indicação do Ministro da Defesa.

Conforme apresentado na Seção 3, há ainda muito espaço para o desenvolvimento de parcerias estratégicas para desenvolvimento de produtos e serviços no mercado. Faz-se necessária, então, a criação de ambientes de inovação capitaneados pela indústria à luz de uma revisão da efetividade da Tríplice à Quíntupla Hélice no Setor Aeroespacial para prevenção aos ataques cibernéticos e aperfeiçoamento legislativo no combate de tais práticas na Estratégia Nacional de Defesa – especialmente tecnologias sensíveis de uso dual.

Tendo em vista que o CTIR Gov é um CSIRT, ou Grupo de Resposta a Incidentes de Segurança, que vem a ser uma organização responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores, há muito espaço para contribuições e parcerias.

O conjunto de serviços providos pelo CTIR Gov à APF pode ser dividido em: Notificação de Incidentes; Análise de Incidentes; Suporte à Resposta a Incidentes; Coordenação na Resposta a Incidentes; Distribuição de Alertas, Recomendações e Estatísticas; Cooperação com outras Equipes de Tratamento de Incidentes.

Recente Instrução Normativa Nº 2, de 24 de julho de 2020 do GSI/PR alterou a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, e prevê a criação nos artigos 16 e 22 de uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) ou estrutura equivalente.

Atualmente, há catalogação de alguns produtos cibernéticos, mas há o desafio de, além de criar novos produtos e serviços fundados nos princípios de PbD (CAVOUKIAN, 2009), criar modelos de maturidade e de certificação desses produtos.

O Projeto de Desenvolvimento de Sistemas de Certificação de Produtos de Defesa Cibernética entre o Inmetro e o Exército Brasileiro abriu igualmente espaço para novas possibilidades e, consequentemente, espaço para novas oportunidades à indústria de Defesa.

A inovação e o aperfeiçoamento do Sistema Militar de Defesa Cibernética (SMDC) demandam estudos e pesquisas específicos em áreas como Pesquisa Operacional, Engenharia de Sistemas, Estruturação e Solução de Problemas Complexos, dentre outras.

No dia 03 de novembro, no Instituto Tecnológico de Aeronáutica (ITA), em São José dos Campos – SP, organização do Departamento de Ciência e Tecnologia Aeroespacial (DCTA) do Comando da Aeronáutica (COMAER), o Exército Brasileiro, representado pelo Comando de Defesa Cibernética (ComDCiber), firmou acordo com o ITA, estabelecendo uma parceria entre as duas instituições com vistas à inovação e ao aperfeiçoamento do SMDC (ITA, 2020). Essa parceria foi realizada em decorrência da assinatura de um TED, que tem por objeto estabelecer a parceria entre o Comando de Defesa Cibernética e o Instituto Tecnológico de Aeronáutica para obtenção da modelagem e da definição dos requisitos para o Sistema Militar de Defesa Cibernética.

Tendo em vista que a parceria entre o ComDCiber e o ITA pretende, ao final, entregar soluções e produtos concretos para problemas operacionais reais e atuais na esfera militar da defesa cibernética, ao definir como um dos seus princípios a integração das diferentes esferas do Poder Público, do setor empresarial e dos demais segmentos da sociedade, o Decreto 9.573 que aprovou a PNSIC, abre espaço para o desenvolvimento do modelo das hélices para os segmentos Aeroespacial e Cibernético.

As soluções existentes e propostas pela indústria de defesa, especialmente as aplicadas à Administração Pública, nos recentes ataques cibernéticos sofridos em 2020, são realmente aptas à defesa da Propriedade Intelectual contra *cyberattacks* nas infraestruturas do Setor Aeroespacial Brasileiro?

Ao informar que os processos de homologação e certificação dos produtos de natureza cibernética podem gerar oportunidades para a indústria de defesa, a literatura propõe parâmetros essenciais para estruturar um panorama da ameaça cibernética como fenômeno que interage e desafia a inteligência da aviação?

Tendo em vista que a Estratégia Nacional de Defesa é inseparável da Estratégia Nacional de Desenvolvimento e a experiência CISB que apresentou sucesso na Tríplice Hélice, partindo das soluções existentes das EED, seriam as teorias relacionadas ao modelo de hélices e as principais funcionalidades para as Hélices Quádrupla, Quíntupla e Sêxtuplas aplicáveis ao Setor Cibernético e Espacial, gerando verdadeiramente oportunidades?

6 Considerações finais

Os resultados incipientes apresentados intencionam retratar e sistematizar diversas soluções a serem implementadas, dentre outras diretrizes, propor a integração com outras

políticas de Estado, incluídos os seus sistemas de gerenciamento e monitoramento; a cooperação entre órgãos e entidades federais, estaduais, distritais e municipais nas ações necessárias à implementação e à manutenção da segurança das infraestruturas críticas, dentre eles o INPI, Ministério da Economia e Ministério da Defesa, bem como o incentivo à cooperação e à realização de parcerias entre os setores público e privado, com vistas a elevar o nível de segurança das infraestruturas críticas tais como as EED e as ICT.

Os documentos citados definem o perfil global de atuação do país e, por isso, o investimento na defesa dos ativos críticos das Infraestruturas do Setor Aeroespacial Brasileiro, podem representar oportunidades para diversos setores da indústria de Defesa, especialmente das ED e EED.

Reportagem nacional veiculada no mês de setembro de 2020 informa que os ataques cibernéticos explodiram durante a pandemia e tendo em vista que expõe as vulnerabilidades das empresas, a segurança de dados passa a ganhar importância também no universo empresarial com previsão de custos da ordem de 6 (seis) trilhões de dólares à economia global em 2021 (MOURA *et al.*, 2020).

No dia 03 de novembro de 2020 o Superior Tribunal de Justiça (STJ) acionou a Polícia Federal para elucidar ataques cibernéticos que culminaram na interrupção das sessões de julgamento como medida de prevenção em virtude de hackers terem criptografados toda a base de dados do Tribunal e a empresa de suporte contratada afirmou não prestar serviços de *cyber* segurança ao STJ, embora consulta ao Sistema Integrado de Administração Financeira do governo federal (SIAFI) via ferramenta Siga Brasil tenha empenhado pelo menos R$ 40,6 milhões em gastos com empresas de tecnologia, incluindo serviços e compra de materiais (SHALDERS, 2020).

Atualmente há catalogação de alguns produtos cibernéticos, mas há o Desafio de além de criar novos produtos e serviços fundados nos princípios de PbD, o de criar modelos de maturidade e de certificação desses produtos. Essas sinalizações visam contribuir para validação e avanço da pesquisa, em especial para os estudos do grupo focal de especialistas em Inovação e Propriedade Intelectual para o Setor de Defesa, para o desenvolvimento de mecanismos de prevenção aos ataques cibernéticos e aperfeiçoamento legislativo no combate de tais práticas.

Referências

ABIMDE. *Associação Brasileira das Indústrias de Materiais de Defesa e Segurança* Disponível em: http://www.abimde.org.br/abimde-diretoria. Acesso em: 04 nov. 2020.

BARBALHO, Sanderson César M.; MONTEIRO, Simone Borges S.; REIS, Ana Carla Bittencourt; MIRANDA, Rhoxanna Crhistianth F. Diagnóstico dos processos de homologação e certificação de produtos de natureza cibernética: perspectivas para a construção de um Sistema Nacional. *Revista Produção Online*. Florianópolis, SC, v. 18, n. 2, p. 424-453, 2018.

BID. *Base Industrial de Defesa*. Disponível em:https://www.gov.br/defesa/pt-br/assuntos/industria-de-defesa/base-industrial-de-defesa. Acesso em: 03 nov. 2020.

BRASIL. *Lei Complementar n° 97 de 9 de junho de 1999*. Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp97.htm. Acesso em: 04nov. 2020.

BRASIL. *Lei Complementar 136 de 25 de agosto de 2010*. Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas, para criar o Estado-Maior Conjunto das Forças Armadas e disciplinar as atribuições do Ministro de Estado da Defesa. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp136.htm. Acesso em: 04 nov. 2020.

BRASIL. *Lei nº 10.973, de 2 de dezembro de 2004*. Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/l10.973.htm. Acesso em: 04 nov. 2020.

BRASIL. *Lei 12.598 de 21 de março de 2012*. Estabelece normas especiais para as compras, as contratações e o desenvolvimento de produtos e de sistemas de defesa; dispõe sobre regras de incentivo à área estratégica de defesa; altera a Lei nº 12.249, de 11 de junho de 2010; e dá outras providências. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12598.htm#:~:text=Estabelece%20normas%20especiais%20para%20as,2010%3B%20e%20d%C3%A1%20outras%20provid%C3%AAncias. Acesso em: 03 nov. 2020.

BRASIL. *Lei 12.737 de 30 de novembro de 2012*.Dispõe sobre a tipificação criminal de delitos informáticos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 04 nov. 2020.

BRASIL. *Decreto-lei no 2.848, de 7 de dezembro de 1940*.Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.Acesso em: 04nov. 2020.

BRASIL. *Decreto nº 5484 de 30 de junho de 2005*. Aprova a Política de Defesa Nacional, e dá outras providências. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/decreto/d5484.htm. Acesso em: 04 nov. 2020.

BRASIL. *Decreto nº 6703 de 18 de dezembro de 2008*. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm. Acesso em: 04 nov. 2020.

BRASIL. *Decreto 7.970 de 28 de março de 2013*. Regulamenta dispositivos da Lei nº 12.598, de 22 de março de 2012, que estabelece normas especiais para as compras, as contratações e o desenvolvimento de produtos e sistemas de defesa. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7970.htm. Acesso em: 04 nov. 2020.

BRASIL. *Decreto nº 9.573, de 22 de novembro de 2018*. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm. Acesso em: 03 nov. 2020.

BRASIL. *Decreto nº 9.637 de 26 de dezembro de 2018*. Institui a Política Nacional de Segurança da Informação. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso em: 04 nov. 2020.

BRASIL. *Decreto 10.222 de 05 de fevereiro de 2020*. Aprova a Estratégia Nacional de Segurança Cibernética. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm. Acesso em: 03 nov. 2020.

BRASIL. Portaria nº 2 de 08/02/2008 / GSIPR - Gabinete de Segurança Institucional da Presidência da República (D.O.U. 11/02/2008). Infraestruturas Críticas (GTSIC). Disponível em: https://www.diariodasleis.com.br/legislacao/federal/198823-infra-estruturas-cruticas-gtsic-institui-grupos-tucnicos-de-seguranua-de-infra-estruturas-cruticas-gtsic-e-du-outras-providuncias.html. Acesso em: 03 nov. 2020.

BRASIL. Portaria Normativa n° 86/GM-MD, de 13 de dezembro de 2018*Estabelece procedimentos administrativos para o credenciamento, descredenciamento e avaliação de Empresas de Defesa - ED, Empresas Estratégicas de Defesa - EED e para a classificação e desclassificação de Produtos de Defesa - PRODE, e Produtos Estratégicos de Defesa – PED.* Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/55442911/do1-2018-12-17-portaria-normativa-n-86-gm-md-de-13-de-dezembro-de-2018-55442698. Acesso em: 04 nov. 2020.

BRASIL. *Instrução Normativa n° 02/GSI de 24 de julho de 2020*. Altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-2-de-24-de-julho-de-2020-268684700. Acesso em: 04 nov. 2020.

CAVOUKIAN, Ann. *Privacy by Design - The 7 Foundational Principles*: Implementation and Mapping of Fair Information Practices. Agosto de 2009. Disponível em:

https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf. Acesso em: 3 nov. 2020.

CISB. *Centro de Pesquisa e Inovação Sueco-Brasileiro. 2020.* Disponível em: http://cisb.org.br/pt/. Acesso em: 04 nov. 2020.

CTIR. *Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo*. 2020. Disponível em: https://www.ctir.gov.br/sobre/#procedimento. Acesso em: 04 nov. 2020.

CTIR.FAB. *Centro de Tratamento de Incidentes de Rede.* 2020. Disponível em:https://www2.fab.mil.br/ctir/index.php/missao-visao-e-valores. Acesso em: 04 nov. 2020.

ETZKOWITZ, Henry; DZISAH, James. Triple Helix Circulation: the heart of innovation and development*. International Journal of Technology Management & Sustainable Development*, v.7, n.2, p.101-15, 2008.

EPEX. Escritório de Projetos do Exército Brasileiro. *Liberdade de Ação no Espaço Cibernético.* Disponível em: http://www.epex.eb.mil.br/index.php/defesa-cibernetica. Acesso em: 03 nov. 2020.

FORTINETCYBERSECURITYSUMMIT BRASIL 2019. Disponível em: https://eventostech.com.br/index.php/event/fortinet-cybersecurity-summit-brasil-2019/. Acesso em: 04 nov. 2020.

FORTIGUARD*.* Disponível em: *https://fortifirewall.com.br/Fortiguard/c/84/.* Acesso em: 04 nov. 2020.

INCAER. *Phishing relacionado ao Covid-19.* Disponível em:https://www2.fab.mil.br/incaer/index.php/slideshow/773-phishing-relacionado-ao-covid-19. Acesso em: 04 nov. 2020.

LIMA, Carlos Rodrigues. VALENTINA, Marcelino. Cibersegurança lançou alerta para administração pública. *Diário de Notícias*, 2017. Disponível em: https://www.dn.pt/sociedade/cibersegurança-lancou-alerta-para-administracao-publica-8475868.html. Acesso em: 03 out. 2020.

GANDELMAN, Marisa. *Poder e conhecimento na economia global:* O regime internacional da Propriedade Intelectual da sua formação àsregras de comércio atuais. Editora Record, 2004. (cap. 4).

GOMES, Sérgio Bittencourt Varella; BARCELLOS, João Alfredo; FONSECA, Paulo Vinicius da Rocha. O apoio ao Desenvolvimento do Setor de aeroespaço e Defesa: visões da experiência internacional*.* Aeroespaço e defesa; *BNDES Setorial,* 45, p. 7-55, mar. 2017.

INMETRO. Inmetro vai desenvolver sistema de certificação de produtos de defesa cibernética. 2019. Disponível em: https://www4.inmetro.gov.br/node/4454. Acesso em: 02 out. 2020.

ITA. O Instituto Tecnológico de Aeronáutica. Disponível em: http://www.ita.br/noticias/itafirmaacordocomcomandodedefesacibernticadoexrcito. Acesso em: 05 nov. 2020.

MD – Ministério da Defesa. *Acesse aqui a Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END) encaminhadas, em 22 de julho de 2020, para apreciação do Congresso Nacional.* Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/politica-nacional-de-defesa. Acesso em: 04 nov. 2020.

MD. *Produtos de Defesa do MD.* Disponível em: https://dados.gov.br/dataset/produtos-de-defesa. Acesso em: 04 nov. 2020.

MELLO, Maria Tereza Leopardi. Propriedade Intelectual e Concorrência*. Revista Brasileira de Inovação*, [S.l.], v. 8, n. 2 jul/dez, p. 371-402, mar. 2010.

MELODY. Luana B. HESSEL. Rosana. *Onda mundial de ciberataques atinge INSS, Petrobras e tribunais.* Vírus WannaCry se espalhou por computadores de, pelo menos, 74 países, além do Brasil. Disponível em: https://www.correiobraziliense.com.br/app/noticia/economia/2017/05/13/internas_economia,594753/onda-mundial-de-ciberataques-atinge-inss-petrobras-e-tribunais.shtml. Acesso em: 03 nov. 2020.

MINEIRO, Andrea A da Costa; SOUZA, Donizete Leandro; VIEIRA Kelly Carvalho; CASTRO, Cleber Carvalho; BRITO, Mozart José. Da Hélice Tríplice A Quíntupla: Uma Revisão Sistemática*. E&G Economia e Gestão*, Belo Horizonte, v. 18, n. 51, Set./Dez. 2018

MOURA, Marcelo. HAIDAR. Daniel. Os ataques cibernéticos explodem durante pandemia e expõe vulnerabilidade das empresas*. Revista Eletrônica Época Negócios*. 23 set de 2020. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2020/09/os-ataques-ciberneticos-explodem-durante-pandemia-e-expoem-vulnerabilidades-das-empresas.html. Acesso em: 03 nov. 2020.

NUNES, Paula, M.S et al. *A eficiência da Propriedade Intelectual como estímulo à inovação: uma revisão bibliográfica*. Instituto de Economia. UFRJ.TD. 001/2009.

MACHLUP, Fritz & PENROSE, Edith. *The Patent Controversy in the Nineteenth Century. The Journal of Economic History.* New York, Economic History Association, v. 10, n.1, p. 1-29, May 1950.

RAMELLO, Giovanni B. What's in a sign? Trademark law and economic theory*. Journal of Economic Surveys*, v. 20, n. 4, p. 547-565, 2006.

SHALDERS, André. Alvo de ataque hacker, STJ gastou R$ 13,7 milhões com empresa de informática investigada. *BBC News Brasil em Brasília*. 06 de novembro de 2020. Disponível em: https://www.bbc.com/portuguese/brasil-54847723.amp. Acesso em: 07 nov. 2020.

SILVA, Mateus Vidal Alves. Panorama da ameaça cibernética à aviação civil. *RBI - Revista Brasileira de Inteligência*. Brasília: Abin, n. 14, dez. 2019.

TCU. Tribunal de Contas da União. Relatório de levantamento. Desenvolvimento de metodologia para identificação de sistemas críticos. Avalição da capacidade do TCU em auditá-los. Produção de inteligência de apoio ao controle. Disponível em: https://pesquisa.apps.tcu.gov.br/#/documento/acordao-completo/*/NUMACORDAO%253A1889%2520ANOACORDAO%253A2020%2520PROC%253A03143620196/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0/%2520?uuid=732b6910-0a23-11eb-8e7b-d16c381817c6. Acesso em: 20 out. 2020.

UNYLEYA. *Conheça os 10 principais ataques cibernéticos da atualidade*. Rock Convert. 15 de janeiro de 2020. Disponível em: https://blog.unyleya.edu.br/bitbyte/ataques-ciberneticos/. Acesso em: 03 out. 2020.

WIPO – *What is Intellectual Property?* 2020. Disponível em: https://www.wipo.int/about-ip/en/. Acesso em: 05 out. 2020.

A LGPD, riscos cibernéticos e o “seguro cibernético"

Patricy Barros Justino

Érica Maia Campelo Arruda

Resumo: O presente trabalho tem o objetivo de analisar o crescente aumento de demanda pelo “seguro cibernético”, seja pelos riscos cibernéticos cuja incidência se percebeu crescente, pela pandemia da COVID-19, pela mudança das novas formas laborais, seja pela entrada em vigor da LGPD. O crescimento da utilização dos meios tecnológicos, a rede mundial de computadores, a mudança das organizações e a própria mudança da sociedade modificaram a forma como a sociedade, os Estados e os negócios se comportam. Foi adotada uma metodologia comparada, fazendo um paralelo entre outros países que já implantaram leis de proteção de dados, em especial a União Europeia, que adotou o RGPD. A famosa frase proferida em 2006 pelo matemático inglês e especialista em ciência de dados Clive Humby, de que “dados são o novo petróleo” retrata a importância do dado nesta era do Big Data. Assim, vivemos em uma economia digital em que os dados são muito valiosos, as companhias de seguro e as organizações em geral estão vivendo o desafio da necessidade de contratação do “seguro cibernético”. Desta forma, a análise, no presente trabalho, do cenário atual, em especial da legislação em vigor no Brasil, na área cibernética, nos faz compreender mais este tema.

Palavras-chave: LGPD. Risco cibernético. Seguro cibernético.

1 Introdução

O crescimento da utilização dos meios tecnológicos, a rede mundial de computadores, a mudança das organizações e a própria mudança da sociedade, fizeram mudar a forma como a sociedade, os estados e os negócios se comportam. Como pontua Castells (2001, p. 22), quando o autor destaca que o fim do século XX foi marcado pela ocorrência de “substantivas mudanças tecnológicas concentradas nas tecnologias da informação que remodelaram a base material da sociedade, formatando novas formas de relação entre a economia, o Estado e a sociedade”.

Nesse contexto, um espaço de comunicação global, transcendendo fronteiras, fez surgir um novo “espaço”, sem dimensões, não físico, aproximando economias, culturas, países e regiões, por meio da *internet*: o ciberespaço, ou “espaço cibernético”. No entanto, essas novas potencialidades comportam também riscos e vulnerabilidades para a defesa e segurança nacional. Inevitavelmente, o desenvolvimento das tecnologias da informação e da comunicação (TIC) suscita algumas apreensões, no que toca ao desenvolvimento de conflitos e guerras, terrorismo e ameaças à segurança de infraestruturas. Para contextualização,

brevemente tratamos de algumas conceituações que são vistas ao longo do presente artigo. Inicialmente falemos de “espaço cibernético”.

Para Lévy (1999, p. 15-16), o conceito de “espaço cibernético” é:

> é o novo meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo.

Não podemos deixar de registrar uma afirmação recente do filósofo francês Lévy, em 26 de outubro de 2020, em que ele afirma: “Gigantes da web são novo Estado”. E continua: “As gigantes da web, como Google, Amazon, Facebook, Apple e Microsoft, adquiriram um poder extraordinário, algo que eu não havia pensado anos atrás. Elas têm um monopólio sobre a memória mundial e registram quase tudo que acontece na internet”. Para o filósofo, “muitas funções sociais e políticas, que são funções tradicionais dos Estados-nação, estão passando para essas companhias. Na minha avaliação, é uma nova forma de Estado, que eu denomino Estado-plataforma” (FERNANDES, 2020).

De acordo com Clarke e Knake (2015) o espaço cibernético é formado por todas as redes de computadores do mundo e tudo o que elas conectam e controlam, não só a internet.

Quanto às condutas ilícitas praticadas no meio virtual, estas podem receber várias denominações, entre as quais crime virtual, ilícito virtual, cibercrime, crime digital, crime informático, *cybercrime*, crime eletrônico, delito de computador, delito computacional, crime de computação, entre outros; tais termos no presente estudo serão tratados como sinônimos.

Rossini trata de ‘delitos informáticos’, afirmando que, dessa forma simples,

> abarcam-se não somente aquelas condutas praticadas no âmbito da internet, mas toda e qualquer conduta em que haja relação com sistemas informáticos, quer de meio, quer de fim, de modo que essa denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta, sem a imprescindível ‘conexão’ à Rede Mundial de Computadores. (ROSSINI, 2001, p. 138).

Crespo (2011, p. 50, entende que o termo “cibercrime” acabou por ser o mais utilizado, entre as demais denominações recebidas pelas condutas ilícitas perpetradas no meio virtual, por ser, inclusive, a nomenclatura adotada na Convenção sobre o Cibercrime, também conhecida como Convenção de Budapeste (ETS 185) (COUNCIL OF EUROPE, 2020).

Para Aras (2010, p. 12):

> [...] a criminalidade informática, fenômeno surgido no final do século XX, designa todas as formas de conduta ilegais realizadas mediante a utilização de um computador, conectado ou não a uma rede, que vão desde a manipulação de caixas bancários à pirataria de programas de computador, passando por abusos nos

> sistemas de telecomunicação. Todas essas condutas revelam "uma vulnerabilidade que os criadores desses processos não haviam previsto e que careciam de uma proteção imediata, não somente através de novas estratégias de segurança no seu emprego, mas também de novas formas de controle e incriminação das condutas lesivas".

Como lembra Bandeira (2016, p. 4), no cenário atual de uso massivo das tecnologias, manter informações protegidas é cada vez mais decisivo para as empresas em um contexto em que ataques virtuais podem ser usados em disputas planetárias entre governos, terroristas e *hackers*. O autor destaca, ainda, que, mesmo gastando altas quantias para evitar vírus, invasão por *hackers* e vazamento de informações, as empresas estão sujeitas a eventos inesperados. Assim, para minimizar os riscos, o as organizações podem aliar as barreiras de proteção com um seguro cibernético para trazer mais tranquilidade em caso de falhas ou ataques.

Por outro lado, a entrada em vigor da Lei Geral de Proteção de Dados (LGPD) acarreta novos impactos para as organizações, trazendo necessidades que venham a exigir até mesmo a restruturação do seu modelo organizacional, e os consequentes custos financeiros e operacionais.

Nesse sentido, é possível mirar para o exemplo da União Europeia (UE), tendo em vista que o Regulamento Geral para a Proteção de Dados (RGPD), em vigor desde 2016, cuja aplicação é obrigatória desde 25 de maio de 2018 (INFORMATION COMISSIONER'S OFFICE, 2020).

Se por um lado, o RGPD é muito protetor em relação ao titular dos dados, por outro, no caso das organizações, observa-se uma necessidade de planejar e implementar políticas de segurança e proteção de dados mais eficientes, com o objetivo de obter melhoria de processos internos, capazes de garantir a conformidade com o novo regulamento. Em sua maioria, as organizações europeias não estavam preparadas para a nova regulação, e, dessa forma, foi necessária uma reestruturação, melhoria de processos e, em consequência, impactos financeiros de elevada monta.

Ainda para ampliar cada vez mais o quantitativo de crimes cibernéticos, o surgimento da pandemia da COVID-19 veio trazer maiores desafios. De acordo com notícia veiculada em agosto de 2020, no *site* do jornal Valor Econômico,

> Os crimes cibernéticos estão crescendo de uma maneira "alarmante" durante a pandemia de Covid-19, com cada vez mais instituições de saúde e governos afetados, alertou [...] a Interpol. De janeiro a abril de 2020, a Interpol detectou mais de 907 mil "spams", 737 incidentes relacionados a malwares (softwares maliciosos) e 48 mil

> links suspeitos, todos relacionados à covid-19. A expectativa é que os números cresçam nos próximos meses. [...] A adoção do home office em grande parte do mundo, uma das estratégias para evitar aglomerações em locais de trabalho e diminuir a propagação do vírus, está sendo explorada pelos hackers em busca de dados. (VITTA, 2020).

Dessa forma, torna-se fundamental desenvolver novas tecnologias voltadas para proteção dos riscos, que se constitui no elemento essencial do Seguro Cibernético. Tal modalidade de seguro foi criada com a finalidade de proporcionar proteção contra os riscos relacionados ao uso de tecnologias, em especial para sistemas que funcionam na *Internet*, visando restabelecer os prejuízos financeiros causados por esses riscos.

Assim, no presente trabalho tem-se o objetivo de analisar o crescente aumento de demanda pelo "seguro cibernético", seja pelos riscos cibernéticos cuja incidência percebeu-se crescente na pandemia da COVID-19, pela mudança das novas formas laborais, seja pela entrada em vigor da LGPD.

Dessa forma, ao final do estudo, pretende-se contribuir para a análise do tema relacionado ao "risco cibernético" e ao "seguro cibernético", tema este ainda não muito explorado academicamente no país.

2 Risco cibernético e seguro cibernético

2.1 Risco cibernético

Neste item pretende-se analisar o risco cibernético, tratando de responsabilidades, perdas e custos visualizados para a sociedade em geral, e, em especial, para as organizações.

Em relação à conceituação de risco cibernético, a Comissão de Valores Mobiliários brasileira (CVM) adota o mesmo conceito da IOSCO (2016), no documento CVM (2017), qual seja: "Risco cibernético refere-se aos potenciais resultados negativos associados aos ataques cibernéticos. Por sua vez, os ataques cibernéticos podem ser definidos como tentativas de comprometer a confidencialidade, integridade e disponibilidade de dados ou sistemas tecnológicos"[31] (CVM, 2017, p. 7).

[31] Do inglês: "*Cyber risk refers to the potential negative outcomes associated with cyber attacks. In turn, cyber attacks can be defined as attempts to compromise the confidentiality, integrity, and availability of computer data or systems*" (IOSCO, 2016; CVM, 2017).

O documento (IOSCO, 2019, tradução nossa), adota ainda este conceito em relação ao Risco cibernético: "O risco cibernético é definido como a combinação da probabilidade de ocorrência de incidentes cibernéticos e seu impacto"[32].

O documento da Comissão de Valores Mobiliários brasileira (CVM) destaca, ainda, que o tema risco cibernético vem ganhando importância nos fóruns internacionais de reguladores de mercados financeiros e de capitais no esteio da tendência de crescente automatização de processos operacionais de seus jurisdicionados (CVM, 2017, p. 6).

Pesquisa realizada pela empresa do mercado de seguros Lloyd's de Londres, com 350 decisores seniores em toda a Europa, produzida em associação com a KPMG no Reino Unido, com a empresa de advocacia internacional DAC Beachcroft e a Lloyd's, no intuito de fornecer uma avaliação intersetorial das ameaças cibernéticas enfrentadas pelas empresas, esclarece:

> À medida que a tecnologia avança, o mesmo ocorre com o cenário de ameaças. Os criminosos organizados estão escalando suas operações e procurando automatizar o direcionamento e a exploração de redes de negócios. Eles também estão redirecionando os ataques para atingir novas instituições em vários setores. [...]
> Os custos de um incidente cibernético geralmente ocorrem em duas fases – imediatos (ou seja, taxas de investigação legal e forense e pagamentos de extorsão) e "slow-burn" (em tradução literal, "queima lenta", ou seja, aqueles associados aos impactos de longo prazo, como a perda de vantagem competitiva e rotatividade de clientes). A extensão desses custos pode variar consideravelmente por setor e estão em constante evolução. (KPMG, 2017, tradução nossa).

A pesquisa detalha, ainda que, embora não seja possível estar 100% seguro contra um ataque cibernético, existem medidas que as empresas podem adotar para mitigar os riscos, minimizar as consequências e recuperar-se mais rapidamente caso ocorra uma violação. E destaca que o seguro cibernético é uma parte fundamental da solução. A demanda por cobertura de risco cibernético continua a ser impulsionada por leis de violação de privacidade em certos países, mas a ausência de medidas semelhantes em outros continentes pode contribuir para a relativa falta de conscientização sobre o seguro cibernético (KPMG, 2017, tradução nossa).

Conforme estudo realizado pela McAfee, em parceria com a Center for Strategic and International Studies (CSIS), divulgado pela Computerworld, o crime cibernético gera um prejuízo de quase US$ 600 bilhões para empresas (0,8% do PIB mundial), refletindo aumento em relação a um estudo de 2014 que avaliou os prejuízos globais em aproximadamente US$ 445 bilhões. O relatório atribui o crescimento dos últimos três anos "à rapidez com que os

[32] Do inglês: "Cyber Risk is defined as the combination of the probability of Cyber Incidents occurring and their impact" (IOSCO, 2019).

criminosos cibernéticos adotam novas tecnologias, à facilidade de ingressar no crime cibernético e à estrutura financeira cada vez mais sofisticada de criminosos cibernéticos profissionais" (COMPUTERWORLD, 2018).

O relatório da AON, empresa corretora de seguros e resseguros, em parceria com o Ponemon Institute, afirma que as principais ameaças são: ataques a sistemas (interrupção de serviços, ataques a infraestruturas críticas); *hacking* (difamação, violação de privacidade/confidencialidade); roubo de informação (vantagem econômica / competitiva); crime cibernético (obtenção ilícita de dinheiro ou bens); e outras causas (eventos naturais e erro humano).

Para dimensionar de forma rápida ("*fast facts*") fatos e valores que envolvem o risco cibernético e o seguro cibernético, o relatório destaca, que, em termos de números tratados por uma única empresa, no caso, a Aon, são 60 ou mais profissionais dedicados aos riscos informáticos em todo o mundo; 400 milhões de euros ou mais em prêmios de seguro geridos em 2016; mais de 500 incidentes informáticos geridos desde 2012; mais de 2.300 clientes cuja gestão de gestão dos riscos informáticos está sob responsabilidade da empresa. E o relatório finaliza com a seguinte frase: "Is not more the question 'if it happens'; is 'how to react when it happens'" (TEIXEIRA, 2017).

No entanto, muito embora as ameaças se encontrem em pleno crescimento, a capacidade de preparação do risco das organizações está decrescendo. De acordo com o relatório da Aon (AON, 2017), apesar da percepção e avaliação do risco cibernético e da adesão a seguros estarem em crescimento, a preparação organizacional está em declínio, passando este de 82% em 2015 para 79% em 2017. O mesmo relatório aponta que isso pode ocorrer devido a duas razões: as empresas utilizam técnicas cada vez mais sofisticadas na gestão de risco cibernético, e, assim, descobrem novos aspectos anteriormente desconhecidos neste risco, necessitando então de aumentar constantemente a sua preparação; a evolução constante da transformação digital cria maiores vulnerabilidades e provoca uma maior exposição da empresa, sendo um desafio maior implementar estratégias mais eficazes (AON, 2017).

Por todo o analisado, observa-se que se faz necessário melhorar a avaliação dos riscos cibernéticos nas organizações, investir na conscientização e formação de todos os colaboradores, promover medidas de prevenção e implementação de melhores práticas para a proteção do risco, definir protocolos e processos, de forma a dar uma resposta mais rápida

no sentido de obter-se a recuperação de forma eficiente após um incidente cibernético, além de recorrer à contratação de um seguro, para permitir a mitigação desses riscos.

Para Ferreira (2020),

> conhecer, estudar e avaliar o risco e a consequente exposição ao mesmo passa inevitavelmente por definir e implementar medidas de controle e contenção do risco, intervindo sobre os fatores que o promovem e condicionam, como sejam, a vertente humana, física e digital, no qual incluímos naturalmente os softwares e hardwares, a segurança de processos e procedimentos, e claro, a formação das pessoas.

Entendemos que um dos aspectos a destacar é sobre a visão puramente tecnicista do problema relacionado ao risco cibernético. Como aponta Madeira (2020, p. 4), "a parte tecnológica em que normalmente os engenheiros informáticos atuam representa apenas uma das vertentes do risco de segurança cibernética, sendo que uma efetiva gestão do risco de segurança cibernética deverá ser feita considerando igualmente as vertentes de governança, pessoas e processos". Para o autor, a maioria dos ataques que ocorrem hoje em dia são iniciados por meio de pessoas; dessa forma, o investimento, em nível de sensibilização e cultura de segurança deve ser igualmente uma área de foco e investimento (MADEIRA, 2020).

Schuh (2020) ressalta que, "este ano, o risco cibernético aparece no *ranking* do Relatório de Riscos Globais 2020 como uma das principais ameaças aos negócios. Nesse relatório produzido pelo World Economic Forum em parceria com a Marsh & McLennan, a Zurich e as universidades de Oxford, Singapura e Pensilvânia, o ataque cibernético está entre os riscos que mais aumentará neste ano. Dessa forma, a ameaça de ataques de *hackers* aos sistemas das organizações é uma preocupação global.

Todos os países modernizaram os seus arcabouços regulatórios criando mecanismos legais para punir crimes cibernéticos. Também foram criadas regras para as organizações públicas e privadas que têm em suas bases um robusto volume de dados e informações dos cidadãos e consumidores. Foi aí, que seguindo o que ocorreu na União Europeia em 2018, com a entrada em vigor do GDPR (General Data Protection Regulation), o Brasil criou a LGPD, em vigor desde agosto deste ano de 2020.

Essa autora menciona ainda que, no contexto de proteger os dados dos consumidores, surge também a Resolução do Banco Central (Bacen). A Circular Bacen nº 3.979, de 30 de janeiro de 2020, dispõe sobre a constituição e a atualização da base de dados de risco operacional e a remessa ao Banco Central do Brasil de informações relativas a eventos de risco operacional. De forma geral, a resolução equipara o risco cibernético ao risco operacional. Em

2018, o Bacen já havia criado a Resolução nº 4.658, com o objetivo de mitigar os riscos cibernéticos e proteger as instituições financeiras.

Assim, Schuh (2020) entende que:

> o seguro cibernético deve ser visto como um mecanismo de mitigação de prejuízos em potencial e de resposta a incidentes que constituem as novas normas regulatórias, uma vez que o seguro não apenas indeniza os custos relacionados a incidentes, mas também possui o amparo de um time de gestão de crises. (SCHUH, 2020).

2.2 Seguro cibernético

No sentido de compreender essa modalidade de seguro, entendemos ser necessário, inicialmente, estudar o conceito de "seguro". Para a Superintendência de Seguros Privados (SUSEP)[33], seguro é um "Contrato mediante o qual uma pessoa denominada Segurador, se obriga, mediante o recebimento de um prêmio, a indenizar outra pessoa, denominada Segurado, do prejuízo resultante de riscos futuros, previstos no contrato" (SUSEP, 2020).

No Brasil, o seguro cibernético foi regulamentado pela Susep em 2007. Desde então, algumas companhias de seguros internacionais passaram a oferecer apólices de proteção cibernética para empresas com sedes localizadas em território nacional. O seguro para riscos cibernéticos protege tanto os contratantes da apólice quanto os possíveis impactados pelo roubo de dados. O produto oferece cobertura para todos os custos pós-ataque *hacker* e vazamento de dados. Cobre também ataques *ransomware*, que bloqueiam os arquivos da organização e exigem pagamento de resgate. Além disso, a seguradora disponibiliza para os clientes uma equipe para atendê-los em caso de sinistro (APÓLICE, 2020).

Como destaca Porup (2020), "o seguro cibernético pode ser uma parte importante e valiosa do gerenciamento de riscos corporativos". Para o autor, entender o que pode ou não ser realizado - e a direção que o setor de seguros cibernéticos está seguindo – é fundamental para tirar o máximo proveito de uma apólice.

[33] A Superintendência de Seguros Privados (SUSEP) é órgão governamental responsável pela autorização, controle e fiscalização dos mercados de seguros no Brasil. A SUSEP foi criada pelo Decreto-lei nº 73, de 21 de novembro de 1966, como entidade autárquica, jurisdicionada ao Ministério da Indústria e do Comércio, dotada de personalidade jurídica de Direito Público, com autonomia administrativa e financeira. Sua primeira função principal é regulamentar o setor de seguros no país, ou seja, estabelecer as regras para operação de todos os envolvidos na oferta e comercialização de seguros no Brasil. Conforme informações disponíveis em: https://www.minutoseguros.com.br/perguntas-frequentes/seguro-auto/o-que-e-a-susep.

Para o autor, a utilidade real do seguro cibernético pode ser o trabalho necessário para obterem-se políticas em primeiro lugar, pois, segundo Porup (2020), a maioria das apólices de seguro inclui questionários longos com consultas cada vez mais detalhadas sobre controles de segurança específicos em vigor na sua organização. Isso significa que, mesmo para obter um seguro cibernético, é necessário realizar uma auditoria de ativos e processos, que darão ao segurado (e à companhia de seguros) informações.

Moura Jr. (2017), entende que, da análise do risco cibernético, facilmente se conclui que, atualmente, as medidas iniciais mais importantes são a aplicação do gerenciamento do risco por parte do usuário, sendo que parte essencial nesse gerenciamento são as questões de controle de risco. Assim, o autor ressalta que a minimização do risco mediante ações de controle de risco é que irá permitir melhores condições de negociação na colocação do risco no mercado segurador (MOURA JR., 2017).

E, ainda, Moura Jr. (2017) explana que nenhuma seguradora irá aceitar um risco cibernético amplo sem antes realizar profundo *assessment* ou avaliação dos sistemas de cada segurado. A avaliação prévia permite o conhecimento o mais exato possível do risco do segurado. Dessa forma, a seguradora terá uma análise dos riscos aceitáveis ou não, tendo como decidir o que é possível garantir ou excluir. Para tal *assessment*, o autor sugere que sua realização seja conduzida por empresa independente, tecnicamente abalizada em TI e em gerenciamento de risco. Essa avaliação e medidas de controle de risco a serem adotados seriam pagas em partes iguais pelo segurado e pela seguradora. Desse modo, o seguro cibernético será resultante de análises específicas e as condições e cláusulas da apólice deverão ser acordados mediante negociação transparente entre as partes e, assim, a taxação do risco cibernético espelha o resultado da análise de risco individual e as garantias efetivas a serem concedidas (MOURA JR., 2017).

A entrada em vigor da LGPD, ao exigir medidas técnicas e organizacionais que garantam a segurança dos dados, além de outros aspectos relacionados ao exercício dos vários direitos ali previstos (portabilidade, apagamento, acesso), sem as quais não é possível assegurar um grau adequado de privacidade, fez crescer a demanda pelo “seguro cibernético”.

Segundo notícia publicada no site TILT (DIEB, 2020), de acordo com a Susep, as empresas de seguros cibernéticos arrecadaram em prêmios (valor pago pelos clientes) R$ 3,5

milhões em janeiro; em abril, houve queda, chegando a R$ 1,3 milhão; em junho, veio nova alta, de R$ 4,1 milhões. Um dos motivos disso é a LGPD.

Cabe registrar ademais, que, no Brasil, foi incluído pela Susep, no grupo de "Responsabilidades" o ramo "Compreensivo Riscos Cibernéticos", por meio da Circular SUSEP n° 579/2018, que alterou a Circular SUSEP n° 535/2016, que estabelece a codificação dos ramos de seguro e dispõe sobre a classificação das coberturas contidas nos planos de seguro, para fins de contabilização (PWC, 2018/2019).

2.3 Documentos-base para consulta ao tema "risco e seguro cibernético"

O documento "Seguro do risco cibernético: um guia de recursos para Atuários" (ACTUARY.ORG, 2019, tradução nossa) apresenta uma base para consulta para profissionais do ramo da atuária. As publicações mencionadas são as seguintes:

1. Organização para a Cooperação e o Desenvolvimento Econômico (OCDE), "realçando o papel do seguro na gestão do risco cibernético" (OECD, 2017a, tradução nossa): este relatório apresenta várias recomendações de políticas destinadas a melhorar a contribuição do mercado de seguros cibernéticos para a gestão do risco apresentado pela digitalização.
2. OCDE, "apoiando um mercado eficaz de seguros cibernéticos": este relatório resume concisamente o relatório abrangente da OCDE "realçando o papel do seguro na gestão do risco cibernético" (OECD, 2017b, tradução nossa).
3. Associação GENEVA, "Seguro cibernético como estratégia de mitigação do risco": este documento "analisa a situação do mercado cibernético e o papel que as seguradoras desempenham no avanço da resiliência cibernética (GENEVA, 2018, tradução nossa).
4. "Relatório de preparação cibernética da Hiscox": este relatório é compilado por meio de uma pesquisa com mais de 4.100 executivos, chefes de departamento, gerentes de tecnologia da informação (TI) e outros profissionais importantes no Reino Unido, EUA, Alemanha, Espanha e Holanda, de organizações de grande e pequeno porte, nos setores público e privado. O relatório não apenas fornece um panorama atualizado da prontidão cibernética das organizações pequenas e grandes, bem como oferece um modelo para as melhores práticas, com o foco de conter uma constante evolução das ameaças (HISCOX, 2018).
5. Carnegie, "Abordando o dilema da segurança cibernética do setor privado": neste relatório discute-se uma série de barreiras que impedem um funcionamento mais eficaz do cibermercado de seguros cibernéticos, incluindo-se desafios práticos, técnicos, operacionais

e estratégicos, dentro e fora da indústria de seguros, explora-se uma série de esforços individuais e complementares da indústria de seguros, dos governos, fornecedores de tecnologias de informação e comunicação (TICs), e de outras partes interessadas importantes no setor privado para a realização de todo o potencial de seguro para remodelar o ambiente de risco. (CARNEGIE, 2018, tradução nossa).

3 O setor segurador e o seguro cibernético

3.1 Aspectos gerais sobre o "seguro de responsabilidade cibernética"

De acordo com “Whitepaper: Cyber Liability InsuranceOverview” (SLTTGCC, 2016), o termo "seguro de responsabilidade cibernética", tradução nossa do termo em inglês “Cyber Liability Insurance”, é frequentemente usado para descrever uma gama de coberturas, em grande parte da mesma forma que a palavra "cibernético" é usada para descrever uma ampla gama de informações relacionadas à segurança, ferramentas, processos e serviços. De acordo com o documento (SLTTGCC, 2016), mesmo que as coberturas variem, os riscos cibernéticos geralmente incluem:

a) roubo de identidade como resultado de violações de segurança, quando informações sensíveis são roubadas por um *hacker* ou divulgadas inadvertidamente, incluindo elementos de dados tais como dados de seguridade social números, números de cartão de crédito, números de identificação de funcionários, números de carteiras de habilitação, datas de nascimento e números *personal identification number* (PIN).
b) Danos à reputação da empresa.
c) roubo de ativos valiosos digitais, incluindo listas de clientes, segredos comerciais de negócios e outros ativos de negócios eletrônicos similares.
d) introdução de *malware*, *worms* e outros códigos maliciosos de computador.
e) erro humano que conduz à divulgação inadvertida de informações sensíveis, tal como um *e-mail* de um funcionário a destinatários indesejados, contendo informações comerciais sensíveis ou informações de identificação pessoal; e
f) ações judiciais alegando violação de direitos autorais ou infrações relativas a marcas registradas.

O documento, no entanto, refere que o risco cibernético continua difícil para as companhias seguradoras quantificarem, devido, em grande parte, a uma falta de dados atuariais. Assim, as seguradoras compensam essas dificuldades, confiando em avaliações

qualitativas de procedimentos de gestão de risco do requerente e à cultura de risco. Como resultado, as políticas de risco cibernético são mais personalizadas que outros seguros de risco, portanto podem ser mais caros. E, ainda, o tamanho e escopo da organização definirão o tipo e o custo da cobertura de responsabilidade cibernética. Além disso, o tamanho e o escopo da organização terão influência direta nas necessidades de cobertura e preços, bem como o número de clientes, a presença na *web*, além do tipo de dados coletados e armazenados, e outros fatores.

Ainda de acordo com SLTTGCC (2016), as políticas de responsabilidade cibernética podem incluir um ou mais dos seguintes tipos de cobertura:

• responsabilidade por violações de segurança ou privacidade. Isso inclui a perda de informações confidenciais ao permitir ou não impedir, o acesso não autorizado aos sistemas de computador;

• custos associados a uma violação de privacidade, como notificação ao consumidor, suporte ao cliente e custos de fornecimento de serviços de monitoramento de crédito aos consumidores afetados;

• custos associados à restauração, atualização ou substituição de ativos comerciais armazenados eletronicamente;

• interrupção de negócios e despesas extras relacionadas a uma violação de segurança ou privacidade;

• responsabilidade associada a difamação, calúnia, violação de direitos autorais, depreciação de produto ou danos à reputação de terceiros quando as alegações envolvem um *site* de negócios, mídia social ou mídia impressa;

• despesas relacionadas a extorsão cibernética ou terrorismo cibernético; e

• cobertura para despesas relacionadas à conformidade regulatória para erros de faturamento, procedimentos de autoencaminhamento médico e procedimentos de demanda espontânea de médicos, tratamento médico de emergência e procedimentos de natureza trabalhista.

Das análises realizadas, visualiza-se que as violações cibernéticas, crescentes em quantitativos e em nível de sofisticação, fazem crescer também os riscos cibernéticos que afetam a todas as organizações, sejam elas públicas ou privadas. A depender do escopo da violação e do tipo(s) de informação comprometida, os custos variam e podem se elevar rapidamente.

Assim sendo, a publicação supramencionada (SLTTGCC, 2016), considera algumas razões para investir-se no seguro cibernético, entre as quais destacam-se:

a) o cenário que se apresenta para a organização, em termos de ameaças é dinâmico e há um número crescente de adversários. A capacidade das organizações de combater ataques, vindos de Estados-nações, criminosos globais e de pessoas mal intencionadas, é suplantada.
b) Segurança não é igual a conformidade, pois os padrões de conformidade são essencialmente os requisitos mínimos. Assim, tratar o assunto da segurança da informação como um problema de conformidade desfoca a implementação de um programa abrangente e, em última análise, resulta em um sentido falso de segurança. Apesar de estarem em conformidade com seus padrões exigidos, muitas organizações já foram vítimas de violação de dados ou de incidentes de segurança.

3.1.1 A evolução dos riscos cibernéticos

O relatório 2019 do World Economic Forum aborda os vários aspectos relativos aos riscos que afetaram o planeta em 2019. Em relação ao aspecto tecnológico, aquele relatório destaca (WORLD ECONOMIC FORUM, 2019, p. 15-17):

A tecnologia continua a desempenhar um profundo papel na formação do cenário global de riscos para indivíduos, governos e empresas. No Global Risks Perception Survey (GRPS)[34], "fraude massiva de dados e roubo" foi classificada como o risco global número quatro, em um horizonte de 10 anos, com "ciberataques" no quinto lugar. Isso mantém um padrão do último ano, com a consolidação de riscos cibernéticos, assegurando sua posição ao lado de riscos ambientais no quadrante de alto impacto e alta probabilidade no cenário de riscos globais".

A pesquisa reflete como as novas instabilidades estão sendo causadas pelo aprofundamento da integração das tecnologias digitais em todos os aspectos da vida. Cerca de dois terços dos entrevistados esperam que os riscos associados a notícias falsas e roubo de

[34] A Pesquisa de Percepção de Riscos Globais (GRPS) é a fonte de dados originais de riscos do Fórum Econômico Mundial, aproveitando a experiência da extensa rede do Fórum que inclui líderes empresariais, governamentais, da sociedade civil e pensadores. A pesquisa foi realizada de 5 de setembro a 22 de outubro de 2019 entre as comunidades multissetoriais do Fórum Econômico Mundial, as redes profissionais de seu Conselho Consultivo e membros do Institute of Risk Management. Conforme informações disponíveis em: https://reports.weforum.org/global-risks-report-2020/appendix-b-methodology.

identidade aumentem em 2019, enquanto três quintos disseram o mesmo sobre a perda de privacidade para empresas e governos.

Ataques cibernéticos maliciosos e protocolos de segurança cibernética frágeis, novamente lideram a violações maciças de informações pessoais em 2018. A maior delas ocorreu na Índia, onde a base de dados de identificação do governo, Aadhaar, supostamente sofreu várias violações, o que potencialmente comprometeu os registros de 1,1 bilhão de cidadãos registrados, tendo sido relatado em janeiro que os criminosos estavam vendendo o acesso ao banco de dados a uma taxa de 500 rúpias por 10 minutos (WORLD ECONOMIC FORUM, 2019, p. 16-17).

Na descrição de tendências e riscos globais em 2019, os riscos foram divididos por categorias, sendo estas: riscos econômicos; ambientais; geopolíticos; sociais; e tecnológicos. Em relação aos riscos tecnológicos, foram verificados:

a) consequências adversas de avanços tecnológicos: consequências adversas intencionais ou não intencionais de tecnologia; avanços, tais como inteligência artificial, geoengenharia e biologia sintética causando danos humanos, ambientais e econômicos;

b) colapso de infraestrutura crítica de informação e redes: dependência cibernética que aumenta a vulnerabilidade à interrupção de um sistema crítico de infraestrutura de informações (como por exemplo, *internet*, satélites, entre outros) e redes, causando perturbações generalizadas.

c) ataques cibernéticos em larga escala: ataques cibernéticos em grande escala ou *malware* que causam grandes danos à economia, tensões geopolíticas ou perda generalizada de confiança na *internet*; e

d) incidentes massivos de dados fraudulentos/roubo: exploração indevida de dados privados ou oficiais que ocorre em uma escala sem precedentes.

3.2 A necessidade de adequação à legislação brasileira que trata de cibercrimes em geral e à LGPD

Souza (2019) lembra que os ataques cibernéticos que chocaram o mundo em 2016 e 2017 — os *ransomwares* Petya e WannaCry, respectivamente – foram fundamentais para despertar preocupação dentro das empresas e incentivar a procura por indenizações pós-incidente. O autor destaca que “os *malwares* causaram prejuízos astronômicos inclusive aqui

no Brasil, sequestrando computadores usados por órgãos públicos e empresas privadas dos mais diversos segmentos, totalizando 616 mil infecções só pelo WannaCry".

Esse autor ressalta, ainda, que um crescimento na demanda pelo seguro cibernético é devido ao "desenvolvimento de uma cultura de proteção de dados no Brasil", o que inclui a Lei de Acesso à Informação (nº 12.5272011), a Lei Carolina Dieckmann (nº 12.737/2012), o Marco Civil da Internet (nº 12.965/2014), a Resolução do Bacen sobre Segurança Cibernética (nº 4.658/2018) e a Lei Geral de Proteção de Dados (nº 13.709/2018).

Em relação à LGPD, de modo geral, as empresas, em 2019, iniciaram seus projetos de diagnóstico de *gaps* em relação à LGPD, no sentido de elaborarem um plano de ação para sua adequação. Muitas delas iniciaram seus trabalhos de adequação em 2019, enquanto outras planejaram iniciar seus trabalhos em 2020. De acordo com PWC (2019/2020, p. 23-24) os setores que saíram na frente foram o de saúde, pelo enorme impacto decorrente do uso intenso de dados sensíveis inerentes ao setor, o de varejo e de produtos de consumo em geral, pelo tratamento intensivo de dados pessoais, o de serviços financeiros, meios de pagamento e seguradoras, pelos volumes no tratamento de dados pessoais, e, em particular, pela convergência de alguns aspectos de segurança cibernética exigidos por resoluções específicas do Banco Central.

A publicação supramencionada PWC (2019/2020, p. 23-24) destaca ainda que, durante o ano de 2019, houve um movimento intenso das empresas privadas e públicas no Brasil para iniciar as respectivas jornadas de adequação à LGPD, incluindo as seguintes atividades:

a) mapeamento das operações de tratamento de dados pessoais;
b) análise dos principais *gaps* em relação às exigências da lei nos processos das empresas, nos modelos de negócio, nos sistemas e bancos de dados e, também, nas práticas de segurança e de proteção de dados pessoais;
c) definição ou nomeação do Encarregado de Tratamento de Dados;
d) elaboração de um plano de ação com as principais atividades de adequação à lei, diante dos *gaps* identificados; e
e) definição do orçamento para implementação dos processos e tecnologia necessários a fim de garantir a conformidade com a legislação.

Entre os motivos pelos quais as empresas devem manter foco na jornada de adequação destacam-se os seguintes: prevenir-se de sanções e penalidades; manter a confiança de clientes e consumidores; evitar impactos nas relações internacionais, tendo em

vista as legislações internacionais que tratam de privacidade de dados, em especial a *General Data Protection Regulation* (GDPR) europeia; desenvolvimento tecnológico e inovação; a proteção de dados no Brasil já é uma realidade, independente do fato de que a LGPD ainda aguarda alguns eventos para sua total implementação. (PWC, 2019/2020, p. 23-24)

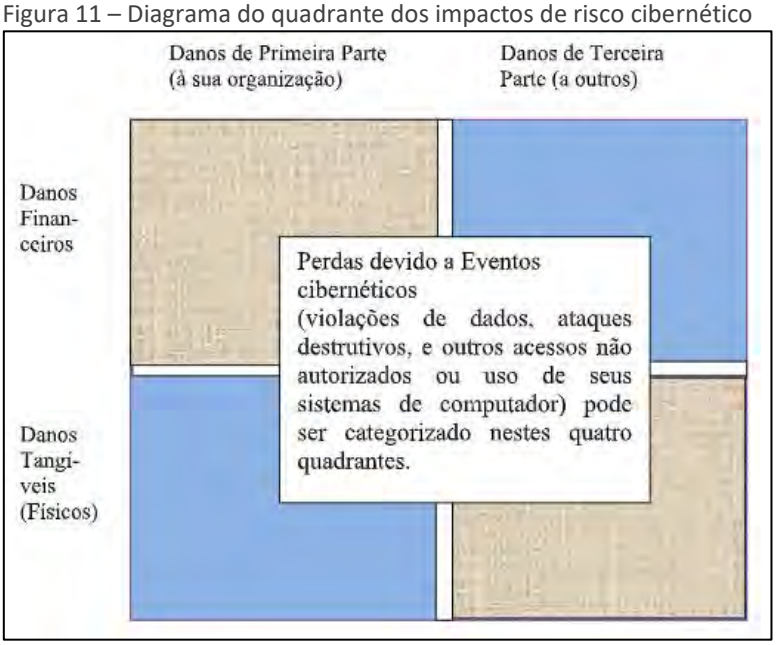
Ao final de 2020, destacam-se importantes perdas de empresas por ataques cibernéticos, bem como em relação a multas aplicadas por não cumprimento à LGPD. De acordo com notícia publicada no *site* do Sindicato das Empresas de Seguros e Resseguros (SINDSEGSP, 2020), a empresa Natura, reportou prejuízos de R$ 392 milhões no segundo trimestre. Um ataque hacker sofrido por sua controlada Avon, em junho, foi citado como principal motivo do resultado negativo. No início do mês de outubro de 2020, a petroquímica Braskem divulgou que um ataque cibernético deixou a empresa fora do ar e prejudicou, por dias, as atividades de faturamento e expedição de produtos. Também no início de outubro deste mesmo ano, a construtora Cyrela foi condenada pela Justiça de São Paulo a pagar indenização de R$ 10 mil por compartilhar dados de um cliente com outras empresas, por meio de decisão judicial que teve como base a LGPD. A mesma notícia dá conta de que a procura pelo seguro para riscos cibernéticos cresceu 40% após a aprovação da LGPD.

3.3 A quantificação do risco cibernético e as coberturas do seguro cibernético

Os modelos de impacto financeiro e de negócios para quantificar o risco já existem. O desafio para o pessoal de segurança é adaptar esses modelos ao ambiente de segurança cibernética. Uma forma usual de ver o risco cibernético é classificando as perdas potenciais devido a incidentes de segurança cibernética em termos de impactos financeiros e físicos. A Figura a seguir ilustra o diagrama de quadrantes comumente utilizado para detalhar essas perdas (CHRISTOPHER, 2020, p. 4, tradução nossa).

Os quadrantes cobrem a forma como esses danos podem afetar as primeiras partes (ao próprio indivíduo e a organização) e terceiros (clientes, parceiros e fornecedores). Alguns dos danos são bastante reduzidos, pois, em princípio, discussões sobre danos financeiros de primeira parte são relativamente comuns para profissionais de segurança.

Figura 11 – Diagrama do quadrante dos impactos de risco cibernético



Fonte: Christopher (2020, p. 4, tradução nossa, com adaptações)

O autor ressalta a necessidade de que os profissionais de segurança criem modelos para quantificar perdas. Para tal, é necessário que a organização reúna informações, com estimativa de valores em moeda corrente, com base nesses modelos. No sentido de fornecer sugestões para alimentar tais modelos de segurança, em relação a riscos cibernéticos, o autor apresenta sugestões de dados necessários para quantificar perdas em cada um dos casos identificados na Figura 1. No Quadro abaixo, são tratados os danos de primeira parte.

Quadro 9 – Sugestões de dados necessários para quantificar perdas de danos de primeira parte

Dados	Danos de Primeira Parte (à sua organização)
financeiros	Custos de resposta: análise forense, notificações, monitoramento de crédito, gerenciamento de crises, relações públicas
	Despesas legais: consultoria jurídica e defesa
	Perdas de receita: interrupções de rede ou computador, incluindo nuvem
	Despesas de restauração de dados perdidos
	Despesas de extorsão cibernética
	Perdas de propriedade intelectual roubadas: incluindo receitas associadas e perdas de participação de mercado
tangíveis (físicos)	Avaria mecânica do seu equipamento
	Destruição ou danos às suas instalações ou outros bens
	Descontaminação ambiental da sua propriedade
	Receitas perdidas por danos físicos ao seu equipamento (ou do qual a organização é dependente) ou instalações (interrupção de negócios)
	Lesões corporais aos seus funcionários

Fonte: Christopher (2020, p. 5-7, tradução nossa)

No Quadro seguinte, são tratados os danos de terceira parte (CHRISTOPHER, 2020, p. 5-7, tradução nossa).

Quadro 10 – Sugestões de dados necessários para quantificar perdas de danos de terceira parte

Dados	Danos de Terceira Parte (a terceiros)
Financeiros	Entidades de terceira parte podem procurar recuperar:
	Perdas de receita consequentes
	Despesas de restauração
	Despesas legais
	Custos de monitoramento de crédito
Danos tangíveis (físicos)	Avaria mecânica de equipamentos de terceiros
	Destruição ou danos às instalações de terceiros ou bens de terceiros
	Descontaminação ambiental da propriedade de outros
	Lesões corporais a terceiros

Fonte: Christopher (2020, p. 6-7, tradução nossa)

Christopher (2020, p. 11) destaca ainda que, durante décadas, os riscos associados à segurança cibernética são discutidos no sentido de aceitar, mitigar, tolerar ou transferir riscos associados à mesma. No entanto, somente os três primeiros são tratados, ou seja, estamos sempre aceitando, mitigando ou tolerando o risco cibernético, pois, a transferência desses riscos quase não é tratada.

O seguro cibernético é um desses mecanismos de transferência; para tal, é necessário obter uma compreensão apurada dos efeitos e perdas devido a um ataque de segurança cibernética, bem como o mecanismo para transferir essas potenciais despesas. A parceria com uma seguradora transfere a responsabilidade financeira pelos riscos que uma equipe de segurança gerencia para a seguradora. Adicionalmente, à medida que uma organização se torna melhor em medir e gerenciar seu programa de segurança cibernética, pode ser capaz de diminuir suas taxas de seguro e ainda receber uma melhor cobertura (CHRISTOPHER, 2020, p. 11, tradução nossa).

A ocorrência do evento NotPetya[35], considerado o ataque cibernético mais caro da história, trouxe à tona a discussão recorrente para a indústria dos seguros: se o NotPetya era

[35] Em julho de 2017, a empresa dinamarquesa Maersk, maior operadora de navios de contêineres e navios de abastecimento do mundo, com escritórios em 130 países e uma força de trabalho de cerca de 90.000, foi vítima de um ataque cibernético que usou uma versão supostamente modificada do *Petya ransomware*, *NotPetya*, derrubando sistemas de TI e controles operacionais em todos os níveis. Após se instalar nas redes de uma embarcação da Maersk, o *software* malicioso criptografou irreversivelmente os registros mestre de inicialização dos computadores, a parte mais profunda de uma máquina que indica onde encontrar seu próprio sistema operacional. Conforme informação disponível em: https://seginfo.com.br/2020/10/08/caso-maersk-saiba-como-o-notpetya-foi-responsavel-por-um-dos-maiores-ataques-ciberneticos-da-historia/.

ligado à guerra e, mais especificamente, se aquela exclusão de guerra encontrada em todas as apólices de seguro cibernético poderia ter evitado a cobertura. Artigo recente do Wall Street Journal descreveu esta questão como: “a pergunta do milhão para as companhias que compram seguros cibernéticos”. O NotPetya provocou perdas de bilhões de dólares em várias empresas: valores monetários perdidos, sistemas de computação danificados e ainda um investimento pesado para restaurar as operações globais.

Conforme mencionado em pesquisa e informativo da Marsh (2018), associar a exclusão por guerra com um evento cibernético não-físico como o NotPetya surge de dois fatores: (1) o NotPetya provocou prejuízos econômicos substanciais a várias empresas; e (2) os governos dos Estados Unidos e do Reino Unido atribuíram o ataque NotPetya ao exército russo. Permanece a discussão sobre o fato de que somente estes dois fatores seriam suficientes para escalar este ataque cibernético não físico na categoria de guerra ou atividade “hostil e bélica”.

Tais argumentos, conforme destaca a pesquisa mencionada, têm sido considerados pelos tribunais, e as decisões resultantes deles, que agora fazem parte das Leis do Conflito Armado, deixam claro que é preciso muito mais para se chegar à conclusão de que uma ação é “bélica”. E, ainda, o debate sobre se poderia ter sido aplicada ou não a exclusão de guerra ao NotPetya demonstra que se as seguradoras continuarão incluindo a exclusão de guerra nas apólices de seguro cibernético; a redação delas deverá ser verificada para deixar claro quais são as circunstâncias necessárias para considerá-la (MARSH, 2018).

Quanto a este aspecto, que trata das circunstâncias de como definir quando a sabotagem é séria o suficiente para se caracterizar como um ato de guerra, Gorman; e Barnes (2011) apresentam o caso da empresa Lockheed Martin, grande fornecedora das Forças Armadas dos EUA, quando esta se disse vítima de infiltração de espiões, apesar de ter minimizado a importância do incidente. Ao analisar este caso e em outros semelhantes, oficiais do Pentágono acreditam que os ataques de computador mais sofisticados exigem os recursos de um governo. Assim, o Pentágono chegou à conclusão de que sabotagem de computadores com origem em outro país pode ser considerada um ato de guerra, uma avaliação que pela primeira vez permite aos Estados Unidos responderem usando a força militar convencional.

James Lewis, um especialista em segurança de informática do Centro para Estudos Estratégicos e Internacionais que assessorou o governo do presidente Barack Obama, disse

que os diretores do Pentágono estão identificando que tipo de ataque cibernético constituiria um uso de força. Muitos planejadores militares acreditam que o gatilho para a retaliação deveria ser a quantidade de dano – real ou tentado – causado pelo ataque. As regras que guiam as guerras tradicionais são resultado de uma série de tratados internacionais, incluindo as Convenções de Genebra, bem como as práticas que os EUA e outros países consideram como lei internacional. Entre outras coisas, elas cobrem a conduta de guerra, o tratamento de prisioneiros e os limites para o uso de certas armas. A guerra cibernética não é coberta pelos tratados atuais e as autoridades militares querem buscar um consenso entre os aliados para saber como proceder (GORMAN; BARNES, 2011).

4 Metodologia utilizada

Foi adotada uma metodologia exploratória, tendo em vista que no país não há ainda uma vasta literatura que trata do tema do "seguro cibernético".

Foi realizada pesquisa bibliográfica e análise de documentos, publicações especializadas e outros, bem como dados e informações publicados que tratam, direta ou indiretamente o tema em análise e os dispositivos legais pertinentes, tendo como base um estudo descritivo e analítico das fontes.

5 Considerações finais

A famosa frase proferida em 2006 pelo matemático inglês e especialista em ciência de dados Clive Humby, de que "dados são o novo petróleo", retrata a importância do dado nesta era do Big Data. Assim, vivemos em uma economia digital, em que os dados são muito valiosos, as companhias de seguro e as organizações em geral, estão vivendo o desafio da necessidade de contratação do "seguro cibernético". Dessa forma, a análise, no presente trabalho, a análise do cenário atual, em especial da legislação em vigor no Brasil, na área cibernética, faz-nos compreender mais esse tema e, desta forma, contribuirmos para o conhecimento do mesmo.

O aumento de violações de segurança cibernética é um fenômeno que, sem dúvida, continuará a aumentar; tais eventos afetam os setores público e privado, grandes e pequenas organizações. Manter um bom programa de segurança cibernética pode, contudo, não ser garantia de que a organização não será uma vítima dessas violações.

Observa-se, por outro lado, que possuir tecnologia de segurança cibernética não é a solução perfeita para proteger a organização contra violação ou perda, da mesma forma que contar com um modelo de gerenciamento de risco cibernético também não garante proteção total. Ou seja, segurança cibernética é mais do que controles técnicos, e o seguro pode ajudar a fornecer controles financeiros reais associados. No entanto, se a organização não conta com proteções básicas em vigor, muito provavelmente não conseguirá contratar um seguro cibernético.

Da mesma forma, qualquer investimento em um seguro cibernético, precisa ser parte de uma abordagem geral de gestão de risco, o que inclui manter e melhorar um programa de segurança cibernética em permanente evolução.

Destaca-se ainda o fato de que um seguro é algo com que os executivos estão familiarizados. Eles conhecem bem os mecanismos de transferência de riscos do negócio às companhias de seguro. Entende-se que este fato é substancialmente favorável ao processo de segurança cibernética como um todo, pois, não somente os técnicos são envolvidos no processo como um todo, mas sim, o envolvimento dos executivos passa a ser mandatório.

Pelos estudos realizados, verifica-se que as necessidades de cada organização são diferentes, no entanto, sempre é importante avaliar o que é necessário fazer para que a organização esteja bem preparada para enfrentar violações cibernéticas, que, mais cedo ou mais tarde, ocorrerão.

Nesse sentido, uma das possibilidades para apoio à gestão de risco, é o surgimento de cobertura de seguro de responsabilidade cibernética. Essa cobertura, existente no mercado há mais de 10 anos, é desconhecida pela maioria das organizações.

Ao construir o tripé que envolve dados, modelos de risco e cobertura de seguro, no sentido de acomodar os riscos descobertos, o risco cibernético pode ser resolvido, e, desta forma, ao combinar estes aspectos, as organizações podem começar de fato a gerenciar seu risco cibernético e se tornar resilientes do ponto de vista cibernético.

Assim, analisar o tema como um todo, tanto em termos da legislação em vigor, quanto das violações cibernéticas e riscos cibernéticos e das possibilidades em relação ao próprio “seguro cibernético”, permite conhecerem-se as possibilidades em relação a esse novo tipo de seguro e, dessa forma, atingir-se o objetivo definido para esta pesquisa.

Finalizando, ao observar o incidente do NotPetya, observa-se que, à medida que a gravidade dos ataques cibernéticos continua aumentando, as seguradoras e os compradores

de seguros voltarão a analisar se a exclusão de guerra deveria ser aplicada a um incidente cibernético. Na falta de uma comprovação, seguradoras e compradores de seguros serão obrigados a apelar para as Leis de Conflito Armado, o que pode conduzir a sentenças infindáveis, buscando discernir as categorias de atividades criminosas e ações bélicas.

Quanto ao caso da empresa americana Lockheed Martin, fornecedora das Forças Armadas dos EUA, uma ideia que ganha força no Pentágono é a de "equivalência". Se um ataque cibernético causa mortes, prejuízo, destruição ou um transtorno de alto nível que um ataque militar causaria, então seria um candidato a ser considerado um "ato de guerra".

Referências

ACTUARY.ORG. CYBER RISK INSURANCE A Resource Guide for Actuaries. Academy Academy of Actuaries, May, 2019. Disponível em: https://www.actuary.org/sites/default/files/2019-06/cyber-risk-insurance.pdf. Acesso em: 10 out. 2020.

APÓLICE. Seguro cibernético gera oportunidades para todo o mercado segurador. 8 de julho de 2020. Disponível em: https://www.revistaapolice.com.br/2020/07/seguro-cibernetico-gera-oportunidades-para-todo-o-mercado-segurador/. Acesso em: 20 out. 2020.

ARAS, Vladimir. Crimes de informática: uma nova criminalidade. *Jus Navigandi*, Teresina, ano 5, n. 51, out. 2001. Disponível em: http://jus.com.br/artigos/2250/crimes-de-informatica. Acesso em: 2 out. 2020.

BANDEIRA, Mauricio. *Seguro Cyber*: proteção para dados de sua empresa e de seu cliente. Aon Risk Solutions. Boletim AON, 2016. Disponível em: https://www.aon.com/brasil/arquivos/pdf/Boletim_ARS-de2016_Final.pdf. Acesso em: 20 out. 2020.

CARNEGIE. *Addressing the Private Sector Cybersecurity Predicament* (November 2018) https://carnegieendowment.org/2018/11/07/addressing-private-sector-cybersecuritypredicament-indispensable-role-of-insurance-pub-77622. Acesso em: 10 out. 2020.

CASTELLS, Manuel. *A Era da Informação*: economia, sociedade e cultura. Volume I, a sociedade em rede. 5. ed., São Paulo: Paz e Terra, 2001.

CLARKE, Richard A.; KNAKE, Robert K. *Guerra cibernética*: a próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro: Brasport, 2015.

COUNCIL OF EUROPE. INTERNET PORTAL. *Cybercrime Convention on Cybercrime*. Disponível em: https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese.pdf. Budapest, Hungria, 23 nov. 2001. Acesso em: 15 set. 2020.

COMPUTERWORLD. *Prejuízo com cibercrimes chega a US$ 600 bilhões no mundo*. Da redação. 22 fev. 2018. Disponível em: https://computerworld.com.br/seguranca/prejuizo-com-cibercrimes-chega-us-600-bilhoes-no-mundo/#:~:text=O%20crime%20cibern%C3%A9tico%20gera%20um,em%20aproximadamente%20US%24%20445%20bilh%C3%B5es. Acesso em: 2 out. 2020.

CRESPO, Marcelo Xavier de Freitas. *O cibercrime*. São Paulo: Saraiva, 2011.

CHRISTOPHER, Jason D. *Incentivizing Cyber Security*: A Case for Cyber Insurance. SANS Institute. Information Security Reading Room, June 2017. Disponível em: https://www.sans.org/readingroom/whitepapers/cyberinsurance/incentivizing-cyber-security-case-cyber-insurance-37845. Acesso em: 5 out. 2020.

CVM. Assessoria de Análise Econômica e Gestão de Riscos (ASA). Trabalhos para Discussão. *Percepção de riscos cibernéticos nas atividades de administradores fiduciários e intermediários*. Julho 2017. Disponível em: http://www.cvm.gov.br/export/sites/cvm/menu/acesso_informacao/serieshistoricas/estudos/anexos/Percepcao_de_riscos_ciberneticos_nas_atividades_de_administradores_fiduciarios_e_intermediarios.pdf. Acesso em: 2 out. 2020.

DIEB, Daniel. TILT. Segurança. *Para se precaver da LGPD, empresas correm atrás de seguro cibernético*. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/08/23/cresce-procura-por-seguro-para-riscos-ciberneticos.htm. Acesso em: 20 out. 2020.

GORMAN, Siobhan; BARNES, Julian E. The Wall Street Journal. EUA preveem resposta militar a ataque de hackers. Defesanet, 31 maio 2011. Disponível em: https://www.defesanet.com.br/tecnologia/noticia/1226/Cyberwar---EUA-preveem-resposta-militar-a-ataque-de-hackers. Acesso em: 20 out. 2020.

FERNANDES, Daniela. "Gigantes da web são novo Estado", diz Pierre Lévy. *Valor Econômico*. 23 out. 2020. Disponível em: https://valor.globo.com/eu-e/noticia/2020/10/23/gigantes-da-web-sao-novo-estado-diz-pierre-levy.ghtml. Acesso em: 2 out. 2020.

FERREIRA, Pedro Moura. Opinião. Será que possui efetivamente a melhor estratégia para combater o 'cyber risk'? *In*: *Jornal Econômico* n. 2025; JE MAIS SEGURO. Portugal, 24 jan. 2020, p.2. Disponível em: https://leitor.jornaleconomico.pt/download?token=91ab9992c7a24e59bd48f5028d952ddc&file=SUP_MS_2025.pdf. Acesso em: 15 set. 2020.

GENEVA. The Geneva Association, *Cyber Insurance as a Risk Mitigation Strategy* (April 2018). Disponível em: https://www.genevaassociation.org/sites/default/files/research-topics-

document-type/pdf_ public/cyber_insurance_as_a_risk_mitigation_strategy.pdf. Acesso em: 10 out. 2020.

HISCOX. *Hiscox Cyber Readiness Report*, 2018. Disponível em: https://www.hiscox.co.uk/cyberreadiness. Acesso em: 10 out. 2020. (HISCOX, 2018)

INFORMATION COMISSIONER'S OFFICE. For organisations/Guide to Data Protection/*Guide to the General Data Protection Regulation* (GDPR)/Principles, UK, 2020. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/. Acesso em: 15 set. 2020.

IOSCO. *Cyber Security in Securities Markets – An International Perspective*: Report on IOSCO's cyber risk coordination efforts. April 2016. Disponível em: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf. Acesso em: 2 set. 2020.

IOSCO. *Cyber Task Force*: Final Report. June 2019. Disponível em: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf. Acesso em: 2 set. 2020.

KPMG. *Closing the gap*: Insuring your business against evolving cyber threats. 12 July 2017. Disponível em: https://home.kpmg/xx/en/home/insights/2017/07/closing-the-gap-insuring-your-business-against-evolving-cyber-threats.html. Acesso em: 15 set. 2020.

LÉVY, Pierre. *Cibercultura*. Tradução Carlos Irineu da Costa. São Paulo: Editora 34, 1999, 264 p. Disponível em: https://mundonativodigital.files.wordpress.com/2016/03/cibercultura-pierre-levy.pdf. Acesso em: 15 out. 2020.

MADEIRA, João. Fórum com consultoras. Cibersegurança é prioritária nas organizações. *In*: *Jornal Econômico* n. 2025; JE MAIS SEGURO. Portugal, 24 jan. 2020, p.4. Disponível em: https://leitor.jornaleconomico.pt/download?token=91ab9992c7a24e59bd48f5028d952ddc&file=SUP_MS_2025.pdf. Acesso em: 15 set. 2020.

MARSH. Pesquisas e Informativos, 2018. Um ano após o ataque do Notpetya fica a pergunta: foi uma Guerra Cibernética? Disponível em: https://www.marsh.com/br/insights/research/um-ano-apos-o-ataque-do-notpetya-fica-a-pergunta--foi-uma-guerra.html. Acesso em: 15 set. 2020.

MOURA JR., Paulo Leão de. Considerações sobre Risco Cibernético. *Revista Opinião*. Seg nº 14. Editora Roncaracti**,** jul. 2017. Disponível em: https://www.editoraroncarati.com.br/v2/Artigos-e-Noticias/Artigos-e-Noticias/Consideracoes-sobre-Risco-Cibernetico.html. Acesso em: 20 out. 2020.

OECD. *Enhancing the Role of Insurance in Cyber Risk Management*, OECD Publishing, Paris. Dez. 2017. Disponível em: https://www.oecd-ilibrary.org/docserver/9789264282148-en.pdf?expires=1604617370&id=id&accname=guest&checksum=89896F127DC6F928ED34FE77401A2C7A. Acesso em: 10 out. 2020. (OCDE, 2017a)

OECD. *Supporting an Effective Cyber Insurance Market* (May 2017). Disponível em: https://www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf. Acesso em: 10 out. 2020. (OCDE, 2017b)

PORUP, J. M*. 5 aspectos que você deve saber sobre seguros cibernéticos*. CIO, 18 fev. 2020. Disponível em: https://cio.com.br/gestao/5-aspectos-que-voce-deve-saber-sobre-seguros-ciberneticos/. Acesso em: 20 out. 2020.

PWC. Sinopse Normativa Nacional. *Demonstrações Financeiras e Sinopses Normativa e Legislativa, Guia 2018/2019*. Disponível em: https://www.pwc.com.br/pt/guia/assets/2018/sinopse-normativa-nacional-cpc.pdf. Acesso em: 10 out. 2020.

PWC. *Demonstrações Financeiras e Sinopses Normativa e Legislativa, Guia 2019/2020*. Disponível em: https://www.pwc.com.br/pt/estudos/guia-demonstracoes-financeiras/2019/guia-demo-financeira-19-20.pdf. Acesso em: 10 out. 2020.

ROSSINI, Augusto Eduardo de Souza. Brevíssimas considerações sobre delitos informáticos. São Paulo: ESMP, jul. 2002. p. 131-142 (*Caderno Jurídico*, ano 02, n. 04). Disponível em: http://www.mpsp.mp.br/portal/page/portal/Escola_Superior/Biblioteca/Cadernos_Tematicos/direito_e_internet.pdf. Acesso em: 15 set. 2020.

SCHUH, Marta Helena. *Resolução do Bacen equipara risco cibernético a risco operacional*. MARSH, 4 mar 2020. Disponível em: https://www.marsh.com/br/insights/risk-in-context/risco-cibernetico-e-risco-operacional.html#:~:text=a%20circular%20bacen%20n%c2%ba3.,risco%20cibern%c3%a9tico%20ao%20risco%20operacional. Acesso em: 2 out. 2020.

SINDSEGSP. Notícias. *Seguro é alternativa para diluir riscos cibernéticos*. Valor Econômico, 19 out. 2020. Disponível em: https://www.sindsegsp.org.br/site/noticia-texto.aspx?id=33334. Acesso em: 20 out. 2020.

SLTTGCC. Whitepaper: *Cyber Liability InsuranceOverview*. Sponsored by the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), Jun 2016. Disponível em: https://thecepp.org/uploads/3/5/5/1/35514945/slttgcc_-_cyber_liability_insurance_2016_06_17_final.pdf. Acesso em: 15 set. 2020.

SOUZA, Ramon. THE HACK. *Seguros cibernéticos*: o que são e porque estão fazendo sucesso no Brasil. 2019. Disponível em: https://thehack.com.br/seguros-ciberneticos-o-que-sao-e-porque-estao-fazendo-sucesso-no-brasil/. Acesso em: 20 out. 2020.

SUSEP. Glossário. *Verbete "SEGURO"*. Disponível em: http://www.susep.gov.br/menu/informacoes-ao-publico/glossario. Acesso em: 2 out. 2020.

TEIXEIRA, Andreia. AON.pt. *Mecanismos de gestão do risco e mitigação do impacto*. Como aliar a prevenção à resposta. Lisboa, 21 jun. 2017. Disponível em: http://cip.org.pt/wp-content/uploads/2017/06/Andreia-Teixeira-Aon.pdf. Acesso em: 2 out. 2020.

VITTA, de Lucas. Adoção do home office em grande parte do mundo está sendo explorada na busca de dados. *Valor Econômico*, 04 ago. 2020. Disponível em: https://valor.globo.com/mundo/noticia/2020/08/04/interpol-alerta-para-crescimento-de-crimes-virtuais-durante-a-pandemia.ghtml. Acesso em: 15 set. 2020.

WORLD ECONOMIC FORUM. *The Global Risks Report 2019*, 14th Edition. Geneva, Switzerland, 2019. Disponível em: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf. Acesso em: 15 out. 2020.

Estratégia Nacional de Segurança Cibernética (E-ciber): comparativo com estratégias de outros países

Patricy Barros Justino

Luciana Quagliane Ribeiro

Resumo: O presente artigo tem como objetivo realizar uma análise do ponto de vista comparativo, entre a Estratégia Nacional de Segurança Cibernética (E-Ciber) brasileira, sua inter-relação com a Política Nacional de Segurança da Informação (PNSI) e outras estratégias elaboradas pelo Chile, União Europeia e aquelas internalizadas por Portugal. A E-Ciber contém uma orientação do governo à sociedade, a respeito das ações planejadas para o quadriênio 2020/2023. O presente artigo realiza uma análise de estratégias equivalentes na União Europeia, Chile e Portugal. Inicialmente são tratados conceitos considerados relevantes para o tema, em uma abordagem conceitual e contextual. Em seguida, são identificados os principais elementos dessas estratégias e seus pontos de semelhanças e diferenças, bem como os desafios a serem enfrentados. Em relação à metodologia, foi utilizado o levantamento legislativo-documental e histórico, sendo analisadas normas produzidas pelos Poderes Legislativo e Executivo nacional, cuja abrangência esteja relacionada ao tema principal do presente trabalho. O conhecimento da análise destas diferentes abordagens traz elementos, por exemplo, para a formação e capacitação de pessoas e o apoio à elaboração de planos de implantação de segurança cibernética em organizações brasileiras.
Palavras-chave: Brasil. Chile. E-Ciber. Portugal. União Europeia.

1 Introdução

Para contextualizar a relevância do tema "Segurança Cibernética" no Brasil, citamos o Relatório do XIII Encontro Nacional de Estudos Estratégicos (XIII ENEE), realizado em Brasília, em 2013, que tratou do tema "O setor cibernético brasileiro":

> A segurança e a defesa cibernética são vetores estratégicos para o Estado, na medida em que afetam positiva ou negativamente aspectos políticos, econômicos e sociais do cotidiano da sociedade da informação. O próprio conceito de realidade foi expandido pelo ambiente virtual.
> Segurança diz respeito à sensação de garantia necessária e indispensável a uma sociedade e a cada um de seus integrantes, contra ameaças de qualquer natureza. Ao Estado compete garantir a segurança de todos, pois a todos deve e pode exigir o cumprimento dos deveres e funções necessários à manutenção dessa condição.
> A segurança cibernética, engloba a defesa cibernética, diz respeito a uma atividade abrangente que congrega uma série de aspectos, que vão da proteção física e lógica da informação, em qualquer meio onde ela esteja abrigada, à proteção dos sistemas e redes de informação. Abrange, ainda, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações computacionais destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento – ou seja, um conjunto de ativos de informação denominado de Infraestrutura Crítica da Informação. (BRASIL, 2013).

Para garantir o rigor na conceituação, não é possível prescindir de recordar alguns conceitos já consagrados em literatura oficial, quais sejam: Cibernética, Segurança Cibernética, Defesa Cibernética, Espaço Cibernético e Guerra Cibernética, termos que são largamente empregados no decorrer do presente artigo.

Os conceitos a seguir são aqueles constantes da publicação "Desafios estratégicos para segurança e defesa cibernética":

> Cibernética – Termo que se refere ao uso de redes de computadores e de comunicações e sua interação dentro de sistemas utilizados por instituições públicas e privadas, de cunho estratégico, a exemplo do MD/FA. No campo da Defesa Nacional, inclui os recursos informatizados que compõem o Sistema Militar de Comando e Controle (SISMC^2) bem como os sistemas de armas e de vigilância.
> Defesa Cibernética – Conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente. No contexto do preparo e emprego operacional, tais ações caracterizam a Guerra Cibernética.
> Segurança Cibernética – Refere à proteção e garantia de utilização de ativos de informação estratégicos, principalmente os ligados às infraestruturas críticas da informação (redes de comunicações e de computadores e seus sistemas informatizados) que controlam as infraestruturas críticas nacionais. Também abrange a interação com órgãos públicos e privados envolvidos no funcionamento das infraestruturas críticas nacionais, especialmente os órgãos da Administração Pública Federal (APF). (BARROS; GOMES; FREITAS, 2011, p. 17).

Para a Doutrina Militar de Defesa Cibernética (DMDC), a conceituação é a que se segue:

> 2.2.4 Cibernética - termo que se refere à comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação. No campo da Defesa Nacional, inclui os recursos de tecnologia da informação e comunicações de cunho estratégico, tais como aqueles que compõem o Sistema Militar de Comando e Controle (SISMC^2), os sistemas de armas e vigilância, e os sistemas administrativos que possam afetar as atividades operacionais.
> 2.2.5 Defesa Cibernética - conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente.
> 2.2.8 Espaço Cibernético - espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas.
> 2.2.10 Guerra Cibernética - corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios

> STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC. (BRASIL, 2014b).

O contexto mundial, face à evolução experimentada pela Tecnologia da Informação e Comunicações (TIC), a partir da segunda metade do século passado, com o advento da internet, permitiu benefícios inúmeros, conferidos pela circulação da informação em tempo real e em nível mundial. No entanto, paradoxalmente, surge um novo tipo de ameaça, a cibernética, que desconhece fronteiras e possui potencial para causar grandes prejuízos. Assim, o espaço cibernético constitui-se um novo e promissor cenário para a prática de toda a sorte de atos ilícitos, incluindo o crime, o terrorismo e o contencioso bélico entre nações.

No Brasil, em 2000, o número de usuários da internet girava em torno de 8,6 milhões e o governo brasileiro alertava que tal número era bastante limitado e precisaria crescer significativamente. Naquele ano, estimava-se que apenas 1% dos usuários da internet no Brasil compraria em lojas virtuais, com média de gasto de apenas 18 dólares mensais. Em 2014, o Brasil é considerado o quarto maior mercado mundial no setor de TIC, movimentando cerca de US$ 170 bilhões, e somente o comércio eletrônico faturou cerca de 35,8 bilhões de reais, e no mundo o movimento foi de cerca de 1,5 trilhões de dólares, demonstrando quão aquecida e intensiva vem sendo a economia digital e com tendência ascendente forte. Para 2020, estima-se um mercado global de TI na ordem de US$ 3 trilhões e um mercado nacional da ordem de US$ 200 bilhões (BRASIL, 2015a).

Em agosto de 2019, segundo a pesquisa *TIC Domicílios*, 126,9 milhões de pessoas usaram a rede regularmente em 2018. E, ainda, observando que o número de brasileiros que usam a internet continua crescendo: subiu de 67% para 70% da população, o que equivale a 126,9 milhões de pessoas.[36]

Em relação à Estratégia Nacional de Segurança Cibernética (E-Ciber), tema central do nosso artigo, vale lembrar o contido no anexo da mencionada Estratégia Nacional: “é orientação manifesta do Governo federal à sociedade brasileira sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética e terá validade no quadriênio 2020-2023” (BRASIL, 2020a).

[36] Dados da pesquisa TIC Domicílios, divulgada em 28 ago. 2019, que afere dados sobre conexão à internet nas residências do país. A pesquisa, feita anualmente pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic), é uma das principais no país (LAVADO, 2019).

O presente artigo tem como objetivo realizar uma análise do ponto de vista comparativo, entre a E-Ciber brasileira, sua inter-relação com a Política Nacional de Segurança da Informação (PNSI) e outras estratégias elaboradas pelo Chile, União Europeia e aquelas internalizadas por Portugal.

Inicialmente, são tratados conceitos considerados relevantes para o tema, em uma abordagem conceitual e contextual. Em seguida, são identificados os principais elementos dessas estratégias e seus pontos de semelhanças e diferenças, bem como os desafios a serem enfrentados.

Com a pesquisa empreendida, entende-se que o conhecimento aqui disposto, bem como a análise realizada, trará elementos para formação e capacitação de pessoas, para apoio à elaboração de planos de implantação de segurança cibernética em organizações brasileiras, entre outros, isto para citar algumas oportunidades, entre as muitas que se apresentam.

2 Legislação brasileira sobre o setor cibernético

2.1 Legislação da Administração Pública Federal

Conforme consta da PNSI (BRASIL, 2018a), a segurança da informação abrange:

I. a segurança cibernética;
II. a defesa cibernética;
III. a segurança física e a proteção de dados organizacionais; e
IV. as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

Nesse sentido, esse documento é um balizador do tema no país. Os assuntos relacionados à Segurança da Informação e Comunicações (SIC) e a Segurança Cibernética, vêm se caracterizando cada vez mais como função estratégica de Estado, sendo essenciais à manutenção e preservação, tanto das infraestruturas críticas de um país, tais como Energia, Transporte, Telecomunicações, Águas, Finanças, a própria Informação, entre outras, quanto dos direitos individuais, em especial da privacidade e da soberania.

No Brasil, os assuntos relacionados à Segurança da Informação, Segurança Cibernética e Segurança das Infraestruturas Críticas são tratados no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), que é presidida pelo Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), conforme consta em Brasil (2019a; 2019b).

De acordo com Brasil (2019b), em seu inciso II do artigo 2º, "A Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo é órgão de assessoramento com a finalidade de":

> [...] aprovar, promover a articulação e acompanhar a implementação dos programas e ações cujas competências ultrapassem o escopo de apenas um Ministério, incluídos aqueles pertinentes a: [...]
> i) segurança de infraestruturas críticas;
> j) segurança da informação; e
> k) segurança cibernética; [...]

No Brasil, o tema "segurança da informação" teve como seu primeiro marco legal, no ano 2000, o lançamento da obra: "Sociedade da Informação no Brasil: livro verde" (TAKAHASHI, 2000), demonstrando as percepções do Ministério da Ciência e Tecnologia do Brasil sobre o tema mais geral da Sociedade da Informação; a abordagem do assunto Segurança da Informação, pela primeira vez na legislação federal, ocorreu no ano de 2000, com o Decreto 3.505/2000 (BRASIL, 2000), o qual instituía a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal (APF), que veio a ser revogado pelo Decreto nº 9.637, de 2018, que institui a PNSI (BRASIL, 2018a). O mesmo Decreto que dispõe sobre a PNSI, institui também, em seu Capítulo V, o Comitê Gestor da Segurança da Informação, com atribuição de assessorar o GSI/PR nas atividades relacionadas à segurança da informação.

Em respeito à coordenação das atividades de segurança da informação e das comunicações na APF, de acordo com a Lei 10.683, de 29 de maio de 2003 (BRASIL, 2003), é competência do GSI/PR. A estrutura do GSI/PR conta também com um órgão, cujas competências estão relacionadas especificamente à segurança da informação; trata-se da Assessoria Especial de Segurança da Informação, entre cujas competências está a de "supervisionar a formulação e a implementação de políticas públicas de segurança da informação" (BRASIL, 2019c).

O período iniciado em 2005 é aquele em que a temática da Segurança Cibernética adentra às preocupações da Defesa do Estado brasileiro. O marco inicial para as percepções brasileiras sobre a ameaça cibernética é a Política de Defesa Nacional, documento de alto nível no âmbito da política de defesa do Brasil; aprovado originalmente por meio do Decreto no 5.484, de 30 de junho de 2005, como Política de Defesa Nacional (PDN), o documento foi atualizado em 2012, passando a denominar-se Política Nacional de Defesa (PND) (BRASIL, 2020b).

Em 22 de julho de 2020, uma versão atualizada da PND foi encaminhada pelo Presidente da República para apreciação do Congresso Nacional, tendo em vista que estão previstas revisões quadrienais, conforme a Lei Complementar nº 97, de 9 de junho de 1999, e suas alterações (BRASIL, 1999). Outro momento na produção legal brasileira referente à Segurança Cibernética é a Estratégia Nacional de Defesa (END), cuja primeira edição foi publicada em 2008. Enquanto a PND apresenta os pressupostos básicos do país em relação à sua defesa e estabelece os Objetivos Nacionais de Defesa (OND), a Estratégia orienta todos os segmentos do Estado brasileiro quanto às medidas a serem implementadas para atingirem-se os objetivos estabelecidos (BRASIL, 2020b).

A END definiu os três setores considerados de importância estratégica para a defesa nacional, quais sejam: o nuclear, o espacial e o cibernético. Nesse contexto, a Segurança e a Defesa Cibernéticas surgem naturalmente como imperativos de proteção das infraestruturas críticas da informação associadas às infraestruturas críticas nacionais do Estado brasileiro. A mais recente atualização da END se deu por meio do Decreto Legislativo nº 179, de 2018 (CÂMARA DOS DEPUTADOS, 2018).

Cada um dos setores estratégicos definidos pela END está associado a uma Força responsável por seu desenvolvimento prioritário, ficando o setor nuclear a cargo da Marinha do Brasil (MB), o setor aeroespacial, com a Força Aérea Brasileira (FAB) e o cibernético, com o Exército Brasileiro (EB).

Com vistas a se organizar, institucionalmente, para responder à nova missão atribuída pela END, o Exército Brasileiro instituiu o "Setor Cibernético" em seu âmbito por meio da Portaria do Comandante do Exército nº 03-RES, de 29 de junho de 2009. Em 4 de agosto de 2010, o Exército decidiu, por meio da Portaria nº 666, criar o Centro de Defesa Cibernética do Exército.

Além destes, vários outros documentos merecem destaque, entre eles o Livro Verde de Segurança Cibernética no Brasil (BRASIL, 2010), que ressalta o seguinte: "A Segurança Cibernética, desafio do século XXI, vem se destacando como função estratégica de Estado e essencial à manutenção das infraestruturas críticas de um país, tais como: Energia, Defesa, Transporte, Telecomunicações, Finanças, da própria Informação, dentre outras."

Assim, deste ponto em diante, tratar-se-á da Legislação relativa ao Setor Cibernético na APF e no âmbito da Defesa, além de serem mencionadas outras obras ou eventos considerados relevantes.

2.2 Legislação no âmbito da Defesa

Como mencionado no item 2.1, os documentos fundamentais no trato de assuntos relacionados ao setor cibernético no país são: a PND e a END. Acrescente-se a estes, o Livro Branco da Defesa Nacional (LBDN) (BRASIL, 2012a), cuja primeira versão foi apresentada pelo Poder Executivo ao Congresso Nacional, na primeira metade da sessão legislativa ordinária de 2012. O LBDF se soma, assim, à END e à PND como documento esclarecedor das atividades de defesa do Brasil. É o 3º nível da PND (ou nível operacional).

Em 2010, a Diretriz Ministerial nº 14/2009 do MD (BRASIL, 2009) atribuiu ao Exército Brasileiro institucionalizar o Núcleo do Centro de Defesa Cibernética do Exército (Nu CDCiber). Em agosto do mesmo ano, foram aprovadas as portarias 666 e 667, do Comandante do Exército, criando o Centro de Defesa Cibernética do Exército (CDCiber) e ativando o Nu CDCiber, respectivamente, tornando realidade o Setor Cibernético do Exército Brasileiro.

Em 2012, foi editada a Política Cibernética de Defesa (PCD), aplicável a todos os componentes da expressão militar do Poder Nacional, bem como às entidades que venham a participar de atividades de Defesa ou de Guerra Cibernética (BRASIL, 2012b).

Em 2014, como medida para implementação das ações previstas na END, o Ministério da Defesa editou a Portaria Normativa MD n. 2.777, de 27 de outubro de 2014, que aprova a diretriz de implantação de medidas, com vistas à potencialização da Defesa Cibernética Nacional, e cria o Comando de Defesa Cibernética (ComDCiber) e a Escola Nacional de Defesa Cibernética (EnaDCiber), na Estrutura Regimental do Comando do Exército, com ênfase na implantação e na consolidação do Sistema de Homologação e Certificação de Produtos de Defesa Cibernética, no apoio à pesquisa e no desenvolvimento de produtos de defesa cibernética, bem como na criação do Observatório de Defesa Cibernética (BRASIL, 2014a).

A DMDC, também publicada em 2014, tem como finalidade:

> estabelecer os fundamentos da Doutrina Militar de Defesa Cibernética, proporcionando unidade de pensamento sobre o assunto, no âmbito do Ministério da Defesa (MD), e contribuindo para a atuação conjunta das Forças Armadas (FA) na defesa do Brasil no espaço cibernético. (BRASIL, 2014b).

Apresenta, ainda, entre outras, a conceituação de Sistema Militar de Defesa Cibernética (SMDC) como:

> um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar as atividades de defesa no Espaço Cibernético, assegurando, de forma conjunta, o seu uso efetivo pelas FA, bem como

> impedindo ou dificultando sua utilização contra interesses da Defesa Nacional. (BRASIL, 2014b).

Outros normativos completam o arcabouço legal da Defesa na área de Segurança da Informação e em relação ao setor cibernético. Entre estes, é possível mencionar a Política de Segurança da Informação para o Sistema Militar de Comando e Controle (SISMC²) (BRASIL, 2015b), que trata das diretrizes estratégicas para aperfeiçoar a gestão da SIC no âmbito desse sistema.

No âmbito do Exército, outros importantes normativos também foram aprovados, tais como o Manual de Campanha EB70-MC-10.232 Guerra Cibernética (BRASIL, 2017a).

3 Contexto atual do Setor Cibernético no País

3.1 Governança do Setor na Administração Pública Federal

De acordo com BRASIL (2010, p. 107), as atuações dos principais atores e órgãos do governo, no setor cibernético, dividem-se em duas vertentes:

a. Segurança Cibernética, contemplando ações que podem ser preventivas ou repressivas; e

b. Defesa Cibernética, mediante ações operacionais, caracterizadas por ações operacionais, de caráter defensivo e ofensivo.

Neste sentido, Carneiro (2012) apresenta um quadro-resumo da atuação desses atores, conforme se segue.

Quadro 11 – Formas de atuação de atores e órgãos do governo no setor cibernético

Vertente	Ações /Atitudes	Medidas
Segurança Cibernética	Preventivas	- Criação e aplicação de metodologias de gestão de risco - Desenvolvimento de planos de contingência e continuidade de infraestruturas críticas - Resposta à incidentes de rede - Correções contra artefatos maliciosos - Disseminação de melhores práticas para proteção de redes e segurança das informações - Especificação e desenvolvimento de algoritmos criptográficos e equipamentos de segurança cibernética
	Repressivas	- Identificação e combate à conduta criminosa caracterizada como crime cibernético - Medidas contra terrorismo cibernético e sabotagem
Defesa Cibernética	Ações operacionais ofensivas e defensivas	- Medidas contraterrorismo cibernético e sabotagem - Medidas de apoio às operações militares conduzidas em situação de emprego militar

Fonte: CARNEIRO, 2012.

Assim sendo, a seguir, mencionamos os órgãos e atores que compõem a estrutura da segurança da informação na APF.

De acordo com a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015/2018:

> o modelo de governança sistêmica de SIC e de Segurança Cibernética da APF – nível Político-Estratégico, de nível político estratégico, apoiará o estabelecimento de competências e respectivas responsabilidades entre os órgãos e entidades da APF de forma a: (i) somar e otimizar esforços; (ii) pactuar ações em prol dos avanços das áreas e efetividade nos resultados; (iii) buscar a excelência da gestão e da maturidade; (iv) estabelecer mecanismos e critérios de acompanhamento e avaliação contínuos; e (v) promover a articulação multissetorial e a inovação. (BRASIL, 2015a).

Após atualização de documentos que tratam da segurança informação e das comunicações no âmbito da Administração pública federal, mudanças foram visualizadas no papel dos atores envolvidos. Assim, conforme Brasil (2019c), ao GSI/PR compete (entre competências relacionadas a outros temas): coordenar as atividades de segurança da informação e das comunicações; planejar, coordenar e supervisionar a atividade de segurança da informação no âmbito da administração pública federal, nela incluídos a segurança cibernética, a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosa.

O documento normativo (BRASIL, 2018a), por sua vez, institui o Comitê Gestor de Segurança da Informação, com atribuição de assessorar o Gabinete de Segurança Institucional da Presidência da República nas atividades relacionadas à segurança da informação. O Comitê Gestor da Segurança da Informação poderá instituir subcolegiados com o objetivo de tratar de temáticas específicas relacionadas à segurança da informação.

O Comitê será composto por um representante titular e respectivo suplente, indicados pelos seguintes órgãos: I - Gabinete de Segurança Institucional da Presidência da República, que o coordenará; II - Casa Civil da Presidência da República; III - Ministério da Justiça; IV - Ministério da Segurança Pública; V - Ministério da Defesa; VI - Ministério das Relações Exteriores; VII - Ministério da Fazenda; VIII - Ministério dos Transportes, Portos e Aviação Civil; IX - Ministério da Agricultura, Pecuária e Abastecimento; X - Ministério da Educação; XI - Ministério da Cultura; XII - Ministério do Trabalho; XIII - Ministério do Desenvolvimento Social; XIV - Ministério da Saúde; XV - Ministério da Indústria, Comércio Exterior e Serviços; XVI - Ministério de Minas e Energia; XVII - Ministério do Planejamento,

Desenvolvimento e Gestão; XVIII - Ministério da Ciência, Tecnologia, Inovações e Comunicações; XIX - Ministério do Meio Ambiente; XX - Ministério do Esporte; XXI - Ministério do Turismo; XXII - Ministério da Integração Nacional; XXIII - Ministério das Cidades; XXIV - Ministério da Transparência e Controladoria-Geral da União; XXV - Ministério dos Direitos Humanos; XXVI - Secretaria-Geral da Presidência da República; XXVII - Secretaria de Governo da Presidência da República; XXVIII - Advocacia-Geral da União; e XXIX - Banco Central do Brasil (BACEN), conforme Brasil (2018a).

3.2 Governança do setor cibernético no âmbito da Defesa

A END, aprovada pelo Decreto nº 6.703, de 18 de dezembro de 2008, e posteriormente atualizada em 2013 e 2018[37], afirma:

> A análise das hipóteses de emprego das Forças Armadas – para resguardar o espaço aéreo, o território e as águas jurisdicionais brasileiras – permite dar foco mais preciso às diretrizes estratégicas. Nenhuma análise de hipóteses de emprego pode, porém, desconsiderar as ameaças do futuro. Por isso mesmo, as diretrizes estratégicas e as capacitações operacionais precisam transcender o horizonte imediato que a experiência e o entendimento de hoje permitem descortinar. (CÂMARA DOS DEPUTADOS, 2018).

A END estabelece três setores estratégicos essenciais para a Defesa Nacional – o espacial, o cibernético e o nuclear:

> Ao lado da destinação constitucional, das atribuições, da cultura, dos costumes e das competências próprias de cada Força e da maneira de sistematizá-las em uma estratégia de defesa integrada, aborda-se o papel de três setores decisivos para a defesa nacional: o espacial, o cibernético e o nuclear. Descreve-se como as três Forças devem operar em rede – entre si e em ligação com o monitoramento do território, do espaço aéreo e das águas jurisdicionais brasileiras. (CÂMARA DOS DEPUTADOS, 2018).

Com vistas a dar provimento ao estabelecido na END para os três setores estratégicos, o Ministério da Defesa emitiu, em 9 de novembro de 2009, a Diretriz Ministerial nº 014, definindo responsabilidades sobre a coordenação e a liderança na condução das ações referentes aos setores nuclear, cibernético e espacial, respectivamente, à Marinha, ao Exército e à Aeronáutica.

Em relação ao setor cibernético, a END define prioridades: “No setor cibernético, as capacitações se destinarão ao mais amplo espectro de usos industriais, educativos e militares” (CÂMARA DOS DEPUTADOS, 2018). Incluirão, como parte prioritária, as tecnologias de

[37] Estratégia Nacional de Defesa: atualizada por meio do Decreto Legislativo nº 373, de 2013 e posteriormente pelo Decreto Legislativo nº 179, de 2018.

comunicação entre todos os contingentes das Forças Armadas, de modo a assegurar sua capacidade para atuar em rede. As prioridades são as seguintes:

(a) fortalecer o Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas;

(b) aprimorar a SIC, particularmente, no tocante à cerificação digital no contexto da Infraestrutura de Chaves-Públicas da Defesa (ICP-Defesa), integrando as ICP das três Forças;

(c) fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional. Nesse contexto, os Ministérios da Defesa, da Economia, da Ciência, Tecnologia e Inovação, da Educação, a Secretaria de Assuntos Estratégicos da Presidência da República (SAE) e o GSI/PR deverão elaborar estudo com vistas à criação da EnaDCiber;

(d) desenvolver sistemas computacionais de defesa baseados em computação de alto desempenho para emprego no setor cibernético e com possibilidade de uso dual;

(e) desenvolver tecnologias que permitam o planejamento e a execução da Defesa Cibernética no âmbito do Ministério da Defesa e que contribuam com a segurança cibernética nacional, tais como sistema modular de defesa cibernética e sistema de segurança em ambientes computacionais;

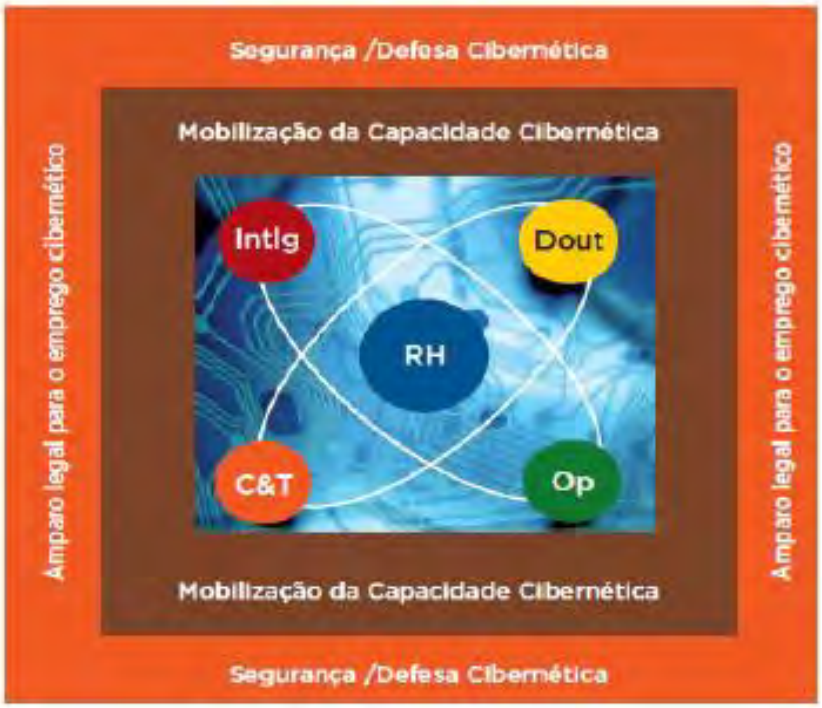
(f) desenvolver a capacitação, o preparo e o emprego dos poderes cibernéticos operacional e estratégico, em prol das operações conjuntas e da proteção das infraestruturas estratégicas;

(g) incrementar medidas de apoio tecnológico por meio de laboratórios específicos voltados para as ações cibernéticas; e

(h) estruturar a produção de conhecimento oriundo da fonte cibernética.

Conforme ressalta Costa (2013), a Figura abaixo sintetiza uma visão inicial e geral de como se pretende organizar os diversos projetos fundamentais que possuem áreas e requisitos indispensáveis à consolidação do Setor Cibernético na Defesa, enfatizando-se a sua integração e o trabalho conjunto.

Figura 12 – Visualização do setor cibernético na Defesa brasileira



Fonte: COSTA, 2013.

Verifica-se, nessa figura, que a capacitação de recursos humanos constitui a atividade prioritária na consolidação do Setor Cibernético, uma vez que ela proporciona as capacitações cibernéticas, no dizer da própria END, indispensáveis para mobiliar os quatro vetores que o integram: a inteligência; a doutrina; a ciência, tecnologia e inovação; e as operações.

A mobilização da capacidade cibernética em nível nacional, atrelada ao amparo legal para a atuação do setor, proporciona os necessários recursos materiais e humanos, com respaldo para a realização das ações no espaço cibernético que caracterizam a defesa cibernética.

Quanto à segurança cibernética, esta faz parte dessa visualização porque o MD dela participa como órgão da APF.

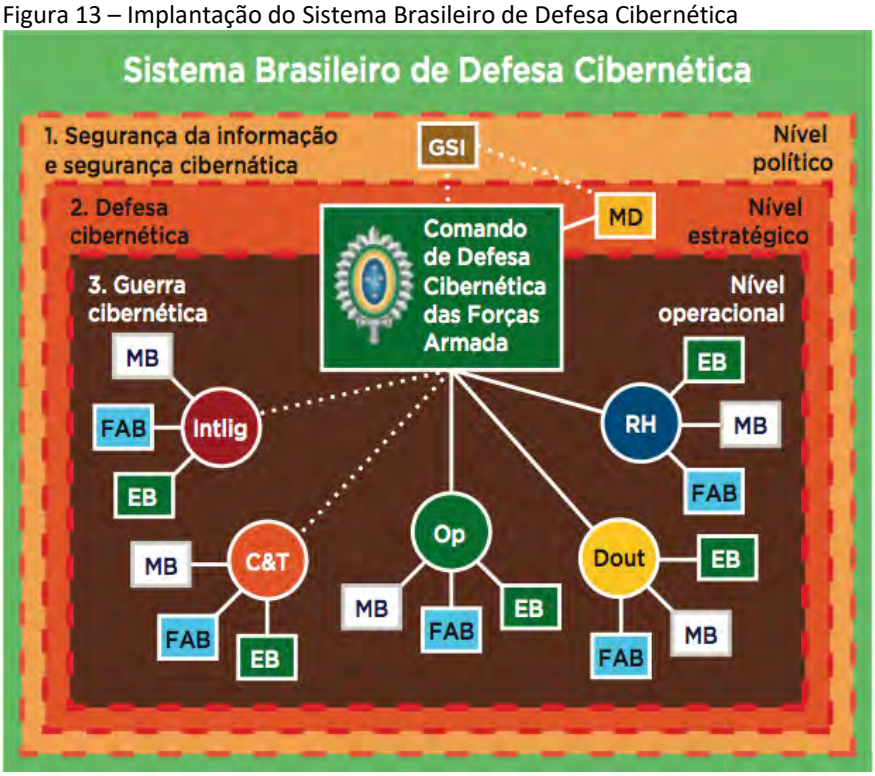
Na Diretriz Ministerial nº 014/MD supramencionada, ficou estabelecido que os trabalhos deveriam ser desenvolvidos em duas fases:

• na primeira, entendida como política, foram definidos os objetivos setoriais e a abrangência do tema; e

• na segunda, foram definidas as ações estratégicas e elaboradas as propostas de estruturas, com o máximo aproveitamento e adequação das já existentes.

A fim de serem atendidos os objetivos da END referentes à Defesa Cibernética, visualiza-se a implantação do SBDC, conforme ilustrado na figura abaixo.

Figura 13 – Implantação do Sistema Brasileiro de Defesa Cibernética



Fonte: http://defesacibernetica.ime.eb.br.

De acordo com a DMDC,

> a partir do estabelecimento do Setor Cibernético, decorrente da aprovação da Estratégia Nacional de Defesa, em 2008, dois campos distintos passaram a ser reconhecidos: a Segurança Cibernética, a cargo da Presidência da República (PR), e a Defesa Cibernética, a cargo do Ministério da Defesa, por meio das Forças Armadas. (BRASIL, 2014b).

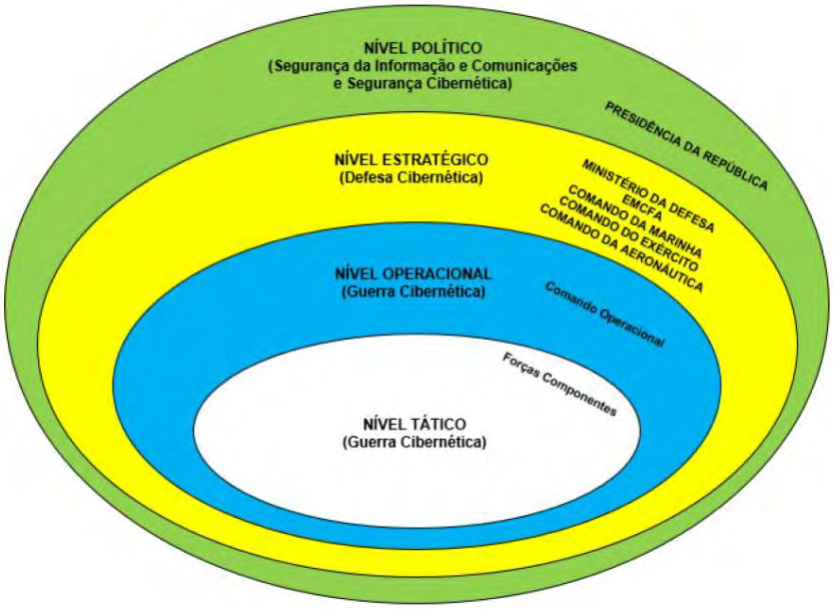
No contexto do Ministério da Defesa, as ações no Espaço Cibernético deverão ter as seguintes denominações, de acordo com o nível de decisão, conforme apresentado na figura mais abaixo:

‣ nível político - Segurança da Informação e Comunicações e Segurança Cibernética - coordenadas pela Presidência da República e abrangendo a Administração Pública Federal direta e indireta, bem como as infraestruturas críticas da Informação Nacionais;

‣ nível estratégico - Defesa Cibernética - a cargo do Ministério da Defesa, Estado-Maior Conjunto das Forças Armadas (EMCFA) e Comandos das FA, interagindo com a Presidência da República e a APF; e

‣ níveis operacional e tático - Guerra Cibernética - denominação restrita ao âmbito interno das Forças Armadas.

Figura 14 – Níveis da Segurança e Defesa Cibernética no Brasil



Fonte: BRASIL, 2014b.

3.2.1 O Setor Cibernético no Ministério da Defesa

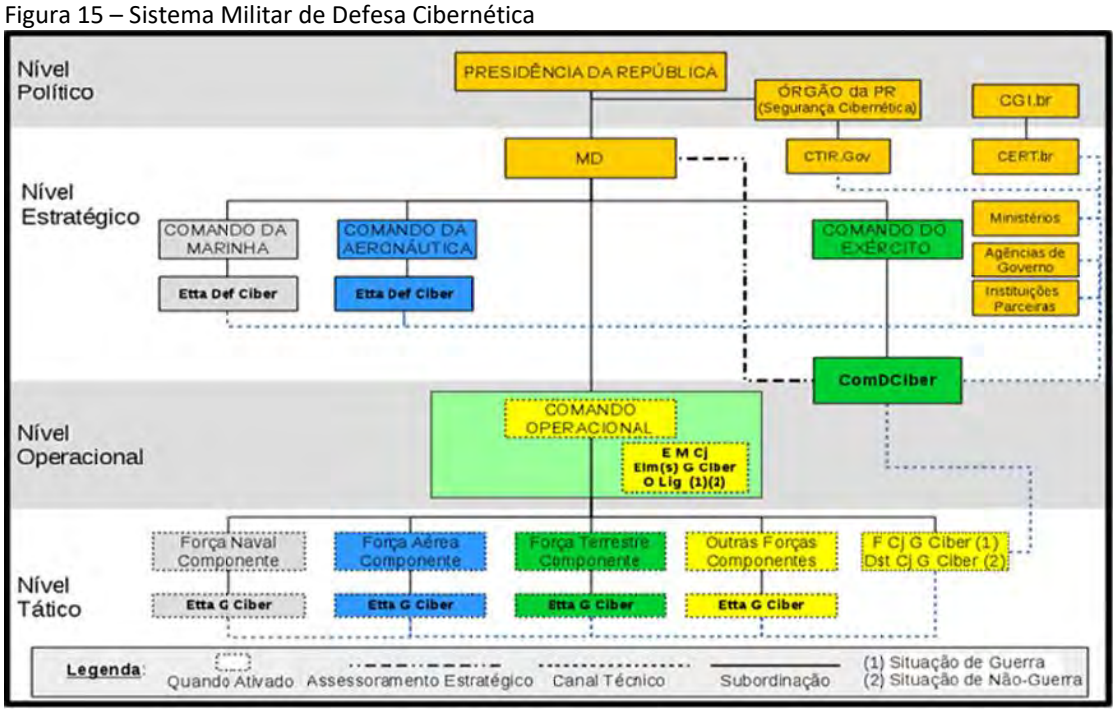
As Forças Armadas (FA) atualmente exercem a proteção de suas estruturas instaladas no território nacional de forma independente, sem a coordenação do Ministério da Defesa (MD). O MD somente passou a dar relevância ao setor cibernético com a aprovação da Estratégia Nacional de Defesa, em 18 de dezembro de 2008.

No Ministério da Defesa, compete ao EMCFA, além das demais competências previstas, aquela constante no Art. 10, inciso VI do Decreto que define a estrutura regimental doo Ministério (BRASIL, 2018b): “acompanhamento dos setores estratégicos nuclear, cibernético e espacial definidos na Estratégia Nacional de Defesa e distribuídos, respectivamente, aos Comandos da Marinha, do Exército e da Aeronáutica”. Ainda, o inciso VIII do artigo 14 prevê que, entre as competências da Subchefia de Comando e Controle, está a de:

> acompanhar os assuntos relacionados a sistemas de comando e controle, tecnologia da informação e comunicação, interoperabilidade, guerra centrada em redes, setor cibernético, infraestruturas críticas, segurança da informação e das comunicações e comunicações por satélites, para apoio às operações conjuntas. (BRASIL, 2018b).

A figura a seguir representa o Modelo de Governança do Setor Cibernético no âmbito da defesa.

Figura 15 – Sistema Militar de Defesa Cibernética



Fonte: BRASIL, 2014b.

4 A Estratégia Nacional de Segurança Cibernética (e-Ciber)

4.1 A Estratégia Nacional de Segurança Cibernética brasileira

A PNSI, conforme supramencionado, dispõe sobre a governança da informação, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e autenticidade da informação em nível nacional. São instrumentos da PNSI: a Estratégia Nacional de Segurança da Informação; e os planos nacionais. A PNSI prevê ainda que (art. 6º):

> A Estratégia Nacional de Segurança da Informação conterá as ações estratégicas e os objetivos relacionados à segurança da informação, [...], e será dividida nos seguintes módulos, entre outros, a serem definidos no momento de sua publicação:
> I - segurança cibernética;
> II - defesa cibernética;
> III - segurança das infraestruturas críticas;
> IV - segurança da informação sigilosa; e
> V - proteção contra vazamento de dados. (BRASIL, 2018a).

De acordo com o Decreto que aprova a E-Ciber (BRASIL, 2020a),

> Em cumprimento ao estabelecido na Política Nacional de Segurança da Informação, e considerada a Segurança Cibernética - Seg Ciber como a área mais crítica e atual a ser abordada, o Gabinete de Segurança Institucional da Presidência da República elegeu, em janeiro de 2019, a Estratégia Nacional de Segurança Cibernética - E-Ciber

> como primeiro módulo da Estratégia Nacional de Segurança da Informação, a seu cargo, a ser elaborada.

Em relação à elaboração do documento, o mesmo documento destaca ainda que, para elaboração da E-Ciber, foi adotada uma metodologia, e que sua construção é resultado de trabalho realizado por representantes de órgãos públicos, de entidades privadas e do meio acadêmico que participaram de uma série de reuniões técnicas para debaterem vários aspectos da segurança cibernética. Ao considerar a vasta gama de assuntos, esses representantes foram divididos em três subgrupos, constituídos do seguinte modo:

- Subgrupo 1 - governança cibernética, dimensão normativa, pesquisa, desenvolvimento e inovação, educação, dimensão internacional e parcerias estratégicas.;

- Subgrupo 2 - confiança digital e prevenção e mitigação de ameaças cibernéticas; e

- Subgrupo 3 - proteção estratégica - proteção do Governo e proteção às infraestruturas (BRASIL, 2020a).

Foram realizadas trinta e uma reuniões dos subgrupos, com a participação efetiva de todos esses representantes de notável saber, o que possibilitou o intercâmbio de conhecimentos e de ideias que contribuíram de forma decisiva para o estabelecimento da concepção estratégica.

Com o fim de estruturar os debates, o trabalho seguiu quatro etapas.

Primeira - Diagnóstico - levantamento e mapeamento de iniciativas, atores relacionados e ações existentes;

Segunda - Debates dos subgrupos - reuniões semanais com os atores relacionados e convidados de notório saber;

Terceira - Consulta pública - disponibilização do documento na internet para contribuições e ampla participação da sociedade em geral; e

Quarta - Aprovação e publicação - finalização da proposta e submissão à aprovação presidencial.

Adicionalmente, foi considerado o modelo de maturidade da capacidade em segurança cibernética, que define cinco dimensões:

- política e estratégia de segurança cibernética;

- cultura cibernética e de sociedade;

- educação, de treinamento e de habilidades em segurança cibernética;

- marcos legais e regulatórios; e

- padrões, organizações e tecnologias.

Essas dimensões, por sua transversalidade, abrangem as extensas áreas que devem ser consideradas no aumento da capacidade em segurança cibernética. Ao considerar as cinco dimensões do modelo, chegou-se à estrutura de sete eixos de atuação da estratégia, que mantém relação direta com o modelo de maturidade da capacidade em segurança cibernética.

Os eixos temáticos da E-Ciber foram considerados de forma transversal e podem ser descritos deste modo.

- Eixos de Proteção e Segurança: governança da segurança cibernética nacional; universo conectado e seguro: prevenção e mitigação de ameaças cibernéticas; e proteção estratégica; e
- Eixos Transformadores: dimensão normativa; dimensão internacional e parcerias estratégicas; pesquisa, desenvolvimento e inovação; e educação.

Essa metodologia descrita permitiu o levantamento de informações relevantes, que resultaram em uma concepção estratégica nacional sistêmica.

- Objetivos estratégicos da E-Ciber

São os objetivos estratégicos:

1. tornar o Brasil mais próspero e confiável no ambiente digital;

2. aumentar a resiliência brasileira às ameaças cibernéticas; e

3. fortalecer a atuação brasileira em segurança cibernética no cenário internacional.

- Ações estratégicas da E-Ciber

1. Fortalecer as ações de governança cibernética.

Fortalecer as ações de governança em segurança cibernética, por parte do setor público e do setor privado, que contemplem iniciativas relacionadas à gestão de pessoas, ao atendimento aos requisitos de segurança cibernética e à gestão dos ativos de informação.

2. Estabelecer um modelo centralizado de governança no âmbito nacional.

Estabelecer um modelo centralizado de governança para o país, por meio da criação de um sistema nacional de segurança cibernética.

3. Promover ambiente participativo, colaborativo, confiável e seguro entre setor público, setor privado e sociedade.

Promover um ambiente participativo, colaborativo e seguro entre as organizações públicas, as instituições privadas, a academia e a sociedade, por meio do acompanhamento contínuo e proativo das ameaças e dos ataques cibernéticos.

4. Elevar o nível de proteção do Governo.

Elevar o nível de proteção do Governo, por meio de ações no campo cibernético.

5. Elevar o nível de proteção das Infraestruturas Críticas Nacionais.

Proporcionar às infraestruturas críticas maior resiliência que possibilite a contínua prestação de serviços essenciais.

6. Aprimorar o arcabouço legal sobre segurança cibernética.

Para aprimorar o arcabouço legal sobre segurança cibernética, revisar e atualizar os normativos existentes, abordar novas temáticas e elaborar novos instrumentos.

7. Incentivar a concepção de soluções inovadoras em segurança cibernética.

Buscar o alinhamento entre os projetos acadêmicos e as necessidades da área produtiva, de modo a incentivar a pesquisa e o desenvolvimento de soluções em segurança cibernética que tragam a necessária inovação aos produtos nacionais nessa área crítica, atual e imprescindível.

8. Ampliar a cooperação internacional do Brasil em Segurança cibernética.

Ampliar a cooperação do Brasil, em segurança cibernética, com o maior número possível de países, de forma transparente, e reforçar a posição do país na constante busca pela paz e pela segurança internacional, conforme a tradição da diplomacia nacional baseada nos princípios estabelecidos no art. 4º da Constituição.

9. Ampliar a parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade.

Ampliar parcerias entre os diversos setores da sociedade, com vistas a elevar, de modo geral, o nível de segurança cibernética. Visualiza-se a efetiva cooperação do setor produtivo com a academia, por meio de recursos financeiros e materiais e, conforme apresentadas suas necessidades, investir na formação de universitários.

10. Elevar o nível de maturidade da sociedade em segurança cibernética.

Elevar o nível de maturidade em segurança cibernética da sociedade, com o fim de ensejar a compreensão das ameaças e dos riscos no espaço cibernético, e possibilitar às pessoas o uso adequado e oportuno de procedimentos e de ferramentas em prol da utilização segura do ambiente digital.

Em termos da repercussão da E-ciber na sociedade, destacamos aspectos positivos pontuados, tais como: a preocupação com a educação digital no documento (MIGALHAS, 2020). Outros aspectos são abordados por Luca (2020), em relação à tipificação de crimes cibernéticos, pois o Novo Código Penal se debruçou muito sobre o tema. Como a estratégia trata de novas tipificações crimes cibernéticos, embora não especifique quais serão eles, o questionamento é que se poderia pensar em extorsão ou estelionato. Isso gera preocupação porque, em geral, defende-se que esses crimes sejam qualificados de forma independente dos meios onde são praticados.

Assim, após uma breve análise quanto às características da E-ciber brasileira, passamos a tratar do comparativo entre as Estratégias de Cibersegurança na União Europeia, em Portugal e no Chile.

Para o item seguinte, selecionamos a União Europeia para o estudo, tendo em vista que o bloco europeu está à frente na regulamentação de aspectos específicos relativos à segurança cibernética, como também em relação ao cibercrime. Em relação a Portugal, pelo país fazer parte da União Europeia e de outras organizações internacionais, no âmbito da cooperação multilateral, como a Organização do Tratado do Atlântico Norte (OTAN), aliança militar de defesa coletiva entre países norte-americanos e europeus, instituída pelo Tratado de Washington em 4 de abril de 1949, sendo, inclusive, um dos fundadores da organização e também membro da OCDE. Nesse sentido, de acordo com as regras das organizações mencionadas, os estados-membros precisam ter sua regulação interna alinhada àquela das organizações. Além desses aspectos, Portugal é um dos países da União Europeia que regulamentaram aspectos específicos de acesso à internet e cibercrime, possuindo regulações exclusivas.

Em relação ao Chile, por ser, até 2020, o único país da América do Sul a fazer parte da OCDE e possuir vasto arcabouço legal sobre o tema, sobre cibercrimes e possuir uma estrutura robusta no país para tratar desses assuntos. Vale ressaltar que, recentemente, em 28 de abril de 2020, a República da Colômbia se tornou o 37º país a juntar-se à Organização e o segundo da América do Sul a integrar a Organização.

4.2 Comparativo entre a E-Ciber brasileira e a de outros países

4.2.1 O caso da União Europeia

Conforme registra Aparício (2017), em 2012, no âmbito da Cimeira de Chicago, os Chefes de Estado e Governo da OTAN constataram o registro de um número crescente de ciberataques, tendo os mesmos evoluído, tanto em sofisticação como em complexidade. Desse modo, de acordo com o autor, foi assumido pelos líderes dos estados-membros da organização o seu empenho em continuar a desenvolver as capacidades de ciberdefesa da OTAN, a par com o apelo à necessidade de maior cooperação entre os estados-membros no domínio da segurança cibernética (APARÍCIO, 2017, p. 57).

Muito em decorrência desses fatos, em 2013, foi publicada a Estratégia de Cibersegurança da União Europeia (EUROPEAN COMISSION, 2013). Segundo Christou (2018, p. 16, *apud* Geraldes 2019, p. 104-105), o desenvolvimento da Estratégia de Segurança Cibernética no seio da União Europeia tem sido justificado pela acumulação de ameaças às redes e aos sistemas informáticos europeus, que deu lugar a uma crescente percepção de vulnerabilidade, traduzindo-se no desenvolvimento de políticas, institucionalização de órgãos e de procedimentos.

Geraldes (2019, p. 102-103) destaca que 2013 foi um ano decisivo em matéria de Segurança Cibernética no âmbito da União Europeia, pois foi publicada a Estratégia de Cibersegurança (ECS, de *Cybersecurity Strategy of the European Union*), resultante de um esforço conjunto entre a Comissária para os Assuntos Internos, Cecilia Malmström, a Alta Representante, Catherine Ashton e a Comissária para a Agenda Digital, Neelie Kroes. Segundo essa autora, essas disposições sinalizam uma transição para uma postura mais assertiva e regulativa da UE, em matéria de Segurança Cibernética, com a criação desse instrumento juridicamente vinculativo.

Geraldes (2019, p. 102-103) registra ainda que a ECS assenta em três pilares principais e evidencia a preocupação da União em abordar essa matéria de forma holística: (1) proteção das infraestruturas de informação crítica; (2) cibercrime; e (3) ciberdefesa. E envolve diversas áreas com mandatos distintos: mercado interno, justiça e assuntos internos, e política externa.

A Estratégia europeia (EUROPEAN COMMISSION, 2013, p. 3) define princípios para Segurança Cibernética e pontua que a *internet* sem fronteiras e multicamadas se tornou um dos instrumentos mais poderosos para o progresso global sem supervisão ou regulamentação governamental. Enquanto o setor privado deve continuar a desempenhar um papel de

liderança na construção e gestão do dia a dia da internet, a necessidade de requisitos de transparência, responsabilidade e segurança se torna cada vez mais proeminente.

Em seguida, a Estratégia esclarece e define os princípios que devem guiar a política de Segurança Cibernética na UE e em nível internacional.

- Os valores fundamentais da UE aplicam-se ao mundo digital e ao mundo físico. As mesmas leis e normas que se aplicam a outras áreas do nosso dia a dia aplicam-se também ao domínio cibernético.

- Proteção dos direitos fundamentais, liberdade de expressão, dados pessoais e privacidade.

A Segurança Cibernética só pode ser sólida e eficaz se for baseada nos direitos fundamentais e liberdades consagradas na Carta dos Direitos Fundamentais da União Europeia e nos valores essenciais da UE. Reciprocamente, os direitos dos indivíduos não podem ser garantidos sem redes seguras e sistemas. Qualquer compartilhamento de informações para fins de segurança cibernética, quando os dados pessoais estão em interesse, deve estar em conformidade com a legislação de proteção de dados da UE e ter plenamente em conta os direitos dos indivíduos nesse domínio.

- Acesso para todos.

Acesso limitado ou nenhum acesso à internet e analfabetismo digital constituem uma desvantagem para os cidadãos, dado o quanto o mundo digital permeia a atividade dentro da sociedade. Todos deveriam ser capazes de ter acesso à internet e a um fluxo desimpedido de informações. A integridade da internet e a segurança devem ser garantidas para permitirem o acesso seguro para todos.

- Governança multissetorial democrática e eficiente.

O mundo digital não é controlado por uma única entidade. Existem atualmente várias partes interessadas, entre as quais, muitas são entidades comerciais e não governamentais, envolvidas no dia a dia da gestão de recursos, protocolos e padrões da internet e no futuro desenvolvimento desta. A UE reafirma a importância de todas as partes interessadas no atual modelo de governança da internet e, desta forma, mantém essa abordagem de governança de múltiplas partes interessadas.

- Uma responsabilidade compartilhada para garantir a segurança.

A crescente dependência das TIC em todos os domínios da vida humana acarretou vulnerabilidades que precisam ser devidamente definidas, analisadas exaustivamente,

remediadas ou reduzidas. Todos os atores relevantes, sejam autoridades públicas, setor privado ou cidadãos individuais precisam reconhecer essa responsabilidade compartilhada, tomar medidas para proteger e, se necessário, garantir uma resposta coordenada para fortalecer a segurança cibernética.

- Prioridades e ações estratégicas.

A UE deve salvaguardar um ambiente *on-line* que proporcione a maior liberdade possível e segurança para o benefício de todos. Embora reconheça que é predominantemente a tarefa de estados-membros lidar com os desafios de segurança no ciberespaço, essa estratégia propõe ações que podem melhorar o desempenho geral da UE. Essas ações são de curto e longo prazos, incluindo uma variedade de ferramentas de política e envolvendo diferentes tipos de atores, sejam instituições da UE, estados-membros ou indústria.

A Estratégia da União Europeia define ainda que a visão do bloco europeu, apresentada na estratégia, está articulada em cinco prioridades estratégicas, que visam enfrentar os desafios já destacados, a saber: (1) alcançar a resiliência cibernética; (2) reduzir drasticamente o cibercrime; (3) desenvolver políticas e capacidades de ciberdefesa relacionadas à *Common Security and Defence Policy* (CSDP); (4) desenvolver os recursos industriais e tecnológicos para a Segurança Cibernética; e (5) estabelecer para a União Europeia uma política internacional coerente sobre o ciberespaço e, simultaneamente, promover os valores essenciais da UE.

Concluindo, a Estratégia europeia afirma:

> Esta proposta de estratégia de cibersegurança da União Europeia, apresentada pela Comissão e o Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança, descreve a visão da UE e as ações necessárias, com base na forte proteção e promoção dos direitos dos cidadãos, para tornar o ambiente *online* da UE o mais seguro do mundo. (EUROPEAN COMMISSION, 2013, p. 19).

Barbas e Sancho (2018) lembram ainda que a estratégia enuncia também um extenso conjunto de iniciativas da Comissão e da Alta Representante, em cooperação com os Estados-membros nos âmbito da: (1) proteção dos direitos fundamentais; (2) apoio ao desenvolvimento de capacidades no acesso à informação, prevenção e combate de acontecimentos acidentais, cibercriminalidade e terrorismo cibernético; (3) capacitação em Segurança Cibernética; (4) proteção de infraestruturas de informação críticas; e (5) cooperação entre as autoridades competentes em matéria de Segurança das Redes e da Informação.

4.2.2 Políticas e Estratégias nacionais de Segurança Cibernética

4.2.2.1 O caso de Portugal

A Estratégia Nacional de Segurança do Ciberespaço (ENSC) 2019 -2023 baseia-se:

> [...]no compromisso de aprofundar a segurança das redes e sistemas de informação, como forma de garantir a proteção e defesa do ciberespaço de interesse nacional e potenciar uma utilização livre, segura e eficiente do mesmo por parte de todos os cidadãos, das empresas e das demais entidades públicas e privadas. (DRE, 2019, p. 288).

A Estratégia portuguesa tem como base a Estratégia da União Europeia para a Cibersegurança, a observância dos princípios da soberania do Estado, bem como a estrita observância da Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa, da Carta dos Direitos Fundamentais da União Europeia, bem como dos demais documentos europeus e portugueses que tratam da proteção dos direitos fundamentais, da liberdade de expressão, dos dados pessoais e da privacidade.

A ENSC 2019-2023 alicerça estes princípios.

1 — Valores, definições e princípios

- Princípio da subsidiariedade: Portugal afirma o seu forte compromisso com a segurança do ciberespaço. Considerando que grande parte das infraestruturas tecnológicas que compõem o ciberespaço é detida por entidades do setor privado, cabe a estas a responsabilidade primária pela sua proteção, uma responsabilidade que inicia no próprio indivíduo, pela forma responsável como utiliza o ciberespaço, e termina no Estado, enquanto garante a soberania e os princípios constitucionais.

- Princípio da complementaridade: A segurança do ciberespaço é uma responsabilidade partilhada entre os diferentes atores, sejam eles públicos ou privados, coletivos ou individuais. Uma abordagem inclusiva, alargada e integradora da segurança do ciberespaço exige diferentes responsabilidades e capacidades, para benefício do interesse comum.

- Princípio da proporcionalidade: A segurança do ciberespaço resulta também de um exercício complexo, verificável e contínuo, de avaliação dos riscos associados ao ecossistema digital. Em consequência, a adequação e a alocação de recursos devem ser proporcionais aos riscos identificados e à execução das linhas de ação constantes da presente Estratégia.

2 — Análise da envolvente

Quando a primeira Estratégia Nacional de Segurança do Ciberespaço foi aprovada, em 2015, a emergência tecnológica e o seu impacto na nossa sociedade já eram evidentes. A tendência para um crescente aumento da dependência das tecnologias de informação e de comunicação e o surgimento de novos fenômenos com impacto direto no desenvolvimento social trouxeram, de igual modo, em sociedades conectadas como a nossa, oportunidades significativas para aqueles que pretendem comprometer as nossas redes e sistemas de informação com intuitos potencialmente perniciosos para o bem-estar da sociedade portuguesa.

3 — Visão

A presente Estratégia estabelece a seguinte visão para 2023: que Portugal seja um país seguro e próspero em ação inovadora, inclusiva e resiliente que preserve os valores fundamentais do Estado de Direito democrático e garanta o regular funcionamento das instituições face à evolução digital da sociedade.

4 — Objetivos estratégicos

1 - Maximizar a resiliência:

2 - Promover a inovação:

3 - Gerar e garantir recursos:

5 - Eixos

As implicações e necessidades associadas a cada um dos objetivos estratégicos permitem definir uma orientação geral e específica que, traduzida em seis eixos de intervenção, enformam linhas de ação concretas destinadas a reforçar o potencial estratégico nacional no ciberespaço por meio do incremento da sua segurança, a saber: eixo 1 — estrutura de segurança do ciberespaço; eixo 2 — prevenção, educação e sensibilização; eixo 3 — proteção do ciberespaço e das infraestruturas; eixo 4 — resposta às ameaças e combate ao cibercrime; eixo 5 — investigação, desenvolvimento e inovação; e eixo 6 — cooperação nacional e internacional.

6 - Avaliação e revisão da Estratégia

A presente Estratégia será objeto de avaliação anual pelo Conselho Superior de Segurança do Ciberespaço. Tal avaliação incluirá uma verificação dos objetivos estratégicos e do plano de ação e adequação dos mesmos à evolução das circunstâncias. Por outro lado, a rápida evolução intrínseca em relação ao ciberespaço exige que essa Estratégia seja objeto de revisão regular e periódica, considerando-se que, sem prejuízo de processos de revisão

extraordinários sempre que as circunstâncias o exijam, a revisão regular e periódica deve ocorrer num prazo máximo de cinco anos.

4.2.2.2 O caso do Chile

A Política Nacional de Cibersegurança (PNCS), principal documento sobre o tema no Chile, estabelece “as diretrizes políticas do Estado do Chile em matéria de cibersegurança, com vistas ao ano 2023, para atingir o objetivo de ter um ciberespaço livre e aberto, seguro e resiliente”. Essa política se baseia na necessidade de proteger a segurança das pessoas no ciberespaço; proteger a segurança do país; e gerenciar os riscos do ciberespaço. A PNCS chilena tem dois eixos principais: “uma política de Estado, desenhada com objetivos orientados para o ano 2022, e uma agenda de medidas específicas, que serão implementadas entre 2017 e 2018” (BARBAS; SANCHO, 2018).

A PNCS é complementada por outras políticas públicas em desenvolvimento, que correspondem aos documentos das referências (GOBIERNO DE CHILE, 2015; 2017):

(1) Agenda Digital 2020: A Agenda Digital 2020 orienta os progressos no desenvolvimento digital do país por meio da definição de objetivos de médio prazo, linhas de ação e medidas concretas;

(2) Diversas medidas da Agenda que, da mesma forma, fortalecem e complementam a PNCS, entre as quais o impulso dado a uma nova Lei de Proteção de dados pessoais, a proteção dos direitos do consumidor na internet, o desenvolvimento de um Plano Nacional de Infraestrutura de Telecomunicações, aprimoramento da regulamentação sobre assinatura eletrônica.

(3) Política Nacional de Defesa Cibernética: os sistemas e redes de informação da Defesa Nacional constituem uma infraestrutura crítica para a segurança externa e o exercício da soberania do país, juntamente com os poderes constitucionais e legais da Defesa Nacional, constituem o pano de fundo que justifica o desenvolvimento pelo Ministério da Defesa Nacional, ao longo de 2017, de políticas específicas de defesa cibernética, que contemplem as definições políticas relativas à proteção de redes, e a forma como as capacidades de Defesa Nacional colaborariam na formação de um ciberespaço livre, aberto, seguro e resiliente para o país.

(4) Política Internacional para o Ciberespaço: um dos objetivos de alto nível do PNCS está relacionado à cooperação internacional e às relações em torno da segurança cibernética

em um ambiente de globalização, no entanto é essencial que esses objetivos estejam vinculados a outros, como o desenvolvimento, os direitos humanos, a defesa etc., a fim de consolidá-los e integrá-los à política externa chilena (GOBIERNO DE CHILE, 2017).

No documento em análise, está posto o compromisso chileno com os objetivos e medidas que permitirão ter um ciberespaço livre, aberto, seguro e resiliente para responder à necessidade de proteger a segurança das pessoas no ciberespaço, proteger a segurança do país e gerenciar os riscos do ciberespaço. A cooperação internacional também é considerada um aspecto-chave na segurança cibernética do Chile, promovendo a participação com diferentes órgãos multilaterais que tratam do tema, tais como Organização das Nações Unidas (ONU) e Organização dos Estados Americanos (OEA).

5 Metodologia utilizada

Em relação à metodologia, foi utilizado o levantamento legislativo-documental e histórico, sendo analisadas normas produzidas pelos poderes Legislativo e Executivo nacional, cuja abrangência esteja relacionada ao tema principal do presente trabalho. Foram realizadas ainda pesquisa bibliográfica e análise dos documentos, de legislações internacionais, publicações especializadas e outros, bem como de dados e informações publicados que tratam, direta ou indiretamente, o tema em análise e os dispositivos legais pertinentes, tendo como base um estudo descritivo e analítico das fontes.

Adotamos ainda a metodologia comparada, pois, por meio dela, é possível identificar semelhanças e diferenças entre as Estratégias de Segurança Cibernética analisadas, ampliando-se o campo de análise do documento brasileiro análogo.

6 Considerações finais

A análise realizada permite obter um comparativo entre os documentos mencionados, todos de suma importância em seus países e bloco. Entendemos ser válida a perspectiva adotada, pois trata de diferentes realidades e diferentes necessidades de países, além de tratar de aspectos relacionados à maturidade do tema nessas diferentes realidades. Assim, o conhecimento da análise dessas diferentes abordagens trará elementos para formação e capacitação de pessoas, para apoio à elaboração de planos de implantação de segurança cibernética em organizações brasileiras, entre outros, isto para citar algumas oportunidades, entre as muitas que se apresentam.

A pesquisa conduzida possibilitou uma análise com profundidade no atendimento ao objetivo proposto, sendo analisada a legislação brasileira existente sobre o setor cibernético e áreas relacionadas, que possibilitou o caminho do Brasil até a atual E-Ciber.

Em relação ao caso brasileiro, a Estratégia Nacional de Segurança Cibernética vem ao encontro de uma demanda interna por um posicionamento do Governo Federal sobre a Segurança Cibernética, pois os recursos de tecnologia estão cada dia mais presentes na realidade do país e no funcionamento do Estado, quer seja na vida privada dos cidadãos, quer seja na atividade econômica do país. Por outro lado, a demanda externa aponta para a necessidade de alinhamento a regulações externas, como, por exemplo, a Convenção de Budapeste, à qual o Brasil aderiu recentemente.

No caso da União Europeia, observa-se que vem demonstrando uma crescente preocupação com a segurança cibernética da própria organização, bem como de seus estados-membros. Assim, a UE tem atuado em conjunto com a OTAN, no sentido de evitar que as próprias organizações e seus estados-membros se coloquem em situação de vulnerabilidade face a ataques provenientes do ciberespaço, desenvolvendo intensa atividade legislativa e de ações práticas.

No caso de Portugal, foi possível observar que o país, há anos, vem avançando na política de Segurança Cibernética. Desde a criação da Lei nº 109/1991, de 17 de agosto (Lei da criminalidade informática, atualmente revogada), vem sendo empreendido um esforço no sentido de envolver governo, administração pública, Forças Armadas, empresas e cidadãos na promoção de medidas de proteção e segurança do ciberespaço.

A ENSC 2019-2023 foi resultado dos trabalhos desenvolvidos pelo grupo de projeto criado pelo Governo português em agosto de 2017, denominado “Conselho Superior de Segurança do Ciberespaço”, cuja missão era propor a revisão da ENSC, tendo em vista a evolução digital ocorrida desde a aprovação da primeira Estratégia, em 2015.

No caso do Chile, visualiza-se que o país dispõe de dispositivos legais em que é possível estabelecer a concatenação de três políticas distintas, articuladas entre si e com objetivos que, de distintos âmbitos de competência e ação, reforçam, complementam e valorizam o quadro de uma vontade única do Estado, no sentido de alcançar níveis de Segurança Cibernética em acordo com as normas internacionais que permitem o respeito pelos direitos das pessoas e o desenvolvimento do país, dos seus cidadãos, organizações e empresas.

Em resumo, o Chile possui uma política de Segurança Cibernética formulada, cujos principais desafios são: cumprir os objetivos propostos, além de dar continuidade, em médio e longo prazos, ao esforço que vem sendo realizado, considerada uma abordagem suprapartidária sobre o tema.

Ao comparar os dois países, Chile e Portugal, é possível perceber que o nível de compromissos internacionais firmados em cada um deles condicionará o nível de autonomia para o desenvolvimento das políticas de segurança cibernética. No caso de Portugal, as orientações emanadas da UE fornecem orientações a serem obrigatoriamente consideradas em nível nacional. No caso chileno, muito embora as recomendações da OEA orientem a formulação das políticas de segurança cibernética, não é obrigatório incluí-las nos documentos nacionais, pois servem somente de guias.

Referências

APARÍCIO, Marcelo da Silva. *O Ciberespaço como Dimensão de Segurança*. Dissertação para obtenção do Grau de Mestre em Aeronáutica Militar, na Especialidade de Piloto-Aviador. Academia da Força Aérea Portuguesa. Sintra, Portugal, maio 2017. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/23108/1/O%20ciberespa%C3%A7o%20como%20dimens%C3%A3o%20de%20seguran%C3%A7a_disserta%C3%A7%C3%A3o.pdf. Acesso em: 2 out. 2020.

BARBAS, João; SANCHO, Carolina. Cibersegurança e políticas públicas: análise comparada dos casos chileno e português. *IDN Cadernos*, n. 29, 2018. Disponível em: https://www.idn.gov.pt/publicacoes/cadernos/idncadernos_29.pdf. Acesso em: 2 out. 2020.

BARROS, Otávio Santana Rêgo; GOMES, Ulisses de Mesquita; FREITAS, Whitney Lacerda de (org). *Desafios estratégicos para segurança e defesa cibernética*. Brasília, DF: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. Disponível em: https://livroaberto.ibict.br/bitstream/1/612/2/Desafios%20estrat%c3%a9gicos%20para%20seguran%c3%a7a%20e%20defesa%20cibern%c3%a9tica.pdf. Acesso em: 2 out. 2020.

BRASIL. *Decreto n. 10.222, de 5 de fevereiro de 2020*. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, DF, 2020a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm. Acesso em: 2 out. 2020.

BRASIL. Ministério da Defesa. *Política Nacional de Defesa (PND) e Estratégia Nacional de Defesa (END) encaminhadas, em 22 de julho de 2020, para apreciação do Congresso*

Nacional. Brasília, DF, 2020b. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/politica-nacional-de-defesa. Acesso em: 11 out. 2020.

BRASIL. *Lei nº 13.844, de 18 de junho de 2019*. Estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios. Brasília, DF, 2019a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13844.htm. Acesso em: 11 out. 2020.

BRASIL. Presidência da República. *Decreto n. 9.819, de 3 de junho de 2019*. Dispõe sobre a Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo. Brasília, DF, 2019b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9819.htm. Acesso em: 10 out. 2020.

BRASIL. Presidência da República*. Decreto n. 9.668, de 2 de janeiro de 2019*. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República e altera o quantitativo de Gratificações de Exercício de Cargo em Confiança devida a Militares - RMP. Brasília, DF, 2019c. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9668.htm#art7. Acesso em: 10 out. 2020.

BRASIL. *Decreto n. 9.637, de 26 de dezembro de 2018*. Institui a Política Nacional de Segurança da Informação. Brasília, DF, 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm#art6i. Acesso em: 2 out. 2020.

BRASIL. *Decreto n. 9.570, de 20 de novembro de 2018*. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Defesa. Brasília, DF, 2018b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9570.htm. Acesso em: 2 out. 2020.

BRASIL. Ministério da Defesa. Exército Brasileiro. *Portaria n. 42/COTER, de 8 de junho de 2017*. Aprova o Manual de Campanha EB70-MC-10.232 Guerra Cibernética. Brasília, DF, 2017a. Disponível em: http://www.bdex.eb.mil.br/jspui/bitstream/1/631/3/EB70MC10232.pdf. Acesso em: 2 out. 2020.

BRASIL. Conselho De Defesa Nacional. Portaria n. 14, de 11 de maio de 2015. Homologa a "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal - 2015/2018, versão 1.0", desdobramento da Instrução Normativa GSI/PR nº 01/2008. *DOU*, Seção 1, n. 88, terça-feira, 12 maio 2015a.

BRASIL. Ministério da Defesa. *Portaria Normativa n. 2.327/MD, de 28 de outubro de 2015*. Dispõe sobre a Política de Segurança da Informação para o Sistema Militar de Comando e Controle - MD31-P-03 (2. Edição/2015). Brasília, DF, 2015b. Disponível em: https://www.in.gov.br/materia/-

/asset_publisher/Kujrw0TZC2Mb/content/id/33296815/do1-2015-10-29-portaria-normativa-n-2-327-md-de-28-de-outubro-de-2015-33296731. Acesso em: 10 out. 2020.

BRASIL. Ministério da Defesa. *Portaria Normativa MD n. 2.777, de 27 de outubro de 2014*. Dispõe sobre a diretriz de implantação de medidas visando à potencialização da Defesa Cibernética Nacional e dá outras providências. Brasília, DF, 2014a. Disponível em: http://www.lex.com.br/legis_26110622_PORTARIA_NORMATIVA_N_2777_DE_27_DE_OUTUBRO_DE_2014.aspx. Acesso em: 10 out. 2020.

BRASIL. Ministério da Defesa. *Portaria Normativa n. 3.010/MD, de 18 de novembro de 2014*. Aprova a Doutrina Militar de Defesa Cibernética - MD31-M-07. Brasília, DF, 2014b. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf. Acesso em: 2 out. 2020.

BRASIL. Presidência da República. Secretaria de Assuntos Estratégicos. *Relatório do XIII Encontro Nacional de Estudos Estratégicos*: o setor cibernético brasileiro. Brasília, DF, 2013. Disponível em: http://www.biblioteca.presidencia.gov.br/presidencia/dilma-vana-rousseff/publicacoes/orgao-essenciais/secretaria-de-assuntos-estrategicos/relatorio-do-xiii-encontro-nacional-de-assuntos-estrategicos. Acesso em: 10 out. 2020.

BRASIL. Presidência da República. *Livro branco de defesa nacional*. Brasília, DF, 2012. Brasília, DF, 2012a. Disponível em: https://www.camara.leg.br/internet/agencia/pdf/LIVRO_BRANCO.pdf. Acesso em: 2 out. 2020.

BRASIL. Ministério da Defesa. *Portaria Normativa n. 3.389/MD, de 21 de dezembro de 2012*. Política Cibernética de Defesa - MD31-P-02. Brasília, DF, 2012b. Disponível em: https://www.camara.leg.br/internet/agencia/pdf/LIVRO_BRANCO.pdf. Acesso em: 2 out. 2020.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. *Livro verde*: segurança cibernética no Brasil. Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; org. Claudia Canongia e Raphael Mandarino Junior. Brasília: GSIPR/SE/DSIC, 2010. Disponível em: http://dsic.planalto.gov.br/legislacao/1_Livro_Verde_SEG_CIBER.pdf. Acesso em: 2 out. 2020.

BRASIL. Ministério da Defesa. Diretriz Ministerial nº 14/2009, de 9 de novembro de 2009: dispõe sobre integração e coordenação dos setores estratégicos da Defesa. Brasília, DF, 2009. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/File/legislacao/emcfa/portarias/0014a_2009.pdf. Acesso em: 2 out. 2019.

BRASIL. Lei n. 10.683, de 29 de maio de 2003. Dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências. Brasília, DF, 2003. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2003/L10.683impressao.htm. Acesso em: 2 out. 2020.

BRASIL. *Decreto n. 3505 de 13 de junho de 2000*. Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília, DF, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm. Acesso em: 2 out. 2020.

BRASIL. *Lei Complementar n. 97, de 9 de junho de 1999*. Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas. Brasília, DF, 1999. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp97.htm. Acesso em: 2 out. 2020.

CÂMARA DOS DEPUTADOS. Decreto Legislativo n. 179, de 2018. Aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional, encaminhados ao Congresso Nacional pela Mensagem (CN) nº 2 de 2017 (Mensagem nº 616, de 18 de novembro de 2016, na origem). Brasília, DF, 2018. Disponível em: https://www2.camara.leg.br/legin/fed/decleg/2018/decretolegislativo-179-14-dezembro-2018-787452-exposicaodemotivos-157024-pl.html). Acesso em: 2 out. 2020.

CARNEIRO, João Marinonio Enke. *A guerra cibernética*: uma proposta de elementos para formulação doutrinária no Exército Brasileiro. Tese (Doutorado) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2012, 203 f.

COSTA, Alan Denilson Lima. O setor cibernético no Exército Brasileiro. *Revista do Exército Brasileiro*, v. 149, p. 62-78, 1. semest. 2013. Disponível em: https://pt.calameo.com/exercito-brasileiro/read/001238206530442dcc28b. Acesso em: 10 out. 2020.

DIÁRIO DA REPÚBLICA ELECTRÓNICO (DRE). *Resolução do Conselho de Ministros n. 92/2019*. Diário da República n.º 108/2019, Série I de 2019-06-05. Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023. Lisboa, 2019. Disponível em: https://dre.pt/home/-/dre/122498962/details/maximized. Acesso em: 2 out. 2020.

EB. Instituto Militar de Engenharia (IME). Laboratório de Pesquisa Cibernética. Disponível em: http://defesacibernetica.ime.eb.br/. Acesso em: 10 out. 2020.

EUROPEAN COMMISSION. *Cybersecurity Strategy of the European Union*: an open, safe and secure cyberspace. Brussels, 7.2.2013 JOIN (2013) 1 final. Disponível em: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdfhttps://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf. Acesso em: 10 out. 2020.

LAVADO, THIAGO. Uso da internet no Brasil cresce, e 70% da população está conectada. *G1*, 28 AGO. 2019. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/08/28/uso-da-internet-no-brasil-cresce-e-70percent-da-populacao-esta-conectada.ghtml. Acesso em: 2 out. 2020.

MIGALHAS. Segurança na Internet. Decreto aprova Estratégia Nacional de Segurança Cibernética. 6 fev. 2020. Disponível em: https://migalhas.uol.com.br/quentes/319928/decreto-aprova-estrategia-nacional-de-seguranca-cibernetica. Acesso em: 10 out. 2020.

GERALDES, Sofia Martins. A Estratégia de Cibersegurança da União Europeia: catastrofista, realista e/ou otimista? *Nação e Defesa*, n. 154, p. 91-108, dez. 2019. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/33162/1/GERALDESSofiaMartins_Aestrat%C3%A9giadeciberseguran%C3%A7adaUni%C3%A3oEuropeia_Na%C3%A7%C3%A3oDefesa_N_154_p_91_108.pdf. Acesso em: 10 out. 2020.

LUCA, Cristina de. Após estratégia, GSI elabora a Política Nacional de Segurança Cibernética. *UOL*, 9 fev. 2020. Disponível em: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdfhttps://porta23.blogosfera.uol.com.br/2020/02/09/apos-estrategia-gsi-elabora-a-politica-nacional-de-seguranca-cibernetica/. Acesso em: 10 out. 2020.

GOBIERNO DE CHILE. *Política Nacional de Ciberseguridad*. Santiago, 2017. Disponível em: https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf. Acesso em: 10 out. 2020.

GOBIERNO DE CHILE. Ministerio del Interior y Seguridad Pública; Ministério de Defensa Nacional. *Bases para una política nacional de ciberseguridad*. Santiago: Marzo de 2015. Disponível em: https://www.ciberseguridad.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADtica-Nacional-sobre-Ciberseguridad.pdf. Acesso em: 10 out. 2020.

TAKAHASHI, Tadao (org.). *Sociedade da informação no Brasil*: livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000. Disponível em: https://livroaberto.ibict.br/handle/1/434. Acesso em: 10 out. 2020.

Os desafios do *compliance* para adequação à LGPD

Aline Marchesini Pinto

Érica Maia Campelo Arruda

Resumo: O presente trabalho tem por objetivo analisar os aspectos que envolvem o compliance, necessários para adequação das organizações à Lei Geral de Proteção de Dados (LGPD). Busca ainda apresentar subsídios para que seja possível, aos profissionais do Direito, apoiar as organizações na elaboração de um Plano de Integridade. Para alcançar o objetivo pretendido, serão abordados os aspectos que tratam das práticas de *compliance*, entre estas as relativas à governança corporativa e conceitos relativos ao Big Data e Business Intelligence, ambos ligados diretamente à Lei referenciada. Assim, serão analisadas as nuances da Lei, no sentido de contribuir para trazer elementos na condução da mudança de cultura nas organizações, buscando levantar subsídios para a conscientização quanto às determinações da lei e o ônus que seu descumprimento pode trazer à organização. Será também analisada a Lei n. 12.846/2013, também intitulada Lei Anticorrupção ou Lei da Empresa Limpa. Trata-se também da necessidade da preparação dos profissionais do Direito para que os mesmos sejam capazes de apoiar as organizações a obter o *compliance* com a nova Lei. O presente trabalho seguiu os princípios de um estudo exploratório, por meio de uma pesquisa bibliográfica e o estudo de casos reais, tanto no País quanto no exterior. No sentido de atender a LGPD e demais dispositivos legais, abordamos os aspectos relacionados à necessidade de que especialistas em Direito Digital e LGPD estudem o negócio das organizações em que atuam, para que as organizações consigam, o quanto antes, realizar ações imprescindíveis para garantir o *compliance* com a nova Lei.
Palavras-chave: *Compliance*. Direito Digital. LGPD.

1 Introdução

Com o advento da Constituição Federal de 1988 (CF88) (BRASIL, 1988), o direito administrativo brasileiro passou por uma importante mudança. A partir desse marco legal, surgiram os trabalhos de diversos doutrinadores, que trazem essa nova perspectiva do direito administrativo.

Assim, como afirma Marchesini Pinto (2020, p. 22), é possível visualizar

> a notória alteração do modelo de Estado-Nação na transição da modernidade para a pós-modernidade, sendo possível colacionar elementos que contribuíram nesse sentido, como a mutação na acepção do individualismo moderno, cuja autonomia passa a ser valorizada, porém, com o condão de conferir fundamento a toda autoridade constituída, o impacto das incertezas e a perda da organização social tradicional, o que repercutiu nas funções estatais e na ampliação do seu horizonte.

Dessa forma, a proteção de direitos, que sugeria supremacia do ente soberano sobre a sociedade, dá espaço à garantia desses mesmos direitos, pois já se encontram estabelecidos como fundamentais aos indivíduos e à sociedade como um todo. Por seu turno, a prestação

de serviços, que foi em certo momento a essência da função estatal, na forma de entrega de bens e serviços pela administração pública, cede lugar à regulação, passando a valorizar a comunicação perene entre usuários e prestadores de serviço (concessionárias e permissionárias), o próprio Estado, e ainda entre os diversos órgãos públicos, em verdadeiro diálogo interinstitucional (MARCHESINI PINTO, 2020, p. 22).

No entanto, a perspectiva pós-moderna é indissociável da obtenção de resultados econômicos, muito por conta, inclusive, da necessidade de alcançar melhoria nos resultados sociais. Tal aspecto se encontra em consonância com o art. 3° da Constituição brasileira, em especial no que se refere à garantia do desenvolvimento nacional, que, por sua vez remete ao comprometimento político e jurídico em termos de políticas públicas e possui aplicabilidade direta, tendo em vista o §1° do art. 5° da Carta Magna de 1988.

Nesse diapasão, a concepção pós-moderna das relações da administração pública com os cidadãos, partindo da base contida no texto constitucional, faz com que a boa e justa atribuição de bens às pessoas seja colocada como um "*proprium* da função administrativa", na terminologia de Sorrentino (2003, *apud* MOREIRA NETO, 2018, p. 178).

Surge então o conceito de governança pública, cuja origem vem do direito privado, com base no conceito de governança corporativa. De acordo com o Referencial Básico de Governança do Tribunal de Contas da União (TCU) (BRASIL, 2014, p. 15), a origem da governança está associada ao momento em que organizações deixaram de ser geridas diretamente por seus proprietários (por exemplo, donos do capital) e passaram à administração de terceiros.

Assim, pela análise de questões que passam pela governança pública, *compliance* e boas práticas de governança e gestão, o presente trabalho tem por objetivo analisar os aspectos que envolvem o *compliance*, necessários para adequação das organizações à Lei Geral de Proteção de Dados (LGPD), com ênfase no setor público. Busca ainda apresentar subsídios para que seja possível aos profissionais do Direito, apoiar as organizações na elaboração de um Plano de integridade.

Como explanam Sztajn e Silva (2020), o termo *compliance* provém do inglês *to comply*, que significa agir de acordo com uma regra, uma instrução interna, um comando ou um pedido. No âmbito institucional e corporativo, *compliance* corresponde a um conjunto de ações que visam ao cumprimento das normas legais e regulamentares, das políticas e diretrizes do negócio e das atividades da organização, com o objetivo de evitar, detectar e

solucionar quaisquer desvios ou inconformidades que venham a acontecer. Assim, em relação à LGPD, que é o marco legal de proteção e transferência de dados no Brasil, o *compliance* pode ser associado, com o objetivo de proteger os cidadãos contra o mau uso de seus dados ou informações relacionadas a pessoas naturais ou jurídicas (SZTAJN; SILVA, 2020).

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Governança pública e *compliance*

De acordo com o "Referencial básico de governança aplicável a órgãos e entidades da administração pública", publicado pelo TCU (BRASIL, 2014), governança pública pode ser entendida como o sistema que determina o equilíbrio de poder entre os envolvidos — cidadãos, representantes eleitos (governantes), alta administração, gestores e colaboradores — com vistas a permitir que o bem comum prevaleça sobre os interesses de pessoas ou grupos. O documento analisa a governança no setor público sob quatro perspectivas de observação: (a) sociedade e Estado; (b) entes federativos, esferas de poder e políticas públicas; (c) órgãos e entidades; e (d) atividades intraorganizacionais.

Em relação à Constituição Federal de 1988, quanto ao tema "fiscalização", visualiza-se que existe uma seção inteira dedicada ao tema fiscalização contábil, financeira e orçamentária, disciplinando a atuação dos tribunais de contas, nos artigos 70 a 75. O *caput* do art. 71, da CF88, destaca que o Tribunal de Contas da União tem a função de auxiliar o Congresso Nacional no exercício do controle externo da administração pública, o que consiste na fiscalização contábil, financeira, orçamentária, operacional e patrimonial da União e das entidades da administração direta e indireta, no que tange à legalidade, legitimidade, economicidade, aplicação das subvenções e renúncia de receitas, de acordo com o disposto no caput do art. 70, da CF88 (MARCHESINI PINTO, 2020, p. 47).

A *compliance*, associada à conformidade com a ética e, mais do que isso, o respeito às leis do país em que, sediadas as empresas, embora já deflua do complexo arcabouço constitucional e legal no domínio público, é reforçada por "linhas mestras" (VALLE; SANTOS, 2019) amparada em valores como a legitimidade das escolhas e a moralidade.

2.2 Administração Pública Federal e o Decreto n° 9.203/2017

Limitando-se aqui o escopo à governança pública, anota-se que Federação Internacional de Contadores (IFAC - *International Federation of Accountants*) no estudo n° 13, de 2001 (IFAC, 2001), indicou três princípios de governança para o setor público, a saber:

i) *openness* (transparência): objetivando assegurar aos interessados confiança no processo de tomada de decisão engendrado pelas organizações do setor público;

ii) *integrity* (integridade): compreendendo a utilização de procedimentos honestos na administração dos recursos públicos de modo geral;

iii) *accountability*: (responsabilidade de prestar contas): no sentido de que os agentes públicos são responsáveis por suas decisões e ações, sendo submetidos aos controles devidos.

O Decreto n° 9.203/2017 (BRASIL, 2017a), que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. foi construído com base na iniciativa de órgãos centrais do governo federal, em articulação com o TCU, que trouxeram a proposta de criação da política de governança na administração pública federal. O TCU identificou a necessidade de um marco legal que pudesse consolidar as melhores práticas de governança para os órgãos e entidades da administração pública federal direta e indireta, servindo também de baliza para os demais Poderes da área federal, de forma a potencializar o desempenho desses órgãos, em especial daqueles que viabilizam políticas públicas, e a obtenção de resultados, com base em três pilares principais: liderança, estratégia e controle (BRASIL, 2018a).

O embasamento para a política de governança posta no Decreto n° 9.203/2017 foi obtido junto às organizações internacionais, com destaque para a Organização para Cooperação e Desenvolvimento Econômico (OCDE). Ressalte-se a importância do Decreto n° 9.203/2017, adicionalmente ao Novo Regime Fiscal instituído pela Emenda Constitucional n° 95/2016 (BRASIL, 2016), que impõe um debate mais capacitado e racional quanto à priorização das políticas públicas e escolhas alocativas do orçamento e não somente trata da contenção do avanço dos gastos públicos, mas também no seu melhor direcionamento, estancando-os quando não estejam produzindo os resultados esperados, de modo a privilegiar a eficiência e a eficácia das políticas públicas (MARCHESINI PINTO, 2020, p. 22).

Para o Decreto n° 9.203/2017, de acordo com seu inciso I do art. 2°, governança pública é o conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de

serviços de interesse da sociedade. A política de governança, concebida no mencionado Decreto supramencionado, apresenta dois fundamentos principais (BRASIL, 2017a), a saber:

a) Confiança: É um elemento fundamental porque gera legitimidade. A confiança, para o Banco Mundial (2017), deriva de: i) da entrega de resultados previamente pactuados; ii) compreensão de que as leis e as políticas foram concebidas e estão sendo realizadas com imparcialidade; iii) de que há valores em comum compartilhados pelos cidadãos e governantes que pautam as escolhas públicas. A confiança gera respeito e contribui para a desburocratização pois a sociedade considera legítima a atuação pública. Por decorrência, há um incentivo ao cumprimento espontâneo das regras postas, o que reduz a necessidade dos controles; e
b) Cooperação e coerência: O Decreto n° 9.203/2017 (art. 2°, inciso I) remete a balizas mínimas a serem seguidas pelas entidades e órgãos públicos. Essa asserção autoriza arranjos institucionais flexíveis e que permitem adaptações, admitindo que as diversas organizações públicas possuem diferentes níveis de amadurecimento. Existe, nesse rumo, um reconhecimento do caráter dinâmico dos princípios e diretrizes predefinidos no decreto, de modo que as diversas entidades que integram a administração pública promovam a adequação das suas ações.

Nesse sentido, o Decreto n° 9.203/2017 trouxe uma lista sucinta de princípios, quais sejam: capacidade de resposta; integridade; confiabilidade; melhoria regulatória; prestação de contas e responsabilidade; e transparência (BRASIL, 2018a, p. 37).

Destacamos um importante mecanismo previsto no Decreto n° 9.203/2017 que visa garantir a coordenação entre os órgãos voltados para as políticas públicas. Esse mecanismo é o Comitê Interministerial de Governança (CIG), que, previsto nos arts. 7°-A e 8°-A, que facilita a solução de problemas transversais e que requerem a atuação concomitante de diversos atores públicos – por exemplo, há acontecimentos que envolvem a temática ambiental, do planejamento e da infraestrutura e, por decorrência, demandam a atuação simultânea dos ministérios respectivos, tal como ocorreu com o recente acidente em Sobradinho/MG. Nesses casos, convém que a atuação ocorra na forma de *whole-of-government approach* (BRASIL, 2018b, p. 23).

Ao tratar o tema racionalização e modernização da atividade administrativa, Valle (2019b) explica o que é abarcado, desde uma rede de boas práticas de governança na administração pública até a abertura à inovação.

Tendo em vista a situação que se faz presente, de dependência tecnológica dos meios digitais, é indispensável abordar, mesmo que de forma breve, as novas tecnologias digitais e seus impactos na gestão. Como explana França (2019, p. 409-411), as dimensões virtuais dependem do homem para existirem e repercutem na realidade concreta, o que implica uma interação cíclica e contínua com a realidade jurídica. Assim, faz-se necessário um "juízo de conformação legal" para os efeitos jurídicos decorrentes do meio ambiente virtual.

Vejamos a perspectiva de Valle (2019b):

> É da lógica do desenvolvimento da legislação contar com o tempo como elemento de maturação. Não decidir, no Legislativo, é classicamente vista como uma estratégia legítima. Mas em tempos de grande aceleração tecnológica, cada vez mais não decidir é dificultar a futura decisão. Isso porque o acervo de informações, de dados de realidade que já se tenha colhido como fundamento para a decisão legislativa tende a rapidamente restar superado. Como pauta de reflexão, essa nova realidade propõe reexaminar os velhos cânones da "reserva da lei" - ainda hoje tão caros à doutrina brasileira e aos Tribunais.
> [...] Aplicar hoje, nos portais do ano 2020, a mesma visão de reserva da lei que se tinha nos anos 90, é condenar o sistema do Direito é um crescente descolamento da realidade concreta sobre a qual ele incide. Disso decorrerá um indesejável é perigosa irrelevância do Direito.

Para França (2019, p. 413), a atividade de *compliance* digital tornou-se, assim, "[...] um importante mecanismo resolutivo voltado à realidade digital sobre a regulação jurídica [...]". Dessa forma, partindo da nova realidade e da diretriz traçada pelo Decreto já mencionado, torna-se impositivo analisar os impactos da atividade regulatória estatal com a ampliação do uso da inteligência artificial e, assim, atuar na melhoria do planejamento voltado para a tecnologia da informação (TI), tanto nos setores públicos quanto nos privados, no sentido de melhor permitir gerenciar corretamente suas repercussões quanto aos direitos fundamentais.

Dessa análise decorre que, tão importante quanto a concepção de leis que regulem a dimensão virtual, tais como a LGPD (Lei 13.709/2018), são os mecanismos para implementação dessas normas, para que, efetivamente, elas possam resultar em condutas consentâneas com o espaço digital e o amparo jurídico constitucional. Nesse sentido, citamos Guerra (2008, p. 138-141):

> É indisputável, sob qualquer ângulo, o distanciamento do circuito legiferante das especificidades tecnológicas e do caso concreto sujeito às oscilações decorrentes do sistema social[...].
> Para que a administração possa funcionar é preciso reduzir as condutas e soluções previamente estabelecidas e cristalizadas na lei, "deixando espaço para uma normatização em nível infra-legal (sic) que permita um melhor ajustamento às peculiaridades de cada caso e a circunstâncias conjunturais". A lei, em sentido estrito, deve conter as decisões políticas fundamentais, traçando rumos e fixando objetivos, mas sem engessar a atividade administrativa; deve, sim, conferir-lhe maior agilidade e

> aptidão na escolha dos meios para atingir os fins legalmente estabelecidos." (GUERRA, 2008, p. 138-141).

Tendo em vista a importância da construção prática de soluções de *compliance* digital em conformidade com os direitos fundamentais, e, ainda, em sintonia com a diretriz que propõe a promoção da simplificação administrativa, modernização da gestão pública e a integração dos serviços públicos, especialmente aqueles prestados por meio eletrônico, França (2019, p. 415) propõe que sejam construídos programas de gestão que contemplem, dentre outros instrumentos possíveis:

> a. elaboração de normas internas claras, objetivas e de fácil compreensão sobre o adequado uso do meio ambiente digital na Organização;
> b. análise de conformidade legal – Constituição Federal (em especial, direitos fundamentais); Lei Geral de Proteção de Dados Pessoais; Lei Anticorrupção; Marco Civil da Internet;
> c. auditoria das organizações *(sic*) – levantamento de soluções tecnológicas; aplicação e atualização de sistemas digitais; identificação de falhas e brechas nos mecanismos de proteção digitais; verificação de ferramentas de aprimoramento de desempenho dos sistemas; qualidade de segurança, de integração e da difusão de dados entre os sistemas;
> d. análise dos licenciamentos digitais contratados/comprados pela Organização e o adequado uso de cada ferramenta licenciada;
> e. aplicação e atualização dos mecanismos de prevenção de ataques cibernéticos;
> f. assessoria técnica para adequação da política de privacidade e termos de uso dos canais de comunicação da empresa com o mundo (*site*, *mails*, redes sociais, etc.) (FRANÇA, 2019, p. 415)

3 A Lei Geral de Proteção de Dados

A LGPD (Lei n° 13.709/2018) dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018c).

Para Lima e Lucca (2020), essa lei inaugura, no Brasil, um sistema de proteção de dados, trazendo princípios basilares para salvaguardar dos titulares dos dados pessoais. Até a promulgação da LGPD, o Brasil dispunha apenas de algumas leis setoriais, como o Código de Defesa do Consumidor (CDC), especialmente seu art. 43, a Lei de Acesso à Informação (LAI, Lei n. 12.527, de 18 de novembro de 2011), a Lei do Cadastro Positivo (Lei n. 12.414, de 09 de junho de 2011) e o Marco Civil da Internet (Lei n. 12.965, de 23 de abril de 2014), entre outras (LIMA; LUCCA, 2020).

Natália Brotto, advogada especialista na LGPD, explica que a lei traz uma mudança de paradigma para dar outros direitos aos donos de dados no Brasil: "Embora a Constituição já

garantisse direitos e o Marco Civil a garantia da proteção de dados, não tinha lei geral que protegesse as pessoas físicas de compartilhamento de dados" (PEDROSO, 2019).

3.1 O dever de transparência na administração pública e a proteção de dados pessoais

Conforme menciona o "Guia de boas práticas para implementação na Administração Pública Federal: LGPD" (BRASIL, 2020),

> a governança no compartilhamento de dados na administração pública federal, autárquica e fundacional segue as diretrizes estabelecidas no Decreto nº 10.046, de 9 de outubro de 2019 (BRASIL, 2019), e precisa ser compreendida à luz das restrições legais, dos requisitos de segurança da informação e comunicações e do disposto pela Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

O documento mencionado relata ainda que, "inicialmente, a adequação dos órgãos e entidades em relação à LGPD envolve uma transformação cultural que deve alcançar os níveis estratégico, tático e operacional da instituição". Tal transformação envolve considerar a privacidade dos dados pessoais do cidadão desde a fase de concepção do serviço ou produto até sua execução (Privacidade *by Design*); além de promover ações de conscientização de todo corpo funcional no sentido de incorporar o respeito à privacidade dos dados pessoais nas atividades institucionais cotidianas (BRASIL, 2020).

Sob um outro prisma, o Poder Público, ao mesmo tempo que precisa dar ampla divulgação de informações afetas a suas atividades, em contrapartida, precisa lidar com a questão relativa aos limites do que pode ser divulgado em matéria de dados pessoais dos cidadãos.

Como explica Curado (2019, p. 22),

> ao mesmo tempo que o texto constitucional traz o princípio da publicidade dos atos da Administração (art. 37, caput) e o direito fundamental de acesso à informação (inciso XXXIII do art. 5º; inciso II do § 3º do art. 37; e § 2º do art. 216), resguarda também os direitos à intimidade e à privacidade (art. 5º, X e LX; e art. 93, IX, segunda parte) – do que deflui a necessidade de compatibilização desses valores.

Silva (2019, p. 36) aborda um relevante tema a ser tratado, em relação ao aspecto da privacidade de dados, qual seja, a criação de um sistema de identificação civil de dimensão nacional, tema tratado pela Lei nº 13.444/2017 (BRASIL, 2017b), que instituiu as bases legais para a formação de uma base de dados pessoais, a Base de Dados da Identificação Civil Nacional (BDICN), o que irá demandar a proteção da lei, dos órgãos e agentes da Administração Pública responsáveis pelo tratamento desses dados, do Ministério Público

Federal (MPF) e dos demais órgãos e entidades responsáveis pela defesa de direitos e garantias fundamentais.

Como é possível perceber, a BDICN tem o potencial de tornar-se uma das maiores bases de dados que o Poder Público manterá a respeito dos cidadãos brasileiros, cuja importância se revela não apenas no volume de dados pessoais que agregará, mas também na sensibilidade de uma parte considerável desses dados. O autor, no entanto, o registra que o texto final da mencionada Lei (Lei nº 13.444/2017) encontra-se omitido, diante da necessidade de criação de normas para a proteção dos dados pessoais que integrarão a BDICN; portanto, o autor aponta que, para solucionar eventuais controvérsias, é possível fazer uso de outras normas de proteção de dados constantes no ordenamento.

Em relação ao aspecto da transparência, o documento (MINAS GERAIS, 2020) traz um importante exemplo, relacionado à administração pública, que se refere à questão da divulgação de dados de servidores no Portal da Transparência. Como consta no mencionado documento, esse fato foi objeto de questionamento, inclusive judicial; no entanto, os tribunais – como o Tribunal Regional Federal da 1ª região (TRF1), o Tribunal Superior do Trabalho (TST) e o Supremo Tribunal Federal (STF) já se manifestaram no sentido de permitir-se a publicidade dos dados. Em decisão unânime proferida em abril de 2011, os ministros do STF concluíram que: “a pessoa que decide ingressar no serviço público adere ao regime jurídico próprio da Administração pública, que prevê a publicidade de todas as informações de interesse da coletividade”. Assim, a remuneração dos agentes públicos é informação de interesse coletivo e fortalece o controle social e, por isso, em princípio, não há mudança com a entrada em vigência da LGPD.

Dessa forma, a LGPD irá coexistir com outras regulamentações existentes. As práticas de transparência institucionalizadas, como o Portal da Transparência, derivam diretamente do princípio constitucional de transparência na Administração Pública. A Lei de Responsabilidade Fiscal (Lei Complementar 101/200) e a LAI (Lei nº 12.527/2011) vêm efetivar esse mandamento, para garantir aos cidadãos o acesso a dados públicos. Pelo analisado, a existência de regulação que disciplina o funcionamento de bancos de dados pessoais governamentais, coexiste com as garantias previstas na LGPD. As soluções legislativas que tratam os dois aspectos, ou seja, a transparência e a privacidade de dados pessoais, precisarão conviver para garantirem a segurança social sem perderem de vista como a falta de controle de dados pessoais afeta a comunicação e participação humanas (MINAS GERAIS, 2020, p. 7).

3.2 Como a organização pode preparar-se para adequação à LGPD

A cartilha do estado de Minas Gerais (2020, p. 14) traz esta orientação simplificada para permitir a adequação das organizações à LGPD, assim discriminada, de forma adaptada.

1. O primeiro passo é observar os fundamentos da proteção de dados pessoais:

• respeito à privacidade;

• inviolabilidade da intimidade, da honra e da imagem;

• autodeterminação informativa;

• liberdade de expressão, informação, comunicação e opinião;

• desenvolvimento econômico e tecnológico, e inovação;

• livre-iniciativa, livre concorrência e defesa do consumidor;

• direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas naturais.

2. O segundo passo é o mapeamento dos dados utilizados, coletados e armazenados na organização. Para realizar esse mapeamento, as seguintes etapas são sugeridas:

2.1 Levantamento dos dados da organização:

- dados estruturados (organizados e representados em uma estrutura previamente planejada para armazená-los, como um banco de dados);

- dados não-estruturados (organizados em uma estrutura rígida definida, mas que estão presentes, por exemplo, em um arquivo de texto - como textos, planilhas, imagens, arquivos de áudio ou vídeo).

2.2 Mapeamento dos dados pessoais: identificação e inclusão dos dados pessoais em uma estrutura previamente definida.

2.3 Classificação dos dados, observados os princípios estabelecidos na lei. Eis os 10 princípios da LGPD para tratamento de dados pessoais:

I - Finalidade: a finalidade do tratamento dos dados deve ser específica e informada explicitamente ao titular.

II - Adequação: os dados devem ser tratados de acordo com a finalidade informada e acordada com o titular.

III - Necessidade: somente o mínimo de dados necessários para realizar a finalidade informada deve ser tratado. A abrangência deve limitar-se a dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento.

IV - Livre acesso: acesso fácil e gratuito dos titulares à forma, duração do tratamento, e integralidade (conteúdo) de seus dados pessoais;

V - Qualidade dos dados: os dados devem ser exatos, claros, atualizados e relevantes, de acordo com a necessidade e finalidade do tratamento.

VI - Transparência: informações claras e facilmente acessíveis sobre o tratamento e os respectivos agentes de tratamento.

VII - Segurança: medidas de proteção aos dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

VIII - Prevenção: medidas para prevenir danos decorrentes do tratamento de dados pessoais.

IX - Não discriminação: não é permitido o tratamento para fins discriminatórios, ilícitos ou abusivos.

X - Responsabilização e prestação de contas: demonstração, do agente, de que adotou medidas eficazes que comprovam o cumprimento das normas de proteção de dados pessoais.

Considerados os princípios para tratamento de dados, a organização precisa demonstrar que os dados pessoais coletados são necessários, mínimos, corretos, de qualidade e atendem uma finalidade de negócio válida. Para tal, os seguintes aspectos devem ser considerados:

- revisão e adequação de políticas (internas e em relação a terceiros), contratos, procedimentos e demais atividades que envolvam tratamento de dados pessoais (agentes públicos e clientes) aos princípios estabelecidos na LGPD;

- manutenção e estruturação de registros, preferencialmente por escrito, que demonstrem a adoção de medidas para adequação das operações de tratamento aos princípios estabelecidos na LGPD, independentemente do tamanho da base de dados existente.

3. Por fim, deve-se ter em mente que a Lei também será aplicada aos subcontratantes de uma organização, como fornecedores e parceiros de tecnologia. Assim sendo, eles também ficam sujeitos às obrigações e podem estar sujeitos a realizar pagamentos de indenização.

Nesse passo, é importante definir, nas relações com terceiros o papel de um fornecedor ou parceiro, se este será encarado como controlador ou operador, ou ambos, para definir os limites da sua responsabilidade.

3.3 Por que a Lei abrange o setor público?

Angela Maria Rosso (2019) destaca que, dentre todos os concentradores de dados pessoais, o Estado se sobressai, pois controla, ainda que indiretamente, a vida financeira, o acesso à saúde, eventuais processos judiciais colecionados durante a vida, dados educacionais, dados trabalhistas do cidadão, entre outros. O Estado é também um empregador de peso, consideradas as instâncias municipais, estaduais e federais da Administração Direta e Indireta. O governo é, ainda, o maior acionista de grandes empresas de tecnologia que operam com esses dados, pois que os coletam, armazenam ou utilizam.

Por outro lado, a inclusão do setor público no escopo da LGPD, obriga-o a adequar-se, investindo em questões de segurança que, muitas vezes, são negligenciadas, e a atuar de forma a evitar a comercialização de dados pessoais para fins diferentes daqueles aos quais foram coletados. Ademais, o governo tem-se tornado cada vez mais digital, utilizando aplicativos, aplicações de *internet* como estratégia para aproximar-se de cidadãos e facilitar o acesso à informação e a prestação de determinados serviços.

Diante do cenário apresentado, torna-se impossível pensar em uma lei de proteção de dados efetiva sem que o setor público esteja incluído, pois, a Administração Pública direta e indireta em todas as esferas - federal, estadual e municipal - é um grande controlador de dados pessoais, e em um Estado democrático de direito deve submeter-se às leis também no que tange à proteção de dados.

3.4 Quando a LGPD não se aplica

O artigo 4º da LGPD é de fundamental importância no tocante ao tratamento de dados realizado pela Administração Pública, em especial no que diz respeito ao seu inciso III, visto que afasta a incidência da LGPD quando o tratamento de dados pessoais for realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais.

Para Angela Maria Rosso (2019), a importância da não incidência se dá na medida em que é a Administração Pública que, por exemplo, detém a posse e controla todos os dados do sistema prisional, da mesma forma que é sua atribuição investigar qualquer ação que coloque em risco a segurança pública ou do próprio Estado. Trata-se assim de casos em que as atividades se revestem de caráter puramente estatal e protegem a Administração Pública de qualquer responsabilidade quanto aos tratamentos realizados.

No entanto, considerando que esse leque de situações é amplo e que a alegação de que é preciso garantir a segurança tem sido utilizada como justificativa para inúmeras violações da privacidade, a lei traz algumas exigências para o afastamento de sua aplicação. Dessa forma, para a aplicabilidade do tratamento dos dados nos casos enumerados no art. 4º, inciso III, é exigida a legislação específica, respeitados todos os princípios constitucionais específicos ao caso. Exemplificando, a Lei n. 12.654/1213 é a base legal que afasta a aplicação da LGPD ao regulamentar a coleta de material genético de pessoas presas.

4 Metodologia utilizada

O presente trabalho seguiu os princípios de um estudo exploratório, por meio de uma pesquisa bibliográfica e o estudo de casos reais, tanto no país quanto no exterior.

Foram também analisadas diversas legislações que tratam do tema estudado, bem como analisadas as práticas recomendadas pela Administração Pública, em todas as suas instâncias.

5 Considerações finais

A pesquisa viabilizou uma análise no atendimento ao objetivo proposto, qual seja, analisar os aspectos que envolvem o *compliance*, necessários para adequação das organizações à LGPD, com ênfase no setor público. Busca ainda apresentar subsídios para que seja possível aos profissionais do Direito apoiar as organizações na elaboração de um Plano de integridade.

A Administração Pública, ao longo do tempo, vem aderindo às inovações tecnológicas, buscando aproximar governo e cidadão, ou objetivando facilitar a vida da sociedade, a exemplo do INSS, o FGTS, a bolsa-família, o e-social, a CNH Digital, o Imposto de Renda, entre outros.

Assim, a transparência e a política de dados abertos governamentais, conjugadas à necessidade de proteção de dados pessoais, adquirem significativa importância, face à transformação das comunicações, intensificada pelo uso massivo das tecnologias digitais. Também, a progressiva disseminação do uso do ambiente virtual como espaço de interação do cidadão com a Administração pública, reforça a necessidade do preparo das organizações públicas para lidarem com as questões da privacidade de dados dos cidadãos, bem como, traz para os órgãos de controle uma maior importância do acompanhamento, quanto ao cumprimento, pelo Poder Público, do dever de transparência em sua atuação, mas também em relação ao resguardo de medidas adequadas de proteção de dados pessoais dos envolvidos.

Assim, analisados todos esses aspectos, no sentido de atender a LGPD e demais dispositivos legais, abordamos os aspectos relacionados à necessidade de que os profissionais do Direito, especializados em Direito Digital e Lei Geral de Proteção de Dados, com ênfase na administração pública, estudem o negócio das organizações em que atuam, para que as organizações consigam o quanto antes possível realizar as ações imprescindíveis para garantir o *compliance* com a nova Lei.

Referências

BANCO MUNDIAL. *World Development Report 2017*: governance and the law. Washington: The World Bank, 2017. Disponível em: http://www.worldbank.org/en/publication/wdr2017. Acesso em: 10 out. 2020.

BRASIL. *Constituição da República Federativa do Brasil*. Brasília: Senado Federal, 1988. Disponível em: https://www2.senado.leg.br/bdsf/item/id/508200. Acesso em: 10 out. 2020.

BRASIL. *Lei Geral de Proteção de Dados (LGPD)*; Guia de Boas Práticas para Implementação na Administração Pública Federal. (BRASIL, 2020)

BRASIL. *Decreto n. 10.046, de 9 de outubro de 2019*. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 10 set. 2020.

BRASIL. Governo Federal. *Guia da Política de Governança Pública*. (2018a). Disponível em: https://www.cgu.gov.br/noticias/2018/12/governo-federal-lanca-guia-sobre-a-politica-de-governanca-publica/guia-politica-governanca-publica.pdf. Acesso em: 10 fev. 2020.

BRASIL. CGU. *Portaria CGU nº 1075, de 23 de abril de 2018*: Aprova o Plano de Integridade do Ministério da Transparência e Controladoria-Geral da União (1. versão). Disponível em: https://www.gov.br/cgu/pt-br/acesso-a-informacao/governanca/programa-de-integridade-da-cgu/arquivos/portaria-1750-2018.pdf. Acesso em: 01 jan. 2020. (2018b)

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*: Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 10 out. 2020. (2018c)

BRASIL. *Lei nº 13.444, de 11 de maio de 2017*: Dispõe sobre a Identificação Civil Nacional (ICN). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13444.htm. Acesso em: 01 jan. 2020. (2017b)

BRASIL. *Decreto n. 9.203, de 22 de novembro de 2017*. Dispõe sobre a política de governança da Administração Pública Federal direta, autárquica e fundacional. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/D9203.htm. Acesso em: 10 fev. 2020. (2017a)

BRASIL. Tribunal de Contas da União. *Governança Pública*: Referencial básico de governança aplicável a órgãos e entidades da Administração Pública. Versão 2. Brasília, DF: TCU, Secretaria de Planejamento, Governança e Gestão, (2014). 80 p. Disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A24F0A728E014F0B34D4A14347. Acesso em: 23 dez. 2019.

CURADO, Lúcio Mauro Carloni Fleury. Dados abertos governamentais e a proteção de dados pessoais, p. 16-29. *In*: Brasil. Ministério Público Federal. Câmara de Coordenação e Revisão. *Sistema brasileiro de proteção e acesso a dados pessoais*: análise de dispositivos da Lei de Acesso à Informação, da Lei de Identificação Civil, da Lei do Marco Civil da Internet e da Lei Nacional de Proteção de Dados – Brasília: MPF, 2019. 85 p. – (Roteiro de Atuação; v. 3). Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr3/publicacoes. Acesso em: 10 out. 2020.

FRANÇA, Phillip Gil. *Ato Administrativo, Consequencialismo e Compliance*: gestão de riscos, proteção de dados e soluções para o controle judicial na era da IA. 4. edição. São Paulo: Revista dos Tribunais. 2019.

GUERRA, Sérgio. *Discricionariedade e Reflexividade*: uma nova teoria sobre as escolhas administrativas. 1ª edição. Belo Horizonte. Editora Fórum. 2008.

MINAS GERAIS. *LGPD*: *Lei Geral de Proteção de Dados Pessoais*. Grupo de Trabalho sobre a Lei Geral de Proteção de Dados no âmbito do Governo do Estado de Minas Gerais, 2020. Disponível em:

http://cge.mg.gov.br/phocadownload/manuais_cartilhas/pdf/Cartilha%20LGPD4%202.pdf. Acesso em: 17 set. 2020.

INTERNATIONAL FEDERATION OF ACCOUNTANTS. Public Sector Committee. Study 13: *Governance in the public sector*: a governing body perspective. New York: IFAC, Aug. 2001. Disponível em: https://portal.tcu.gov.br/en_us/biblioteca-digital/governance-in-the-public-sector-a-governing-body-perspective.htm. Acesso em: 17 set. 2020.

LIMA, Cíntia Rosa Pereira de. LUCCA, Newton De. Polêmicas em torno da vigência da Lei Geral de Proteção de Dados. Polêmicas em torno da vigência da Lei Geral de Proteção de Dados. *Informativo Migalhas n. 4.964*, 7 de agosto de 2020. Disponível em: https://migalhas.uol.com.br/coluna/migalhas-de-protecao-de-dados/331758/polemicas-em-torno-da-vigencia-da-lei-geral-de-protecao-de-dados. Acesso em: 15 set. 2020.

MARCHESINI PINTO, Aline. *Governança pública e escolhas administrativas planejadas*. Dissertação (Mestrado). Universidade Federal do Estado do Rio de Janeiro, Programa de Pós-Graduação em Direito, 2020. Rio de Janeiro, 2020. 182 f.

MOREIRA NETO, Diogo de Figueiredo. *O Direito Administrativo no Século XXI*. 1a Ed. Belo Horizonte: Fórum, 2018.

PEDROSO, Juliana. Lei prevê pena leve para crimes cibernéticos como o do hacker de Moro. *Gazeta do Povo*. 27 jul. 2019. Disponível em: https://www.gazetadopovo.com.br/republica/crimes-ciberneticos-moro/. Acesso em: 15 set. 2020.

ROSSO, Angela Maria. LGPD e setor público: aspectos gerais e desafios. *Migalhas, Informativo n. 4.973*, 18 abr. 2019. Disponível em: https://www.migalhas.com.br/dePeso/16,MI300585,31047-LGPD+e+setor+publico+aspectos+gerais+e+desafios. Acesso em: 17 set. 2020.

SILVA, Manoel Antonio Gonçalves da. A Identificação civil nacional e a proteção de dados pessoais, p. 30-56. *In*: Brasil. Ministério Público Federal. Câmara de Coordenação e Revisão. *Sistema brasileiro de proteção e acesso a dados pessoais*: análise de dispositivos da Lei de Acesso à Informação, da Lei de Identificação Civil, da Lei do Marco Civil da Internet e da Lei Nacional de Proteção de Dados – Brasília: MPF, 2019. 85 p. – (Roteiro de Atuação; v. 3). Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr3/publicacoes. Acesso em: 17 set. 2020.

SORRENTINO, Giancarlo. *Diritti e Partecipazzione nell`amministrazione di resultado*. Napoli: Scientifica, 2003.

SZTAJN, Rachel; e SILVA, Reinaldo Marques da. A relação entre *compliance* e a LGPD. *Consultor Jurídico*, 8 set. 2020. Disponível em: https://www.conjur.com.br/2020-set-08/sztajn-marques-silva-relacao-entre-compliance-lgpd. Acesso em: 10 out. 2020.

VALLE, Vanice Regina Lírio do; SANTOS, Marcelo Pereira dos. Governança e compliance na administração direta: ampliando as fronteiras do controle democrático. *Revista de Direito Administrativo e Constitucional*, Belo Horizonte, ano 19, n. 75, p. 161-177, jan./mar. 2019. Disponível em: https://www.researchgate.net/publication/333723958_Governanca_e_compliance_na_administracao_direta_ampliando_as_fronteiras_do_controle_democratico/link/5d97c09292851c2f70eb9369/download. Acesso em: 27 nov. 2019.

VALLE, Vanice Regina Lírio do. *Repensar a função legislativa a partir da aceleração das novas tecnologias.* 2° #tbt New law. 2019b. Acesso por e-mail: https://us7.campaign-archive.com/?u=c3d51024e48cc8b74a6a8dbd0&id=003c5e6c80&e=0cb81c7f1d. Acesso em: 17 fev. 2020.

A LGPD, os cibercrimes e a adesão do Brasil à Convenção de Budapeste

Érica Maia Campelo Arruda

Patricy Barros Justino

Resumo: O presente artigo tem como objetivo de analisar o impacto, em termos dos crimes cibernéticos, tanto da entrada em vigor da LGPD como em relação à pandemia da COVID-19 e a recente adesão do Brasil à Convenção de Budapeste. Com a pandemia, o número de crimes cibernéticos cresceu em todo o planeta, em muito alavancada pelo uso maciço de meios tecnológicos e da Internet. Sem dúvida, o combate ao cibercrime no País vem evoluindo, inicialmente com o Marco Civil da Internet e agora com a Lei Geral de Proteção de Dados (LGPD). No entanto, somente a Convenção de Budapeste garante a cooperação entre países nas investigações deste tipo de crime. Assim, foi adotada uma metodologia exploratória, tendo em vista que no país não há ainda uma vasta literatura que trate o tema do cibercrime relativo à adesão do Brasil à Convenção de Budapeste, embora os impactos da LGPD já tenham sido amplamente abordados. A adesão do Brasil à Convenção de Budapeste é uma demanda antiga, em que precisava demonstrar alinhamento contra a criminalidade cibernética, em relação aos demais países. Destacamos a importância desta adesão em relação à agilidade nas ações no combate ao cibercrime, quando existe este alinhamento. Outro aspecto abordado é a necessidade da capacitação das polícias e dos profissionais de direito neste tipo de crime, destacando a importância da troca de informações que a Convenção permite.
Palavras-chave: Cibercrime. Convenção de Budapeste. LGPD.

1 Introdução

Atualmente o ciberespaço assume uma posição como um *global common*[38], sem fronteiras físicas e espaços de soberania definidos corretamente, o que torna difícil diferenciar público e privado, civil e militar, nacional e internacional e potencializa o aparecimento de

[38] Pose (2003) ampliou o conceito de *common* (que inicialmente o grande estrategista americano Alfred Thayer Mahan (1840-1914) aplicava ao mar), ao ar e ao espaço – designando-os como os *global commons* – os *global commons* não pertencem a nenhum estado e ninguém pode reclamar soberania sobre eles ou proibir seu uso. Em 2009, a "Cyberspace Policy Review" assinada pelo Presidente Obama, identifica o ciberespaço como uma das propriedades de segurança dos EUA, assemelhando-o, em termos de importância estratégica, aos outros espaços comuns. Em janeiro de 2010, foi publicado um estudo do Center for New American Security, intitulado "Contested Commons: The Future of American Power in a Multipolar World", que acrescentou, à lista de Commons apresentada por Posen, um novo espaço comum: o ciberespaço. Dessa forma, atualmente, no âmbito dos estudos estratégicos militares, considera-se que os *global commons* são o mar, o ar, o espaço e o ciberespaço, conforme Monteiro (2014, p. 5).

novas ameaças. Este novo espaço global tem-se vindo a converter num vetor privilegiado para a realização de ataques contra indivíduos, empresas, redes públicas e privadas, infraestruturas críticas ou mesmo contra os próprios processos e sistemas de governança eletrônica do Estado. O aumento da ciberconflitualidade e a crescente militarização do ciberespaço otimizam o uso da força e a ocorrência de conflitos armados no ciberespaço, o que exige um esforço da comunidade internacional para fazer convergir e promover o ajustamento das várias legislações nacionais, de forma a facilitar o combate ao cibercrime e reduzir o nível da ciberconflitualidade mais violenta.

Destarte, a nova criminalidade recorre às tecnologias de informação, à especialização de tarefas, à inteligência combinada com violência, à internacionalização, ao trabalho em rede, e caracteriza-se por um grande espírito de iniciativa e mentalidade empresarial, respondendo a situações de mercado em constante mutação, fatores que preconizam conforme Souza (2001, p. 326) uma resposta dinâmica, coordenada, integrada e multidisciplinar.

Como destaca Castells (2001, p. 22), o final do século XX foi marcado pela ocorrência de "substantivas mudanças tecnológicas concentradas nas tecnologias da informação que remodelaram a base material da sociedade, formatando novas formas de relação entre a economia, o Estado e a sociedade".

Se, por um lado, existem muitos aspectos positivos no uso massivo da tecnologia e no acesso à internet, por outro, tal realidade fez surgir crimes especializados no mundo virtual, que a cada dia mais trazem riscos à sociedade.

Dessa forma, o presente artigo tem o objetivo de analisar o impacto, em termos dos crimes cibernéticos, tanto da entrada em vigor da LGPD como em relação à pandemia da Covid-19 e à recente adesão do país à Convenção de Budapeste.

Com o advento da pandemia da Covid-19, o número de crimes cibernéticos cresceu em todo o planeta, em muito alavancada pelo uso maciço de meios tecnológicos e da Internet. Sem dúvida, o combate ao cibercrime no país vem evoluindo, inicialmente com o Marco Civil da Internet e agora com a Lei Geral de Proteção de Dados (LGPD). No entanto, somente a Convenção de Budapeste garante a cooperação entre países nas investigações desse tipo de crime.

A adesão do Brasil à Convenção de Budapeste é uma demanda antiga, pois a Convenção data de 2001. O país precisava demonstrar alinhamento contra a criminalidade cibernética, em relação aos demais países. A análise realizada busca destacar a importância dessa adesão em relação à agilidade nas ações no combate ao cibercrime, quando existe este alinhamento. Outro aspecto abordado é a necessidade da capacitação das polícias e dos profissionais de direito nesse tipo de crime, destacando a importância da troca de informações que a Convenção permite.

Nesse sentido, são abordadas as leis brasileiras que tratam do cibercrime, em especial a Lei nº 12.737/2012 - Lei Carolina Dieckmann (BRASIL, 2012a), a Lei nº 12.965/2014 - Marco Civil da Internet (BRASIL, 2014) e a LGPD (BRASIL, 2018a), que recentemente entrou em vigor.

São também estudados os tratados e convenções internacionais sobre o Ciberespaço, com destaque à Convenção de Budapeste (Convenção do Conselho da Europa sobre o Cibercrime)[39]. No decorrer do estudo realizado, observa-se que o caminho mais adequado para combater os cibercrimes são os acordos internacionais, pois, devido à sua própria natureza internacional, passam a uniformizar as práticas nos países membros e permitem a troca de informações entre países signatários.

Com vistas a uma conceituação a ser utilizada no presente artigo, é trazido também um arcabouço de conceituações, tratando de espaço cibernético, cibercrime e suas classificações, passando por uma breve preleção sobre direito digital.

Assim, ao final do estudo, pretende-se contribuir para o conhecimento do tema relacionado ao cibercrime, em especial quanto às possibilidades que a adesão à Convenção de Budapeste abre para o país.

Como observação de cunho geral, um registro não pode deixar de ser colocado. Pelos estudos realizados, nota-se que os operadores de direito no Brasil se mostram ainda distantes da realidade dos cibercrimes, das condutas adequadas no mundo virtual e do conhecimento dos tipos de invasores e de invasões que podem ser encontrados no espaço cibernético. O segmento legislativo também precisa de maior desenvolvimento em nosso país, pois as leis

[39] A Convenção sobre o Cibercrime, também denominada Convenção de Budapeste, foi adotada pelo Comitê de Ministros do Conselho da Europa, em 8 de novembro de 2001, durante a sua 109ª Sessão Plenária, e foi aberta à assinatura na cidade de Budapeste, em 23 de novembro de 2001, na Conferência Internacional sobre o Cibercrime (COUNCIL OF EUROPE, 2001).

bem elaboradas, oportunas e atualizadas são mais aderentes às demandas inerentes ao ciberespaço. Além desses aspectos, a celeridade nos processos por meio da justiça se faz premente na dinâmica dos cibercrimes. Em decorrência, planos para a adaptação do ensino jurídico no país são também postos à mesa, além da visualização clara da necessidade de melhor preparar e aparelhar polícias para treinamento de policiais, além de investir na atualização técnica de servidores do Poder Judiciário e dos operadores do direito em geral. Nesse sentido, cabe destaque à frase de Pinheiro (2016): "o Direito deve adaptar-se às demandas, aos anseios da sociedade, onde as transformações são cada vez mais rápidas".

2 Fundamentação teórica

2.1 Contextualização: "espaço cibernético e cibercrime"

2.1.1 "Espaço cibernético" ou "ciberespaço"

O termo "espaço cibernético" foi cunhado pelo escritor norte-americano Willian Gibson, em seu romance "*Burning Chrome*", pela primeira a vez publicado em 1982; o termo advém da junção dos termos cibernética e espaço. Gibson descreve esse "espaço cibernético" explicando que "a matriz é uma representação abstrata dos relacionamentos entre sistemas de dados. Programadores legítimos entram no setor da matriz de seus empregadores e se veem cercados por geometrias brilhantes representando os dados corporativos" (GIBSON, 2003, p. 25, tradução nossa).

O autor já demonstra em sua obra a existência e manuseio de grandes quantidades de dados, que trazem para ele uma preocupação com a segurança desses dados: "Torres e campos variavam no não-espaço incolor da matriz de simulação, a alucinação de consenso eletrônico que facilita o manuseio e intercâmbio de grandes quantidades de dados" (GIBSON, 2003, p. 25, tradução nossa).

Na obra "Neuromancer", publicada em junho de 1984, Gibson descreve um novo local, um espaço virtual criado pela interação da tecnologia com o homem, onde uma nova realidade poderia surgir, trazendo modificações profundas nas relações humanas e na própria forma de conduzir suas relações, sejam elas pessoais, profissionais ou de negócios (CARNEIRO, 2012, p. 23).

Para Clarke e Knake (2015), o espaço cibernético é formado por todas as redes de computadores do mundo e tudo o que elas conectam e controlam, não só a internet.

De acordo com Lévy (1999), o conceito de “espaço cibernético” é:

> o novo meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo. (LÉVY, 1999, p. 15-16).

É importante destacar que esse novo meio de comunicação, que ocorre entre comunidades virtuais, trouxe novas formas de relacionamentos entre as pessoas, como observa Corrêa (2004, p. 5):

> De qualquer modo, o ciberespaço potencializa o surgimento de comunidades virtuais e de agregações eletrônicas em geral que estão delineadas em torno de interesses comuns, de traços de identificação, pois ele é capaz de aproximar, de conectar indivíduos que talvez nunca tivessem oportunidade de se encontrar pessoalmente. Ambiente que ignora definitivamente a noção de tempo e espaço com barreiras.

Como afirma Lévy (1999), “o ciberespaço constitui, assim, um universo paralelo onde flui intenso fluxo de ligações entre o mundo material e o mundo imaterial, o que leva a uma maior compreensão entre ambos os espaços”.

2.1.1.1 Ordenamento jurídico no “ciberespaço”

Em relação ao “controle” do ciberespaço, o primeiro estudioso a tratar do tema foi o poeta, escritor e ativista da internet, o norte-americano John Perry Barlow, cujas ideias surgiram e tomaram força por ocasião do aumento da utilização comercial da internet, em 1996. A expressão de liberdade na rede fez surgir um sentimento coletivo de que as leis ora existentes não teriam validade no ciberespaço. O pensamento de Barlow tornou-se mais robusto com a publicação, em 1996, da “*Declaration of independence of cyberspace*” (Declaração de independência do ciberespaço)[40], que se contrapunha às medidas jurídicas adotadas pelo governo dos Estados Unidos com o *Communications Decency Act* (CDA), um conjunto de regras, cujo objetivo era o de regular a “indecência” na internet (BARLOW, 1996).

Como destaca Silva Junior (2005), a corrente de ideias de Barlow teve repercussões no Brasil, pois acabou por retardar a adoção de legislação específica para regular as questões jurídicas do ciberespaço.

[40] Trecho da Declaração de Independência do ciberespaço de John Perry Barlow: “Governos do Mundo Industrial, vocês gigantes aborrecidos de carne e aço, eu venho do espaço cibernético, o novo lar da Mente. Em nome do futuro, eu peço a vocês do passado que nos deixem em paz. [...] Eu declaro o espaço social global aquele que estamos construindo para ser naturalmente independente das tiranias que vocês tentam nos impor” (BARLOW, 1996).

Registre-se, ainda, que, no mesmo ano em que Barlow publicou sua "Declaração", David R. Johnson, do Cyberspace Law Institute e David Post da Georgetown University Law nos Estados Unidos, publicaram o artigo "Law and Borders - The rise of law in cyberspace" (O Direito e suas fronteiras – o crescimento do direito no ciberespaço) em uma importante revista jurídica americana, reforçando assim as ideias defendidas por Barlow (JOHNSON; POST, 1996).

Para as autoridades legislativas da época consideravam o ciberespaço como um "ambiente profundamente ameaçador". Os autores depreendem ainda que nessa nova realidade, "novas regras surgirão, em uma variedade de espaços on-line", como se segue, em um trecho do artigo desses mesmos autores supramencionados:

> As comunicações globais baseadas em computador ultrapassam as fronteiras territoriais, criando um novo domínio da atividade humana e minando a viabilidade – e a legitimidade – da aplicação de leis baseadas em fronteiras geográficas. Enquanto essas comunicações eletrônicas causam estragos nas fronteiras geográficas, surge uma nova fronteira, feita de telas e senhas que separam o mundo virtual do mundo real dos átomos. Esta nova fronteira define um ciberespaço distinto que precisa e pode criar novas leis e instituições legais próprias. As autoridades legislativas e de aplicação da lei com base territorial consideram este novo ambiente profundamente ameaçador. Mas as autoridades territoriais estabelecidas ainda podem aprender a submeter-se aos esforços de autorregulação dos participantes do ciberespaço que se preocupam mais profundamente com este novo comércio digital de ideias, informações e serviços. Separadas da doutrina ligada às jurisdições territoriais, novas regras surgirão, em uma variedade de espaços on-line, para governar uma ampla gama de novos fenômenos que não têm paralelo claro no mundo não virtual. Essas novas regras desempenharão o papel da lei, definindo a personalidade jurídica e a propriedade, resolvendo disputas e cristalizando uma conversa coletiva sobre os valores fundamentais. (JOHNSON; POST, 1996, p. 1, tradução nossa).

O que se visualiza nesta concepção utópica de ciberespaço, um espaço sem controle no qual as leis vigentes não alcançam, é que, tal como explica Silva Junior (2005, p. 94), tais ideias alimentaram a polêmica a respeito da impossibilidade de "controle" da Internet e do ciberespaço.

Em oposição a essa corrente doutrinária, como explica Rohrmann, (2005, p. 22), surgiu, a partir das ideias de Lawrence Lessig, professor da Harvard University Law, com a publicação do artigo "Code and Other Laws of Cyberspace" (Código e outros direitos do ciberespaço) em 1999, a corrente "escola da arquitetura da rede". Para Lassig, a relevância da regulação da internet e do ciberespaço não estaria nas leis tradicionais, na regulação imposta pelo Estado, mas sim seria obtida por meio da arquitetura do *hardware* e dos *software*s. Essa regulação

seria obtida, por exemplo, por meio da instalação de filtros de conteúdo e não por meio de leis, o que viria a limitar visivelmente a liberdade de acesso aos usuários da rede.

Entre as correntes jurídicas descritas, que tratam da regulação e controle da Internet, tratamos a seguir da "corrente tradicionalista", que trata da aplicação de leis nacionais a casos concretos, de aplicação das leis ao mundo virtual, embora nem sempre essa corrente não tenha sofrido questionamentos, como destaca Rohrmann (2005):

> A corrente tradicionalista não nega eventuais dificuldades que podem ser encontradas em casos específicos que envolvem o espaço virtual (notadamente os aspectos que envolvem o direito internacional), especialmente no tocante a pontos como produção de provas e combate à fraude e à criminalidade. Todavia, deve-se lembrar que, em relação a este último ponto, há dificuldades muito grandes também quando se fala em combate à criminalidade que ocorre, por exemplo, nos grandes centros urbanos, a despeito de todo o aparelho policial disponível nas mãos do Estado. (ROHRMANN, 2005, p. 34).

Entretanto, com a nova realidade posta, a regulação específica para a Internet e o ciberespaço começou a se firmar no Brasil em 2012, com a Lei Carolina Dieckmann (Lei 12.737/2012) e o Marco Civil da Internet (Lei n. 12.965/14) que tratamos em item a seguir no presente trabalho.

Após as reflexões já efetivadas, para concluir esse item, nova reflexão ocorre: em paralelo aos atributos característicos dos usuários da internet, entre os quais citamos a liberdade de expressão, a privacidade, entre outros, estão postas também as questões do direito, ou seja, como compatibilizar os benefícios que a rede proporciona, com a eminente possibilidade de práticas criminosas, e que, adicionalmente, podem ocorrer em escala mundial?

E mais uma vez recorremos à especialista em direito digital Patricia Peck Pinheiro:

> Até onde um ordenamento jurídico tem alcance? O problema não está apenas no âmbito da internet, mas em toda sociedade globalizada e convergente, na qual muitas vezes não é possível determinar qual o território em que aconteceram as relações jurídicas, os fatos e seus efeitos, sendo difícil determinar que norma aplicar utilizando os parâmetros tradicionais. (PINHEIRO, 2016, p. 38).

É nesse novo espaço de desenvolvimento de múltiplas relações, por meio da internet, que um novo tipo de criminalidade surgiu, muito com base na sensação de anonimato e liberdade, especialmente para os mais jovens. Aparentemente, por trás de um computador, é possível criar e assumir múltiplas identidades, tanto verdadeiras quanto falsas, facilitando, assim, que uma pessoa, com conhecimento médio de informática, seja capaz de passar-se por outra, com o propósito deliberado de praticar ilícitos.

2.1.2 “Cibercrime”

As condutas ilícitas perpetradas no meio virtual podem receber várias denominações, tais como cibercrime, crime digital, crime informático, *cybercrime*, crime virtual, crime eletrônico, delito de computador, delito computacional, crime de computação, entre outros. No presente trabalho, os termos são usados como sinônimos.

Antes de tratar especificamente do cibercrime, analisamos brevemente os tipos e as características dos diferentes invasores de sistemas, meios digitais e eletrônicos em geral. Os mais conhecidos são: *Hacker*, *Cracker*, *Carder*, *Defacer*, *Phreaker*, *Cheater*, *Lammer*, *Noob*, e *Script Kiddie* (TACIO, 2010).

O *Hacker* é aquele indivíduo que, com amplo conhecimento em informática, faz uso desse conhecimento para descobrir a falhas de segurança no sistema e apontar as medidas de correção; em geral, atua como consultor de segurança para empresas; trata-se de um indivíduo bem intencionado, que explora a deficiência na segurança de um sistema ou produto computacional, porém sem intenção escusa.

O C*racker*, por sua vez, também dispõe de amplo conhecimento em informática, porém se utiliza do seu conhecimento de segurança da informação para realizar invasão em sistemas, quebrar senhas, roubar informações, destruir sistemas, em geral para obter valores para si próprio ou para grupos para os quais atua.

O *Carder* utiliza informações bancárias, como números de cartões de crédito, cartões de conta corrente ou poupança, ou contas em *sites* de movimentações bancárias, para benefício próprio, como comprar produtos, fazer transferência para contas de “laranjas” entre outros atos ilícitos.

O *Defacer* utiliza a técnica *Deface* para pichar *sites*, explora vulnerabilidades por meio de técnicas para obter acesso administrativo a um *site*, com a finalidade de alterar a página inicial do mesmo, substituindo-a por uma que ele, invasor, criou.

O *Phreaker* é o *hacker* da telefonia móvel e fixa.

O nome *Cheater* é dado aos indivíduos que usam *cheats* (códigos que burlam o sistema de um jogo) para adquirirem algum privilégio no jogo *online* ou local (advindo de *Cheats* em inglês, trapaças em português). Os *Cheater* são, então, trapaceiros (TACIO, 2010).

Já o *Lammer* é um termo utilizado para as pessoas que não possuem nenhum ou pouco conhecimento e utilizam ferramentas desenvolvidas por outros para realizarem seus ataques.

O *Lammer* não possui um bom conhecimento em informática, ele apenas procura tutoriais na Internet que ensinam a fazer invasões básicas.

O *Noob* ou *Neewbie* é aquele indivíduo que está iniciando (neste caso, em *Hacking*) e possui vontade de aprender, não se denomina *Hacker* e sabe que ainda precisa estudar muito. Em geral, os *Noobs* fazem perguntas bobas e iniciantes em fóruns, comunidades e *sites*.

O *Script kiddie*, tais como os *Noobs*, são aprendizes, sendo que os *Noobs* são como aprendizes de Hackers, já os *Script Kiddies* são como aprendizes de Crackers. Normalmente, essas pessoas utilizam técnicas que ainda não dominam para prejudicarem computadores e obterem benefícios próprios, no entanto, como se trata de Crackers, entre os quais não há lei, a maioria dos *Script Kiddies* caem em armadilhas deixadas pelos próprios Crackers (TACIO, 2010).

Entre as denominações recebidas pelas condutas ilícitas perpetradas no meio virtual, Crespo (2011, p.50) lembra que o termo “cibercrime” acabou por ser o mais utilizado, inclusive por ser a nomenclatura adotada pelo Tratado do Conselho Europeu sobre Crime Cibernético (Convenção de Budapeste).

Como destaca Romano (2019), o Tratado do Conselho Europeu sobre Crime Cibernético (Convenção de Budapeste), usa o termo "cibercrime" para definir delitos que vão de atividades criminosas contra dados até infrações de conteúdo e de copyright (KRONE, 2005 *apud* ROMANO, 2019). Para outros autores (ZEVIAR-GEESE, 1997 *apud* ROMANO, 2019), no entanto, sugerem que a definição é mais ampla e inclui atividades como fraude, acesso não autorizado, pornografia infantil e *cyberstalking* (assédio na Internet).

Segundo Aras (2010, p. 12),

> [...] a criminalidade informática, fenômeno surgido no final do século XX, designa todas as formas de conduta ilegais realizadas mediante a utilização de um computador, conectado ou não a uma rede, que vão desde a manipulação de caixas bancários à pirataria de programas de computador, passando por abusos nos sistemas de telecomunicação. Todas essas condutas revelam "uma vulnerabilidade que os criadores desses processos não haviam previsto e que careciam de uma proteção imediata, não somente através de novas estratégias de segurança no seu emprego, mas também de novas formas de controle e incriminação das condutas lesivas”.

O eminente professor alemão Tiedmann (1985), no texto “Criminalidad mediante computadoras”, conceitua a “criminalidade por meio de computadores”:

> A expressão "criminalidade por meio de computadores" se refere a todos os comportamentos antijurídicos segundo a lei vigente (ou socialmente prejudiciais e por isso, passíveis de punição no futuro) realizados graças ao emprego de um equipamento automático de processamento de dados. Tal conceito, então, abrange,

> por um lado, o problema da ameaça à esfera privada do cidadão, por meio da acumulação, arquivo, associação e difusão de dados por meio de computadores. Na verdade, porém, apenas alguns casos de violação de direitos pessoais foram conhecidos até o momento na Alemanha Ocidental em razão do uso abusivo de dados armazenados em um computador. De qualquer modo, o legislador alemão, na "Lei Federal de Proteção de Dados", reforçou a regulação com normas penais pouco precisas. E, por outro lado, o conceito mencionado se refere aos danos patrimoniais produzidos pelo uso abusivo de dados processados automaticamente. (KLAUS TIEDMANN, 1985, p. 481-482, tradução nossa).

Como pontua Vianna (2001, p. 182), os crimes informáticos, por suas características, exigem estudo de técnicas que permitam o domínio do computador para utilizá-lo na conduta criminosa, o que faz com que o hacker necessite aprender para praticar seus crimes, diferentemente dos crimes clássicos, como homicídio, furto e estupro, que não exigem qualquer tipo de conhecimento para serem cometidos.

2.1.3 Classificação dos "Cibercrimes"

O surgimento de novas condutas ilícitas praticadas na *internet*, envolvendo a utilização de computadores, é cada vez mais intensa e variada e acompanha o desenvolvimento das novas realidades tecnológicas e sociais. Não se observa um consenso em torno das classificações dos cibercrimes. É possível, no entanto, elencar algumas delas, iniciando com aquela proposta por Tiedmann (1985).

O professor Tiedmann (1985), no texto mencionado, explana que, na Alemanha Federal, naquela ocasião, o ponto de partida da discussão acerca da criminalidade por meio de computadores consistiu em determinar se, efetivamente, existia tal forma de delinquência. Tiedmann então esclarece que as investigações conduzidas pelo Instituto de Criminología y Derecho Penal Económico da Universidade de Friburgo, durante dez anos, levaram a uma compilação bastante completa dos assuntos penais, tanto da República Federal de Alemanha como também em âmbito europeu, para acreditar na existência de tal criminologia. Os fatos conhecidos podem ser divididos em quatro grupos, sem levar em conta o emprego de computadores pela comissão de atos econômicos puníveis de carácter geral (tais como delitos em balanços e delitos fiscais). Tais grupos são: manipulações, espionagem, sabotagem e furto de tempo (TIEDMANN, 1985, p. 483-486, tradução nossa).

1) Manipulações. Essas podem afetar tanto a fase de alimentação, ou entrada (*input*) de dados, como a saída (*output*) e a de seu processamento (na forma de manipulações no programa ou na console.

2) Espionagem. No âmbito do processamento de dados, a espionagem econômica acaba por ser favorecida pelo fato de que as informações se encontram arquivadas em um espaço mínimo e podem ser transferidas sem nenhum problema para outra estrutura de suporte. Ademais, no centro do uso indevido de dados figura sempre o também denominado furto de *software* ou emprego indevido de programas de computação, cuja elaboração implica geralmente uma considerável inversão de esforços e, frequentemente, comporta um valioso *know-how* comercial. A título acessório, trata-se principalmente de dados de pesquisa, arquivos referentes a clientes e balanços.

3) Sabotagem. Tanto pela perspectiva da magnitude do dano quanto pelo modo de realizar o fato, merecem ser considerados os casos de sabotagem no processamento de dados. Também estes se beneficiam pela alta compressão de informações em um mínimo espaço. Os serviços secretos de outros países, os fanáticos políticos e os empregados desejosos de vingança devem ser considerados possíveis autores.

4) Furto de tempo. Esse é o último grupo de casos de criminalidade por meio de computadores. A utilização indevida de instalações de cômputos por parte de empregados desleais ou de estranhos pode produzir perdas consideráveis, especialmente naqueles sistemas de processamento de dados a distância, ao serem efetuados cômputos com números de "contas" alheias.

Para Wendt e Jorge (2012), existem as ações prejudiciais atípicas e os crimes cibernéticos. Quanto às ações prejudiciais atípicas, trata-se daquelas condutas que causam prejuízo ou transtorno para a vítima, por meio da rede mundial de computadores, porém não são tipificados em lei. Para os crimes cibernéticos, os autores entendem que estes se dividem em “crimes cibernéticos abertos” e “crimes exclusivamente cibernéticos”. Os “crimes exclusivamente cibernéticos” são aqueles em que, necessariamente, precisa-se do meio da informática para cometer o crime, como se caracteriza no caso do crime de invasão de dispositivo informático, previsto nos artigos 154-A e154-B do código penal, introduzidos pela Lei Carolina Dieckmann. Já os crimes cibernéticos abertos são aqueles que podem ou não ser praticados via meio informático, como é o caso, por exemplo, dos crimes de violação de direito do autor, que pode ser praticado no ambiente virtual ou no analógico.

Para Ivete Ferreira (2001), Crespo (2011) e Schmidt (2014), os crimes virtuais podem ser “próprios” e impróprios”. Os próprios “são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)”. Nessa categoria

entrariam as condutas praticadas por hackers, tanto de invasão de sistemas quanto de modificação, alteração, inserção de dados falsos, ou seja, que atinjam diretamente o *software* ou *hardware* do computador e só podem ser concretizados pelo computador ou contra ele e seus periféricos. Nessa modalidade, o crime só ocorrerá por meio da informática, sem a qual não ocorrerá (esse é o caso, por exemplo, do crime de inserção de dados falsos em sistema de informações, art. 313-A do CP). Quanto aos crimes cibernéticos impróprios, seriam aqueles que atingem um bem jurídico comum, como o patrimônio, e utilizam os sistemas informáticos apenas como animus operandi, ou seja, um novo meio de execução, podendo ser praticados de diversas formas, seja por meio da informática ou não, como ocorre nos casos dos crimes contra a honra e violação direitos do autor, estelionato, crimes contra o patrimônio em geral, pornografia infantil, entre outros.

Há uma outra visão, segundo a qual os crimes cibernéticos podem ser estudados, levando-se em consideração o papel desempenhado pelo computador no contexto da prática do ato ilícito. Nesse sentido, a classificação proposta por Robson Ferreira em seu trabalho sobre crimes eletrônicos é a seguinte (FERREIRA, 2001 *apud* PINHEIRO, 2007, p. 250-251):

1) quando o computador é o alvo do crime cometido. Ex.: crime de invasão, contaminação por vírus, sabotagem do sistema, destruição ou modificação de conteúdo do banco de dados, furto de informação, furto de propriedade intelectual, vandalismo cibernético, acesso abusivo por funcionário, acesso abusivo por terceirizados, acesso abusivo por fora da empresa;

2) quando computador é o instrumento para o crime. Ex.: crime de fraude em conta corrente e/ou cartões de crédito, transferência de valores ou alterações de saldos e fraude de telecomunicações, divulgação ou exploração de pornografia;

3) quando o computador é incidental para outro crime. Ex.: crimes contra honra, jogo ilegal, lavagem de dinheiro, fraudes contábeis, registro de atividades do crime organizado;

4) quando o crime está associado com o computador. Ex.: pirataria de *software*, falsificações de programas, divulgação, utilização ou reprodução ilícita de dados e programas de comércio ilegal de equipamentos e programas.

Para contextualização de um panorama do quantitativo de crimes cibernéticos no Brasil, recorremos aos dados da SaferNet Brasil[41], que, em 14 anos, por meio da sua Central

[41] A SaferNet Brasil é uma associação civil de direito privado, com atuação nacional, sem fins lucrativos ou econômicos, fundada em 20 de dezembro de 2005 por um grupo de cientistas da computação, professores,

Nacional de Denúncias de Crimes Cibernéticos[42], recebeu e processou 4.134.808 denúncias anônimas envolvendo 790.390 páginas (URL) distintas, das quais 574.730 foram removidas, escritas em 9 idiomas e hospedadas em 73.000 domínios diferentes, de 267 diferentes TLD e conectados à *Internet* por meio de 71.049 números IP distintos, atribuídos para 104 países em 6 continentes. As denúncias foram registradas pela população pelos *3 hotlines* brasileiros que integram a Central Nacional de Denúncias de Crimes Cibernéticos. São parceiros da SaferNet Brasil: NIC.br (CGI.br); Petrobras; Ministério Público Federal (MPF) (MPF-SP; MPF-RS; MPF-GO; MPF-PB; MPF-PR; e PMF-RJ); MPRJ; ABECS; Comissão Parlamentar de Inquérito (CPI) da Pedofilia, criada em março de 2008 no Senado Federal; Google; MySpace; Secretaria Especial de Direitos Humanos, Departamento de Polícia Federal; e teles (empresas de Telecomunicações, como Brasil Telecom, OI, TIM, Telefônica/Vivo, Claro, Embratel e NET).

O relatório da autoridade europeia Europol[43], intitulado "Beyond the pandemic – How Covid-19 will shape the serious and organised crime lanscape in the EU", publicado em abril de 2020, dá conta de um aumento no número de cibercrimes e alerta que a pandemia da Covid-19 não é apenas um grave problema de saúde pública, mas também um risco para a segurança virtual.

Sobre as ocorrências do cibercrime, durante a pandemia da Covid-19, o documento da Europol registra:

> O crime grave e organizado está explorando a mudança de circunstâncias durante a pandemia. Desde o início desta crise, a Europol monitorou estes desenvolvimentos para ajudar os Estados-membros a entenderem e lidarem com esses fenômenos emergentes.
> O impacto total da pandemia - não apenas sobre o crime, mas também mais amplamente na sociedade e na economia - ainda não é aparente. No entanto, a aplicação da lei deve estar preparada para ser capaz de responder aos sinais de alerta enquanto o mundo lida com as consequências da pandemia Covid-19. Agora mais que nunca, o policiamento internacional precisa trabalhar com o aumento conectividade tanto no mundo físico quanto no virtual. Esta crise mais uma vez prova que a troca de informações criminais
> é essencial para combater o crime na aplicação da lei comunidade (EUROPOL, 2020, p. 2, tradução nossa).

pesquisadores e bacharéis em Direito, quando os fundadores desenvolveram pesquisas e projetos sociais voltados para o combate à pornografia infantil na Internet brasileira (SAFERNET BRASIL, 2020).

[42] A Central Nacional de Denúncias de Crimes Cibernéticos da SaferNet Brasil é única na América Latina e Caribe, e recebe em média 2.500 denúncias (totais) por dia, envolvendo páginas com evidências dos crimes de Pornografia Infantil ou Pedofilia, Racismo, Neonazismo, Intolerância Religiosa, Apologia e Incitação a crimes contra a vida, Homofobia e maus tratos contra os animais (SAFERNET BRASIL, 2020).

[43] A Europol é a Agência da União Europeia para a Cooperação Policial. responsável por assegurar o cumprimento da lei. O seu principal objetivo é tornar a Europa mais segura, em benefício de todos os cidadãos da União Europeia, conforme informações disponíveis em: https://epso.europa.eu/job-opportunities/institutions-and-agencies/3154-europol-european-union-agency-law-enforcement_pt-pt.

Sobre o futuro do cibercrime, após a pandemia da Covid-19, o mencionado documento destaca:

> O crime cibernético é altamente dinâmico e é difícil projetar que formas a atividade cibercriminosa assumirá no longo prazo. [...]
> As medidas de bloqueio e quarentena introduzidas durante a pandemia ampliaram significativamente a superfície de ataque e os vetores de ataque abertos aos cibercriminosos, à medida que os cidadãos e as empresas estão
> usando soluções digitais e online mais do que nunca para organizar todos os aspectos de suas vidas e atividades. [...]
> Os cibercriminosos continuarão a buscar oportunidades para explorar esses hábitos adaptando os existentes ou inventando novos ataques.
> O fim da crise atual e o levantamento das medidas de bloqueio podem resultar no aumento do número de denúncias de abuso infantil, tais como os abusos ocorridos durante a pandemia COVID-19 foram descobertos e as autoridades de aplicação da lei foram notificadas. (EUROPOL, 2020, p. 10, tradução nossa).

Ainda sobre o tema, o Relatório publicado em maio de 2020 pela Kaspersky, resultado do estudo “Como a Covid-19 mudou a forma das pessoas trabalharem", demonstrou que 67% dos profissionais que estão trabalhando remotamente não receberam treinamento e/ou orientações específicas sobre cibersegurança e 40% dos entrevistados declararam ter sido alvos de ciberataques com o tema Covid-19. Segundo o relatório, é fundamental estabelecer medidas de segurança *on-line* eficientes, pois o trabalho remoto também pode provocar novos riscos, como o aumento de ataques de *phishing* e *spam*, conexões com pontos de *Wi-Fi* comprometidos ou o uso da TI Invisível (*Shadow IT*) pelos funcionários (CIO-IDG, 2020).

2.2 Direito Digital

O direito digital pode ser definido como os direitos e restrições legais que regem o uso da tecnologia. No mundo de hoje, muitas pessoas não são cidadãs digitais responsáveis. São criminosas, infringindo a lei, sabendo ou não o que é apropriado ou inapropriado para o uso da tecnologia.

Podemos asseverar que o direito digital nasceu de uma necessidade de regularem-se questões surgidas com o desenvolvimento da tecnologia e a expansão da *internet*, que são elementos responsáveis por intensas mudanças comportamentais e sociais, bem como para fazer frente aos novos dilemas da sociedade da informação.

Sustenta Peck (2008, p. 29) ao conceituar direito digital que este estabelece um liame com o próprio Direito, afirma que “[...] todos os princípios fundamentais e institutos que estão

vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas.

Asseveram ainda Peck, Pinheiro e Sleiman (2006), diante do cenário que ora se vislumbra, ou seja, da comunicação em tempo real e interatividade de uma sociedade conectada, é de se esperar que o direito também acompanhe esse avanço.

Assim, as autoras entendem que o Direito Digital é a evolução do próprio Direito, pois não se trata de uma nova área, mas sim de todas as áreas já existentes e conhecidas no âmbito jurídico que passam então, diante das novas circunstâncias, a integrar questões tecnológicas. Em consequência, o Direito Digital abrange todos os princípios fundamentais e institutos vigentes que são aplicados até hoje, bem como introduz novos institutos e elementos para o pensamento jurídico, em todas as suas áreas. E observam ainda que, quanto à legislação específica, a velocidade das transformações pode se tornar uma barreira para a evolução jurídica, pois qualquer lei que venha a ser criada a fim de tratar os novos institutos jurídicos devem ser genéricas e flexíveis o suficiente a fim de sobreviver e atender os diversos formatos, formas e resultados que ainda possam surgir.

Na fala de Peck Pinheiro (2007),

> [...]mesmo assim, a generalidade pode ser aplicada aqui, amparada por novos processos de pensamento do Direito como um todo: a norma deve ser genérica, aplicada no caso concreto pelo uso da analogia e com o recurso à arbitragem, em que o árbitro seja uma parte necessariamente atualizada com os processos de transformação em curso.

Para Pimentel (2018, p. 18), "o Direito Digital nasceu da necessidade de se regularem as questões surgidas com a evolução da tecnologia e a expansão da internet, elementos responsáveis por profundas mudanças comportamentais e sociais". Para o autor, a doutrina tem assinalado um aspecto interessante desse ramo do Direito: afirma que o Direito Digital não tem objeto próprio. Seria um Direito com um *modus operandi* diferente, sendo, na verdade, a extensão de diversos ramos da ciência jurídica, que cria novos instrumentos para atender a anseios e ao aperfeiçoamento dos institutos jurídicos em vigor" (ARAÚJO, 2017, p. 24).

Assim Pimentel (2018, p. 37) resume o seu entendimento sobre o Direito Digital: "[o] Direito Digital abrange todas as áreas do Direito, de maneira transversal, e congrega novos elementos para dirimir os conflitos surgidos com a tecnologia, especialmente a Internet, e regular as relações da denominada 'sociedade da informação'". E lembra ainda que, no campo

do Direito Penal, o computador e a Internet têm sido cada vez mais usados para a prática de crimes, o que fez surgir o "bem jurídico informático" e a necessidade de se preverem novos tipos penais. No âmbito internacional o autor destaca a existência de normas específicas destinadas à contenção dos crimes cibernéticos e a disciplinar o manejo de dados pessoais, com vista à proteção da privacidade (PIMENTEL, 2018, p. 37).

3 A Convenção de Budapeste e as leis brasileiras que tratam de cibercrimes

3.1 Leis brasileiras que tratam de cibercrimes: principais aspectos e o caminho até 2020

De forma resumida, o quadro a seguir apresenta a trajetória legislativa brasileira para regular o tema "privacidade" e também os "cibercrimes", até o advento da LGPD, cuja entrada em vigor se deu recentemente, em 18 de setembro de 2020.

Quadro 12 – Legislação brasileira sobre privacidade e crime cibernético

Ano/documento/ legislação	Principais aspectos
- Constituição de 1988 (BRASIL, 1988); - Código Civil de 2002 (BRASIL, 2002)	- A Constituição de 1988 trata, também, de *sigilo* (de correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas) e da *inviolabilidade da casa*. Assim, no Brasil, previsto tanto na Constituição quanto na legislação infraconstitucional, o direito à privacidade é considerado direito fundamental *e* direito da personalidade [...]. - O constituinte optou pelo uso dos termos *intimidade* e *vida privada*, para fazer referência à privacidade, sendo a última expressão também a opção do legislador ao elaborar o Código Civil de 2002 (Lei n. 10.406) (CANCELIER, 2017).
2010	Em novembro de 2010 foi iniciado o debate sobre a proteção de dados pessoais, visando elaborar uma lei específica sobre o tema para o país. Até abril de 2011, o Ministério da Justiça manteve um *blog* para colher manifestações na plataforma Cultura Digital, do Ministério da Cultura. O resultado dessas primeiras discussões nunca foi enviado pelo Poder Executivo ao Congresso Nacional.
2011 – Lei 12.527 de Acesso à Informação (BRASIL, 2011)	Em 2011 surgiu a Lei de Acesso à Informação, chamada de "LAI", cujo objetivo era promover a transparência das informações de posse do poder público, disciplinando o direito de acesso à informação previsto na Constituição Federal.
junho de 2012 Projeto de Lei nº 4060/2012 (CÂMARA DOS DEPUTADOS, 2012)	Em junho de 2012, o Deputado Milton Monti (PR-SP) apresentou na Câmara dos Deputados o Projeto de Lei nº 4060/2012 que: "Dispõe sobre o tratamento de dados pessoais, e dá outras providências", o qual foi produto das discussões do V Congresso Brasileiro da Indústria da Comunicação.
Lei 12.735/12 – "Lei Azeredo" (BRASIL, 2012b)	Alterou o inciso II do § 3° do art. 20 da Lei n° 7.716/8918, conhecida como Lei do Crime Racial, para permitir que uma solicitação de retirada de conteúdo discriminatório, de qualquer meio possível, não somente de rádio, TV ou Internet, fosse feita pelo Juiz. O texto aprovado determina ainda que os órgãos da polícia judiciária deverão criar delegacias especializadas no combate a crimes digitais (art. 4º) (CRESPO, 2015).
30 de novembro de 2012 Lei Carolina Dieckmann (BRASIL, 2012b)	A Lei Carolina Dieckmann, como ficou conhecida a Lei Brasileira 12.737/2012, sancionada em 30 de novembro de 2012 pela então presidente Dilma Rousseff, promoveu alterações no Código Penal Brasileiro (Decreto-Lei 2.848, de 7 de dezembro de 1940). Ficou conhecida com o nome da atriz, pois, em 2012, um escândalo envolvendo a atriz, por terem sido vazadas suas fotos íntimas, causou

	pressão da sociedade nesse sentido, agilizando a tramitação, na Câmara, de projetos de Lei que já se encontravam em andamento. A Lei criminaliza a invasão de aparelhos eletrônicos com a intenção de obtenção de dados pessoais, tipificando, assim, os chamados delitos ou cibercrimes. - A Lei inseriu os arts. 154-A e 154-B no Código Penal, criando a "invasão de dispositivo informático" e regulamentando sua ação penal, que será condicionada à representação como regra e, no caso de prática em desfavor da Administração Pública, será pública incondicionada (CRESPO, 2015).
2014 PLS 181/2014 (SENADO FEDERAL, 2014)	Foi apresentado pelo Senador Vital do Rêgo o Projeto de Lei do Senado PLS 181/2014 que "Estabelece princípios, garantias, direitos e obrigações referentes à proteção de dados pessoais".
2014 – Lei 12.965 "Marco Civil da Internet" (BRASIL, 2014)	O Marco Civil da Internet, sancionado em 2014, prevê proteção da privacidade, proteção dos dados pessoais, inviolabilidade da intimidade e da vida privada, entre outros pontos da vida on-line regulamentados. (PEDROSO, 2019) O Marco Civil, reforçava (com a devida modernização) o direito à privacidade, mas ainda não garantia a proteção de dados como a LGPD propõe hoje.
2015	Em 2015, o Ministério da Justiça lançou consulta pública para discutir a proteção de dados pessoais armazenados em centrais dentro ou fora do País. Conforme notícia divulgada no site da Câmara dos Deputados à época, o então ministro da Justiça, afirmou: "a ideia é estimular o debate entre a sociedade civil e o Congresso Nacional, nos moldes do Marco Civil da Internet, para construir um "texto democrático tanto na forma quanto no conteúdo" (CÂMARA DOS DEPUTADOS, 2015).
abril de 2016 Aprovação, pela União Europeia (UE), do GDPR (INFORMATION COMISSIONER'S OFFICE, 2020)	A aprovação, pela União Europeia do Regulamento Geral de Proteção de Dados Pessoais (GDPR), em abril de 2016, acabou por precipitar os fatos, tendo em vista que, entre as exigências do GDPR, todos os países e organizações que pretendessem manter relações comerciais com a União Europeia deveriam dispor de uma legislação de proteção de dados pessoais em conformidade com o que determinava o Regulamento.
2016: Decreto nº 8.771, de 11 de maio de 2016 (BRASIL, 2016)	Decreto nº 8.771, de 11 de maio de 2016. Regulamenta a Lei nº 12.965, de 23 de abril de 2014.
13 de maio de 2016: encaminhado ao Congresso o Projeto de Lei n. 5276/2016 CÂMARA DOS DEPUTADOS, 2016)	Em 13 de maio de 2016, a então presidente Dilma Rousseff encaminhou ao Congresso, em regime de urgência, Projeto de Lei n. 5276/2016, pelo Poder Executivo, que: "Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural". Em julho de 2016, o presidente interino Michel Temer retirou o regime de urgência e foi apensado o Projeto de Lei n. 5.276/2016 ao Projeto de Lei n. 4.060/2012.
15 de agosto de 2018 publicada no Diário Oficial da União a Lei nº 13.709 de 14 de agosto de 2018: LGPD (BRASIL, 2018a)	Em julho de 2018 o Projeto Lei da Câmara 53/2018 foi aprovado por unanimidade, e em regime de urgência, no plenário do Senado, gerando a Lei nº 13.709 de 14 ago. 2018: Lei Geral de Proteção de Dados (LGPD). Assim, a LGPD foi publicada no Diário Oficial da União em 15 de agosto de 2018, e republicada parcialmente no mesmo dia, em edição extra. Estava previsto que o início da vigência seria em 18 meses a contar da publicação. O texto é aplicável mesmo a empresas com sede no exterior, desde que a operação de tratamento de dados seja realizada no território nacional. Apesar de sancionada, houve o veto à criação da Autoridade Nacional de Proteção de Dados e a condição de entrada em vigor 18 meses (fevereiro de 2020) após sua publicação.
27/12/2018 Medida Provisória nº 869, de 27 de dezembro de 2018	Editada pelo então presidente Temer a Medida Provisória nº 869, de 27 de dezembro de 2018, prevendo a criação da ANPD e alterando o início da vigência da lei para agosto de 2020.

novembro de 2018: Medida Provisória nº 869/2019	Ao final de 2018, o então Presidente da República Michel Temer promulga a Medida Provisória nº 869/2019 que autoriza a criação da Autoridade Nacional de Proteção de Dados e aumenta o prazo da entrada em vigor da Lei para 24 meses (agosto de 2020) e retira a obrigatoriedade de revisão humana de decisões tomadas no tratamento automatizado de dados pessoais.
julho de 2019	O Presidente da República promulga o decreto nº 9936/2019: Regulamenta a Lei nº 12.414, de 9 de junho de 2011, que disciplina a formação e a consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.
08 de julho de 2019	A Lei 13.853/2019 foi aprovada, e dentre as suas mudanças, estava a criação da ANPD – Autoridade Nacional de Proteção de Dados e a alteração da data de início de vigência da LGPD, para 08/2020.
outubro de 2019	Projeto de lei (não acatada) sugere prorrogação da entrada em vigor da LGPD para 15 de agosto de 2022 (48 meses depois)
03 de abril de 2020	Por conta da situação pandêmica do país, o PL 1.179 é aprovado no Senado. Ele alterava a data de entrada em vigor da LGPD para 01/2021, com sanções administrativas valendo para 08/2021.
29 abril de 2020	Presidência da República promove a edição da MP 259/2020 que alterava a eficácia da lei e as penalidades ficariam para 05/2021.
14 maio 2020	O PL 1.179 foi aprovado na Câmara e, conforme já mencionado acima, previa a aplicação das penalidades para 08/2021.
19 maio 2020	O PL 1.179 foi votado novamente no Senado, acatando a situação proposta pela Câmara alguns dias antes, fazendo com que este projeto de lei seguisse para sanção do Presidente da república.
02 de junho de 2020	Depois de diversas sugestões de modificações, especialmente devido a pandemia do covid-19, o PL 1179/2020 é sancionado e convertido na Lei nº 14.010/2020 que mantém a vigência da LGPD para agosto de 2020, mas com a condição de que as multas e sanções só começariam a valer a partir de 1º de agosto de 2021.
25 de agosto de 2020	Câmara aprova a MP 959/2020, que definia a entrada da LGPD para 01/2021 e as penalidades para agosto do mesmo ano.
Um dia depois da aprovação da MP pela Câmara	Senado derruba o artigo 4º da MP 959/2020 que tratava da prorrogação da vigência da lei, fazendo com que a entrada da LGPD retornasse à 08/2020 com penalidades para 08/2021.
17 de setembro de 2020	Sanção da presidência, aprovando a LGPD.
18 de setembro de 2020	LGPD entra em vigor.

Fonte: https://www.portaldaprivacidade.com.br/lgpd-linha-do-tempo; https://www.serpro.gov.br/lgpd; e Fernandes (2020)

3.2 A cooperação penal internacional: breves considerações

Historicamente, antes do estabelecimento de um processo de penalização de graves crimes contra a humanidade, é possível identificar as dificuldades de efetiva punição por tais condutas pelos Estados nacionais.

Delgado (2007, p. 35-36) aponta que:

> A cooperação penal internacional não é um fenômeno recente. A sua manifestação mais remota nos remete ao longínquo tratado de paz, celebrado em 1280 a. C. entre Ramsés II, Faraó do Egito e Hatussilli III, Rei dos Hititas, sendo considerado o mais antigo tratado de extradição da humanidade. É evidente que não possuía as

> características que atualmente apresenta, tanto é assim que previa-se a extradição de criminoso político e não de criminoso comum.

O Tratado de Versalhes, de 1919, estabelecido no período de depressão do pós-1ª Guerra Mundial, foi um marco na tentativa de criação de uma jurisdição penal internacional, com a previsão de Tribunais *Ad hoc* (art. 227, composto por 5 membros indicados pelos EUA Grã-Bretanha, França, Itália e Japão) para o julgamento do ex-Kaiser Guilherme II da Alemanha, denunciado nominalmente pelos aliados por "ofensa suprema contra a moral internacional e a autoridade sagrada dos tratados", que, no entanto, não chegou a ser instituída (CARDOSO, 2012, p. 20).

Tais iniciativas fizeram surgir, juntamente com a conjuntura social posta à época, a necessidade da criação de um organismo internacional de jurisdição penal, que, no entanto, foi dificultada pela valorização da assim chamada soberania nacional, que inviabilizava a possibilidade de existência de um órgão supranacional para julgamento de crimes de guerra.

Como registra Paiva (2008), a ocorrência da 2ª Guerra Mundial e os horrores nela praticados, tornaram definitivo o reconhecimento da necessidade de existência de uma jurisdição penal internacional:

> Entretanto, o verdadeiro marco de reconhecimento de uma jurisdição penal internacional retroage aos eventos chocantes experimentados pela humanidade no curso da Segunda Guerra Mundial, impostos pelos regimes políticos nacional-socialista alemão e fascista italiano. De fato, não resta dúvida de que, concretamente, as definições acerca de uma Jurisdição Penal Internacional forma construídas a partir do contexto geopolítico emanado do final do conflito internacional de 1945. (PAIVA, 2008, p. 65-66).

O pós-Guerra Fria teve como consequência um rearranjo nas forças geopolíticas mundiais. Como explica Cardoso (2012), "nos anos 1990, após o fim da confrontação Leste-Oeste, abriram-se novas perspectivas para as Nações Unidas e o seu Conselho de Segurança (CSNU), que se destravou e passou a atuar com mais intensidade que durante a Guerra Fria". Assim, em reação à "limpeza étnica" ocorrida na Bósnia e ao genocídio em Ruanda, foram estabelecidos, pelo CSNU, dois tribunais penais ad hoc com vistas a processar e julgar indivíduos responsáveis pelas atrocidades. Como destaca o autor, esta foi uma resposta algo improvisada que fez ressurgir uma ideia antiga discutida nas Nações Unidas nos anos 1940: a criação de um tribunal penal internacional de caráter permanente. E prossegue Elio Cardoso (2012, p. 15):

> A ideia sempre esbarrou nas resistências decorrentes da contraposição entre soberania dos Estados e jurisdição penal internacional. Apesar delas, colocou-se em

> marcha o processo que culminou na Conferência da ONU em Roma. O Estatuto do Tribunal Penal Internacional (TPI) foi aprovado, em 1998, por ampla maioria, estabelecendo-se uma instância judicial permanente e competente para julgar indivíduos responsáveis por genocídio, crimes contra a humanidade, crimes de guerra e agressão. O novo órgão internacional teria como parâmetro a primazia dos sistemas judiciais nacionais – somente poderia ser chamado a atuar em casos de patente incapacidade ou falta de disposição dos Estados em instaurar inquéritos ou processos relativos aos crimes em questão. À luz do princípio da complementaridade, as instâncias nacionais teriam prioridade para processar e julgar os crimes sob a sua jurisdição.

Registre-se ainda que, em 17 de julho de 1998, o Estatuto de Roma, na Itália, estabeleceu o TPI. No entanto, por não ser o foco do presente trabalho, abreviamos o conteúdo histórico referente ao Tribunal Internacional, para registrar as palavras do embaixador Marcel Biato, que, em seu prefácio na obra de Cardoso (2012), destaca:

> A adesão do Brasil ao Estatuto de Roma, em 2002, foi uma das primeiras e precoces manifestações da determinação coletiva de assumir esse novo status de potência emergente. Dava-se assim mais um passo na caminhada rumo ao papel mais ativo, confiante e engajado que se espera do Brasil no mundo globalizado do século XXI.

Destaca ainda Marcel Biato que "a incorporação do Brasil ao Tribunal Penal Internacional não se deu sem certa hesitação inicial [...]. É o que sugere o intenso debate sobre como adequar o ordenamento interno brasileiro às complexas inovações trazidas pelo Estatuto de Roma. Essa adesão marcaria, em última análise, o abandono de um casulo onde o país não mais cabia".

Cardoso (2012, p. 70) lembra ainda que "não há dúvidas de que o TPI resulta de uma empreitada multilateral: a ideia de um tribunal permanente, que remonta à fundação das Nações Unidas, frutificou-se em conferência sob os auspícios da Organização". Em junho de 2003, foi adotada a Posição Comum do Conselho da União Europeia, com o objetivo de apoiar o funcionamento efetivo do TPI, e, dessa forma, a instituição nasceu em Roma e está sediada em Haia[44].

3.3 A criação da União Europeia e o caminho até a Convenção de Budapeste

Decorridos alguns anos após o fim da Segunda Guerra Mundial, as nações europeias vencedoras e vencidas, começaram a associar-se para cooperação em algumas áreas. Assim, deu-se o primeiro passo, quando seis países – Bélgica, República Federal da Alemanha, França,

[44] Os documentos relativos ao funcionamento do TPI estão disponíveis em: http://ec.europa.eu/external_relations/human_rights/icc/index_en.htm.

Itália, Luxemburgo e Holanda (Países Baixos) – criaram a Comunidade Europeia do Carvão e do Aço. Este foi também o primeiro passo em todo o processo de integração europeia.

De acordo com a obra "*Europe in 12 lessons*", do *Publications Office of the European Union*, as bases constitutivas da União Europeia foram consagradas nos seguintes tratados (FONTAINE, 2010):

- Tratado de Paris, que instituiu a Comunidade Europeia do Carvão e do Aço (CECA), em 18 de abril de 1951 (seis membros fundadores: Bélgica, República Federal da Alemanha, França, Itália, Luxemburgo e Holanda);

- Tratados de Roma, que instituíram a Comunidade Econômica Europeia (CEE) e a Comunidade Europeia da Energia Atómica (Euratom), em 25 de março de 1957 (os mesmos seis membros fundadores do Tratado de Paris).

Os tratados fundadores foram posteriormente alterados pelos Acto Único Europeu (1986); Tratado da União Europeia (Maastricht, 1992); Tratado de Amesterdã (1997); e Tratado de Nice (2001).

O Tratado da União Europeia, assinado em Maastricht a 7 de fevereiro de 1992, entrou em vigor em 1 de novembro de 1993. A União criada pelo Tratado de Maastricht foi investida de determinadas competências, classificadas em três grandes grupos, habitualmente designados "pilares".

O primeiro "pilar" era constituído pelas Comunidades Europeias e fornecia um quadro no âmbito do qual deveriam ser exercidas pelas instituições comunitárias as competências que eram objeto de transferência de soberania pelos Estados-Membros nos domínios visados pelo Tratado; o segundo "pilar" era constituído pela política externa e de segurança comum, regida pelas disposições do Título V do Tratado da União Europeia; o terceiro "pilar" era constituído pela cooperação nos domínios da justiça e dos assuntos internos, prevista no Título VI do Tratado. As disposições dos títulos V e VI estabeleciam uma cooperação de tipo intergovernamental que recorria a instituições comuns e se encontrava dotada de certos elementos supranacionais, nomeadamente a associação da Comissão Europeia e a consulta do Parlamento Europeu (PARLAMENTO EUROPEU, 2020).

Assim, no âmbito da União Europeia, são estabelecidos laços de cooperação entre os serviços nacionais de polícia, serviço nacionais aduaneiros e autoridades judiciárias nacionais e se efetivam em termos práticos e operacionais com as atividades desempenhadas pela Eurojust, Europol e Rede Judiciária Europeia em Matéria Penal. Dessa forma, o

amadurecimento dessas relações jurídicas foi natural para os trabalhos desenvolvidos no âmbito da União Europeia, que culminaram com o estabelecimento da Convenção do Conselho da Europa sobre o Cibercrime, também conhecida como Convenção de Budapeste (ETS 185), datada de 23 de novembro de 2001 (MORAIS NETO, 2009, p. 119; COUNCIL OF EUROPE, 2001).

3.4 A União Europeia e a Convenção de Budapeste

Conforme lembra Schjolberg (2008, p. 2), a primeira iniciativa internacional sobre crimes informáticos na Europa foi a Conferência do Conselho da Europa sobre aspectos criminológicos do crime econômico em Estrasburgo, em 1976. Várias categorias de crimes por computador foram introduzidas.

O autor destaca ainda que, em 1982, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), em Paris, decidiu instituir um comitê de especialistas para tratar do crime relacionado a computadores e da necessidade de mudanças nos códigos penais. Como resultado das propostas do comitê de especialistas, o Comitê ICCP da OCDE, em 1986, recomendou fortemente: “no que diz respeito aos aspectos transnacionais da atividade criminosa relacionada à informática, foram observadas questões importantes que apontam para a conveniência de cooperação internacional na repressão e controlar tal atividade. E que todos os países membros considerem até que ponto os atos cometidos com conhecimento de causa neste campo devem ser cobertos pela legislação penal nacional. Esses atos podem ser expressos, tanto quanto possível, em termos de funções, em vez de tecnologia” (SCHJOLBERG, 2008, p. 4).

Chawki (2006, p. 152) explica que a emergente preocupação levou os líderes europeus a reunirem-se, no evento denominado a Cimeira de Tampere, em 1999, com o objetivo de estabelecerem definições, incriminações e sanções comuns relacionadas aos “crimes de alta tecnologia”. Nessa linha, uma série de recomendações, no âmbito do Conselho da União Europeia, foram fixadas. Destaca-se a Resolução nº 3, adotada na 23ª Conferência dos Ministros Europeus da Justiça (Londres, 8 e 9 de junho de 2000), que incentivava as partes intervenientes nas negociações a seguirem esforços para viabilizar soluções coerentes. Permitia cooperação para que o maior número possível de Estados participasse do encontro que viria a culminar com a Convenção de Budapeste.

Assim, em 23 de novembro de 2001, em Budapeste, Hungria, Estados Unidos e 29 outros países assinaram o Conselho de Convenção sobre o Cibercrime da Europa, o primeiro instrumento multilateral elaborado para abordar os problemas colocados pela disseminação da atividade criminosa nas redes de computadores. A Convenção do Cibercrime exigirá que as partes estabeleçam leis contra o cibercrime, para garantir que seus encarregados da aplicação da lei tenham as autoridades processuais necessárias para investigar e processar crimes cibernéticos de forma eficaz e para fornecer cooperação internacional a outras partes na luta contra o crime relacionado com a informática (CHAWKI, 2006, p. 29, tradução nossa).

3.5 A Convenção de Budapeste: principais características e o processo de adesão do Brasil

A Convenção de Budapeste do Conselho da Europa sobre crime cibernético marca uma nova era de cooperação internacional nas áreas penal e criminal. Conforme descrito na Convenção, os Estados-Membros da UE, bem como outros signatários, têm procurado fornecer uma regulamentação supranacional a fim de efetivamente combater crimes relacionados com o computador, facilitando a detecção, investigação e ação penal de tais infrações criminais em ambos os níveis, nacional e internacional, e fornecendo mecanismos de rápida e confiável cooperação internacional.

A Convenção é o primeiro tratado internacional sobre crimes cometidos por meio da Internet e de outras redes de computadores, tratando particularmente de violações de direitos autorais, fraude relacionada a computadores, pornografia infantil e violações de segurança de rede. Contém também uma série de procedimentos, tais como a busca de redes de computadores e interceptação. O seu principal objetivo, enunciado no preâmbulo, é o prosseguimento de uma política penal comum que vise à proteção da sociedade contra a cibercriminalidade, em especial por meio da adoção de legislação adequada e do fomento da cooperação internacional (COUNCIL OF EUROPE, 2001).

A Convenção é dividida em quatro segmentos principais (capítulos) e cada um desses segmentos consiste de vários artigos. O primeiro segmento ou seção delineia os aspectos substantivos do direito penal, ou seja, que todos os países ratificantes devem implementar para prevenir os crimes listados. A segunda seção delineia os requisitos processuais e de investigação, e os padrões aos quais os países individuais devem aderir. A terceira seção estabelece diretrizes para a cooperação internacional, que mais comumente envolvem investigações conjuntas das infrações penais listadas na seção um. Finalmente, a quarta seção

contém as disposições relativas à assinatura da Convenção, aplicação territorial das declarações da Convenção, emendas, retiradas, e a importante cláusula de federalismo (CHAWKI, 2006, p. 24-30, tradução nossa).

O Capítulo I, trata de terminologia e contém somente um artigo.

O Capítulo II estabelece medidas a serem tomadas em nível nacional, com a fixação de aspectos relativos ao direito penal material, processual e competência, da seguinte forma: Secção 1 – Direito penal material; secção 2 – Direito Processual; secção 3 – Competência.

O Capítulo III, da Convenção, trata da cooperação internacional e está composto por duas seções: Seção 1 – Princípios gerais; seção 2 – Disposições específicas.

No capítulo IV, são expostas as disposições finais, destacando-se os artigos que tratam da adesão à Convenção, da aplicação territorial e de seus efeitos (COUNCIL OF EUROPE, 2001).

Em relação à adesão do Brasil à Convenção, conforme matéria publicada na revista *online* Digital Security, somente em 2019 o Brasil foi convidado a aderir à Convenção de Budapeste, após iniciativa do Ministério da Justiça e Segurança Pública, e dos esforços do Grupo de Trabalho constituído para esse fim, envolvendo MRE, Polícia Federal, Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI), GSI, Agência Brasileira de Inteligência e MPF. Para o advogado especialista em combate a cibercrimes, Ygor Valerio, CEO do Ltahub, convidado na matéria, "a demanda pela adesão do Brasil vem somar-se ao Marco Civil da Internet, visando suprir a carência por um marco equivalente na seara criminal com parâmetros de persecução penal para tais crimes que, por sua própria natureza, transcendem as fronteiras geográficas" (DIGITAL SECURITY, 2020).

O especialista entende ainda que

> o ingresso do Brasil na Convenção proporcionará às autoridades brasileiras acesso mais ágil a provas eletrônicas sob jurisdição estrangeira, além de mais efetiva cooperação jurídica internacional, indicando também parâmetros para o armazenamento de dados sensíveis, busca e apreensão de dados informáticos, e princípios gerais relativos à extradição. (DIGITAL SECURITY, 2020).

Ferreira da Silva *et al.* (2020) relatam que, em painel da IV Reunião da Rede de Cooperação Penal Internacional da Associação Ibero-Americana de Ministérios Públicos (Aiamp), ocorrido em 22 de julho de 2020, o MPF compartilhou os desafios oriundos da experiência brasileira no combate aos crimes cometidos a partir do uso de tecnologias digitais,

ocasião na qual foi pontuada a importância da adesão dos países à Convenção sobre o Cibercrime (também denominada Convenção de Budapeste).

Os autores relatam ainda que o processo de adesão do Brasil à Convenção de Budapeste já vinha ganhando força, a partir do trabalho de coordenação interinstitucional do Ministério das Relações Exteriores, do Ministério da Justiça e Segurança Pública, da Agência Brasileira de Inteligência e do MPF, que já haviam se manifestado favoravelmente à tomada de providências legais internas, necessárias à adesão do país à Convenção. Em julho de 2019, o Comitê de Ministros do Conselho da Europa formalizou o convite para que o Brasil se tornasse país signatário do respectivo Tratado.

Finalmente, no dia 24 de julho de 2020, o Brasil deu prosseguimento à sua adesão ao instrumento normativo internacional, encaminhando o texto da Convenção de Budapeste ao Congresso Nacional, por meio do Despacho nº 412, de 22 de julho de 2020.

Para os autores, a possibilidade de tornar-se país signatário da Convenção de Budapeste representa um passo importante no desenvolvimento de mecanismos de cooperação entre os Estados, que visam, fundamentalmente, ao combate da criminalidade cibernética para além das fronteiras nacionais (FERREIRA DA SILVA *et al.*, 2020).

4 Metodologia utilizada

Foi adotada uma metodologia exploratória, tendo em vista que, no país, não há ainda uma vasta literatura que trata o tema do cibercrime relativo à adesão do Brasil à Convenção de Budapeste, muito embora estudos sobre a LGP já tenham sido amplamente abordados.

Foi realizada pesquisa bibliográfica e análise dos documentos, publicações especializadas e outros, bem como dados e informações publicados que tratem direta ou indiretamente o tema em análise e os dispositivos legais pertinentes, tendo como base um estudo descritivo e analítico das fontes.

5 Considerações finais

A pesquisa viabilizou uma análise com profundidade no atendimento ao objetivo proposto, qual seja, analisar o impacto, em termos dos crimes cibernéticos, tanto da entrada em vigor da LGPD como em relação à pandemia da COVID-19 e a recente adesão do país à Convenção de Budapeste.

Foi possível, por meio dos estudos realizados, analisar a legislação que conduziu ao atual cenário em que se encontra a regulação no Brasil, tanto sobre o cibercrime quanto, especificamente, à privacidade de dados. Ainda, foi possível constatar que, no enfrentamento ao cibercrime, os conceitos tradicionais de tempo e lugar do crime, jurisdição e competência, e até mesmo soberania de estados, precisam ser olhados sob uma nova perspectiva, levando à conclusão da necessidade cada vez mais premente de integração entre estados e da importância de existir uma instância penal internacional.

O cibercrime é, portanto, ameaça real, cujos quantitativos pudemos analisar e cujos índices estão em ascensão, em especial, devido à pandemia do novo Coronavírus, que fez com as pessoas estivessem cada vez mais conectadas e dependentes da tecnologia.

O Brasil encontra-se entre os cinco países onde ocorrem mais ameaças cibernéticas; em 2019, o país ocupava a 70ª colocação no índice de comprometimento com segurança cibernética da União Internacional de Telecomunicações (ITU), órgão da ONU que empreende esforços na área. Os prejuízos com os ataques cibernéticos, segundo dados da organização, ultrapassaram a marca de US$ 20 bilhões durante o período de 2017 e 2018, em uma medição de 12 meses (SENADO FEDERAL, 2019).

No estudo empreendido, verifica-se que o Brasil hoje já dispõe de instrumentos jurídicos adequados ao enfrentamento de ciberameaças, entretanto, ainda se nota uma necessidade de ações de educação em todos os níveis, tanto dos profissionais de segurança pública quanto dos operadores do direito, até mesmo da sociedade em geral, no sentido de haver um melhor preparo na prevenção ao cibercrime.

A construção de uma cooperação contra o cibercrime na União Europeia, em especial aquela obtida pela Convenção de Budapeste, é algo que se vislumbra imprescindível na conjuntura em que vivemos. Da análise realizada da Convenção de Budapeste, observa-se que os parâmetros de cooperação por ela fixados propiciam aos Estados partes, diversos poderes em relação aos crimes praticados e a seus praticantes.

O Brasil foi convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética em dezembro de 2019; em 24 de julho de 2020, o presidente da República encaminhou o texto da Convenção ao Congresso Nacional. Tal adesão permitirá às autoridades brasileiras acesso mais ágil a provas eletrônicas sob jurisdição estrangeira e, ainda, tornará mais efetiva a cooperação jurídica internacional relacionada à perseguição

penal dos crimes cibernéticos. Por enquanto, até a conclusão do processo, o Brasil participará do grupo como observador.

Referências

ARAS, Vladimir. Crimes de informática: uma nova criminalidade. *Jus Navigandi*, Teresina, ano 5, n. 51, out. 2001. Disponível em: http://jus.com.br/artigos/2250/crimes-de-informatica. Acesso em: 2 out. 2020.

ARAÚJO, Marcelo Barreto de. *Comércio eletrônico*; Marco Civil da Internet; Direito Digital. Rio de Janeiro: Confederação Nacional do Comércio de Bens, Serviço e Turismo, 2017.

BARLOW, John Perry. *Declaração de Independência do Ciberespaço* (1996). Disponível em: http://www.cultura.gov.br/site/2006/10/23/declaracao-de-independencia-do-ciberespaco/. Acesso em: 2 set. 2020.

BRASIL. *Constituição da República Federativa do Brasil*. Brasília: Senado Federal, 1988. Disponível em: https://www2.senado.leg.br/bdsf/item/id/508200. Acesso em: 10 out. 2020.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012: *Dispõe sobre a tipificação criminal de delitos informáticos*; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 26 set. 2020. (BRASIL, 2012a)

BRASIL. *Lei n. 12.735, de 30 de novembro de 2012*: Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 16 out. 2020. (BRASIL, 2012b)

BRASIL. *Lei n. 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 2 out. 2020. (BRASIL, 2014)

BRASIL. *Decreto n. 8.771, de 11 de maio de 2016*. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm. Acesso em: 24 set. 2020.

BRASIL. *Lei n. 13.709, de 14 de agosto de 2018***.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 2 out. 2020. (BRASIL, 2018a)

BRASIL. *Lei n. 12.527, de 18 de novembro de 2011*. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Acesso em: 10 out. 2020. (BRASIL, 2011)

BRASIL. *Lei n. 10.406, de 10 de janeiro de 2002*. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm. Acesso em: 12 out. 2020.

SENADO FEDERAL. *Projeto de Lei nº 181, de 2014*. Estabelece princípios, garantias, direitos e obrigações referentes à proteção de dados pessoais. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/117736. Acesso em: 10 out. 2020.

CANCELIER, Mikhail Vieira de Lorenzi. Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro. *Sequência (Florianópolis)* n. 76 Florianópolis May/Aug. 2017. Disponível em: https://www.scielo.br/scielo.php?script=sci_arttext&pid=S2177-70552017000200213. Acesso em: 7 out. 2020.

CÂMARA DOS DEPUTADOS. *Projeto de Lei PL 4060/2012*: Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em: 12 out. 2020.

CÂMARA DOS DEPUTADOS. *Projeto de Lei PL 5276/2012*: Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378. Acesso em: 12 out. 2020.

CÂMARA DOS DEPUTADOS. Política e Administração Pública. *Consulta pública será base para projeto de lei sobre proteção de dados pessoais*. Agência Câmara de Notícias, 28 jan. 2015. Disponível em: https://www.camara.leg.br/noticias/449278-consulta-publica-sera-base-para-projeto-de-lei-sobre-protecao-de-dados-pessoais/. Acesso em: 18 set. 2020.

CASTELLS, Manuel. *A Era da Informação*: economia, sociedade e cultura. Volume I, a sociedade em rede. 5. ed., São Paulo: Paz e Terra, 2001.

CIO-IDG. Gestão. *Dois terços dos brasileiros em home office não receberam treinamento de cibersegurança*. Da redação, em 12 maio 2020. Disponível em:

https://cio.com.br/gestao/dois-tercos-dos-brasileiros-em-home-office-nao-receberam-treinamento-de-ciberseguranca/. Acesso em: 15 out. 2020.

CORRÊA, Cynthia Harumy Watanabe. *Comunidades Virtuais gerando identidades na sociedade em rede*. Universiabrasil.net, 2004. Disponível em: http://www.uff.br/mestcii/cyntia1.htm+&cd=1&hl=pt-BR&ct=clnk&gl=br. Acesso em: 2 set. 2020.

COUNCIL OF EUROPE. Treaty Office. Details of Treaty No.185 *Convention on Cybercrime*. Explanatory Report. Budapest, 23.XI.2001. Disponível em: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm. Acesso em: 20 set. 2020.

CARDOSO, Elio. *Tribunal Penal Internacional*: conceitos, realidades e implicações para o Brasil. Brasília: FUNAG, 2012, 176 p. Disponível em: http://funag.gov.br/biblioteca/download/986-Tribunal_Penal_Internacional_CONCEITOS.pdf. Acesso em: 20 set. 2020.

CARNEIRO, João Marinonio Enke. *A Guerra Cibernética*: uma proposta de elementos para formulação doutrinária no Exército Brasileiro. Tese (Doutorado) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2012, 203 f.

CHAWKI, Mohamed. WAHAB, Mohamed S. Abdel. *Identity Theft in Cyberspace*: Issues and Solutions. Lex Electronica, vol.11 n.1 (Printemps / Spring 2006). Disponível em: http://www.lex-electronica.org/docs/articles_54.pdf. Acesso em: 11 out. 2020.

CLARKE, Richard A.; KNAKE, Robert K. *Guerra cibernética*: a próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro: Brasport, 2015.

CRESPO, Marcelo Xavier de Freitas. *O cibercrime*. São Paulo: Saraiva, 2011.

CRESPO, Marcelo. *As Leis nº 12.735/2012 e 12.737/2012 e os crimes digitais*: acertos e equívocos legislativos. Canal Ciências Criminais, 24 jun. 2015. Disponível em: https://canalcienciascriminais.com.br/as-leis-no-12-7352012-e-12-7372012-e-os-crimes-digitais-acertos-e-equivocos-legislativos/. Acesso em: 12 set. 2020.

DAVID R. Johnson; David G. Post. *Law and Borders* - the Rise of Law in Cyberspace.Stanford Law Review, Vol. 48, p. 1367, 1996. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=535. Acesso em: 19 set. 2020.

DELGADO, Vladimir Chaves. *Cooperação internacional em matéria penal na convenção sobre o cibercrime*. 2007. 315p. Dissertação. (Mestrado em Direito das Relações Internacionais) - Centro Universitário de Brasília. Brasília, 2007.

FERREIRA, Ivete Senise. A criminalidade informática. *In*: LUCCA, Newton.; SIMÃO FILHO, Adalberto (Coord.). *Direito e internet*. Bauru: Edipro, 2001.

FERNANDES, Vanessa. *A linha do tempo da LGPD no Brasil*. Viceri Insights, Comunidade, 21 set. 2020. Disponível em: https://www.viceri.com.br/insights/linhadotempolgpd. Acesso em: 30 set. 2020.

FERREIRA, Robson. *Monografia apresentada em defesa de tese de pós-graduação lato sensu em Direito Processual Penal*. Centro Universitário das Faculdades Metropolitanas Unidas (FMU), 2000.

FERREIRA DA SILVA, Ricardo Barretto; SERRAGLIO, Lorena Pretti; LIMA, Beatriz Canhoto; ARAGÃO, Isabella de Castro Satiro; CHICARONI, Camilla Lopes. *Instrumentos jurídicos de combate ao cibercrime no Brasil*. LEXLATIN. Opinião. Publicado em 04 ago. 2020. Disponível em: https://br.lexlatin.com/opiniao/instrumentos-juridicos-de-combate-ao-cibercrime-no-brasil. Acesso em: 10 out. 2020.

FONTAINE, Pascal. Publications Office of the European Union. *Europe in 12 lessons*. European Union, Belgium, 2010. Disponível em: https://op.europa.eu/en/publication-detail/-/publication/20691fde-ea17-4c58-bb7a-6aeb23024a84. Acesso em: 2 set. 2020.

GIBSON, William. *Burning Chrome*. Reprint (29 de julho de 2003). Ed. Voyager, 2003.

GIBSON, William. *Neuromancer*. 4. ed. São Paulo: Aleph, 2008.

INFORMATION COMISSIONER'S OFFICE. For organisations/Guide to Data Protection/*Guide to the General Data Protection Regulation* (GDPR)/Principles, UK, 2020. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/. Acesso em: 15 set. 2020.

JOHNSON, David R; POST, David. *Law and Borders* - The rise of law in cyberspace. First Monday, Volume 11, Number 2, 2006. Disponível em: http://www.firstmonday.org/issues/issue1/law/index.html. Acesso em: 10 out. 2020.

KRONE, T., 2005. *High Tech Crime Brief.* Australian Institute of Criminology. Canberra, Australia. ISSN 1832- 3413. 2005.

DIGITAL SECURITY. Redação Digital Security. Webinar *debate adesão do Brasil à Convenção de Budapeste, de combate a crimes cibernéticos*; publicado em 10/09/2020. Disponível em: https://revistadigitalsecurity.com.br/webinar-debate-adesao-do-brasil-a-convencao-de-budapeste-de-combate-a-crimes-ciberneticos/. Acesso em: 10 out. 2020.

LÉVY, Pierre. *Cibercultura*. Tradução Carlos Irineu da Costa. São Paulo: Editora 34, 1999, 264 p. Disponível em: https://mundonativodigital.files.wordpress.com/2016/03/cibercultura-pierre-levy.pdf. Acesso em: 15 out. 2020.

MONTEIRO, Sardinha. A2 /AD Raízes Marítimas. Strategia, Revista da Armada, n. 486, ano XLIII, junho 2014, pág. 4-5. Disponível em: https://www.marinha.pt/Conteudos_Externos/RevistaArmada/_FlipVersion/2014/486/files/assets/basic-html/index.html#1. Acesso em: 15 out. 2020.

MORAIS NETO, Arnaldo Sobrinho de. *Cibercrime e cooperação penal internacional*: um enfoque à luz da Convenção de Budapeste. Dissertação apresentada ao Programa de Pós-Graduação em Ciências Jurídicas da Universidade Federal da Paraíba, na área de concentração em Direito Econômico, nível Mestrado. João Pessoa, 2009.

PAIVA, Bruno Teixeira de. *Ampliação da competência do Tribunal Penal Internacional para o julgamento de crimes ambientais transfronteiriços*. 2008. 112p. Dissertação. (Mestrado em Ciências Jurídicas) - Universidade Federal da Paraíba, João Pessoa, 2008.

PARLAMENTO EUROPEU. Fichas temáticas sobre a União Europeia. Evolução histórica da integração europeia. *Os Tratados de Maastricht e de Amesterdão*. Disponível em: https://www.europarl.europa.eu/factsheets/pt/sheet/3/os-tratados-de-maastricht-e-de-amesterdao#:~:text=O%20Tratado%20de%20Maastricht%20alterou,dos%20assuntos%20internos%20(JAI). Acesso em: 10 out. 2020.

PEDROSO, Juliana. Lei prevê pena leve para crimes cibernéticos como o do hacker de Moro. *Gazeta do Povo*. 27 jul. 2019. Disponível em: https://www.gazetadopovo.com.br/republica/crimes-ciberneticos-moro/. Acesso em: 15 set. 2020.

PIMENTEL, José Eduardo de Souza. Introdução ao Direito Digital. *Revista Jurídica da Escola Superior do Ministério Público de São Paulo*, v. 13, n. 1, (2018), p. 16-39. Disponível em: https://es.mpsp.mp.br/revista_esmp/index.php/RJESMPSP/article/view/352/340340364. Acesso em: 10 out. 2020.

PINHEIRO, Patrícia Peck. *Direito digital*. 6. Ed. São Paulo: Saraiva, 2016.

PINHEIRO, Patrícia Peck. *Direito Digital*. 2 ed. São Paulo: Saraiva, 2007.

PINHEIRO, Patricia Peck; SLEIMAN, Cristina Moraes. *ÂMBITO JURÍDICO*. Direito digital e a questão da privacidade nas empresas. 31 jul. 2008. Disponível em: https://ambitojuridico.com.br/edicoes/revista-55/direito-digital-e-a-questao-da-privacidade-nas-empresas/. Acesso em: 5 out. 2020.

POSEN, Barry R. Command of the Commons: The Military Foundation of U.S. Hegemony. International Security, v. 28, n. 1, summer, 2003, pp. 5–46. Disponível em: https://www.belfercenter.org/sites/default/files/files/publication/posen_summer_2003.pdf .

ROMANO, Rogério Tadeu. JUS.COM.BR. Artigos. *Convenção de Budapeste e cibercrimes*. Publicado em mar 2019. Disponível em: https://jus.com.br/artigos/72969/convencao-de-budapeste-e-cibercrimes. Acesso em: 10 out. 2020.

ROHRMANN, Carlos Alberto. *Curso de direito virtual*. Belo Horizonte: Del Rey, 2005.

SCHJOLBERG, Stein. The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva. December, 2008. Disponível em: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf Acesso em: 6 abr.2009.

SAFERNET BRASIL. *Indicadores da Central Nacional de denúncias de Crimes Cibernéticos*. 2015-2020. Disponível em: https://indicadores.safernet.org.br/. Acesso em: 10 out. 2020.

SCHMIDT, Guilherme. Crimes Cibernéticos. *JUSBRASIL*, publicado em 6 nov. 2014. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos#:~:text=Crimes%20Cibern%C3%A9ticos%20Pr%C3%B3prios%20e%20Impr%C3%B3prio&text=Os%20crimes%20cibern%C3%A9ticos%20impr%C3%B3prios%20seriam,um%20novo%20meio%20de%20execu%C3%A7%C3%A3o. Acesso em: 15 set. 2020.

SENADO FEDERAL. Senado Notícias. Brasil é 2. no mundo em perdas por ataques cibernéticos, aponta audiência. Agência Senado, 05 set. 2019. Disponível em: https://www12.senado.leg.br/noticias/materias/2019/09/05/brasil-e-2o-no-mundo-em-perdas-por-ataques-ciberneticos-aponta-audiencia. Acesso em: 15 out. 2020.

SILVA JÚNIOR, Ronaldo Lemos. *Direito, tecnologia e cultura*. São Paulo: FGV, 2005.

TACIO, Paulo. [Termos hacker] os nomes. *Mundo dos hackers*. 17 jun. 2010. Disponível em: https://www.mundodoshackers.com.br/termos-hacker-os-nomes. Acesso em: 7 out. 2020.

TIEDEMANN, K. Criminalidad mediante computadoras. *Nuevo Foro Penal*, v. 12, n. 30 (1985), p. 481-492, 11. Disponível em: http://publicaciones.eafit.edu.co/index.php/nuevo-foro-penal/article/view/4315. Acesso em: 7 out. 2020.

VIANNA, Túlio Lima. Fundamentos de direito penal informático. Rio de Janeiro: Forense, 2003.

ZEVIAR-GEESE, G. 1997-98. *The State of the Law on Cyberjurisdiction and Cybercrime on the Internet*. California Pacific School of Law. Gonzaga Journal of International Law. Volume 1. 1997-1998.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. *Crimes cibernéticos*: ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012.

CONSIDERAÇÕES FINAIS

Como destacado até aqui, o objetivo geral deste II Seminário foi discutir como a Segurança e a Defesa Cibernéticas do Setor Espacial estão sendo estrategicamente pensadas, planejadas e postas em prática pela FAB, por organizações nacionais e internacionais e empresas que atuam nesse imprescindível setor para a soberania nacional brasileira.

Praticamente em todos os dias de evento, os convidados – e a própria audiência, por meio do Slido – pontuaram que atualmente os programas e indústrias espaciais nacionais vivem uma janela de oportunidade, especialmente pelo contexto engendrado pela segunda corrida espacial em que o mundo se depara – o que alguns chamam de *New Space* –, para adquirir e desenvolver novos negócios e modelos disruptivos de produtos e servidos baseados em ativos espaciais. Todavia, essa oportunidade tem se transformado em constantes desafios em termos de Segurança Cibernética, seja pela concepção e/ou uso de sistemas e programas de código-fonte aberto ou compartilhado, seja pela natureza interdependente dos ativos cibernéticos. Logo, a literatura, os exemplos e os *cases* vistos nacionalmente e nas relações internacionais trazidos, ao longo do II Seminário, mostram que é cada vez mais necessário pensar a componente cibernética não apenas sob os prismas tático e operacional – que lhe são tão característicos –, mas igualmente do estratégico e político.

Além disso, esta segunda edição do Seminário também destacou como a cibernética tem jogado um papel fundamental para compreender as relações entre os Estados, sob o viés estratégico-militar. Não por menos, vários casos ao redor do mundo ilustraram como diversas FA têm lidado com a segurança da informação de suas infraestruturas críticas ilustraram as falas dos convidados, bem como as perguntas da audiência, a exemplo de armas cibernéticas como o *worm* Stuxnet, doutrinas militares como a DMDC brasileira e instituições como a USSF. Neste ponto, a questão da militarização do espaço exterior ganhou amplo relevo, demonstrando como este é um tema atual, necessário e caro às principais forças aéreas – e espaciais – do mundo, inclusive a brasileira.

Como não poderia deixar de ser, o evento buscou apresentar a relação entre os Setores Estratégicos Espacial e Cibernético de forma transversal e interseccional, e não apenas separadamente. Portanto, um dos principais achados deste evento foi o fato de que, neste século XXI, nenhuma força área – e espacial – poderá tratar da segurança de seus ativos

críticos espaciais sem pensar estrategicamente na segurança e na defesa cibernéticas e vice-versa, haja vista que recursos vitais para o funcionamento e desenvolvimento do ciberespaço estão baseados ou passam por ativos aeroespaciais, como satélites e antenas.

Outro tema bastante recorrente nas falas dos convidados e nos trabalhos aprovados foi em relação ao vácuo deixado pelo direito internacional acerca dos ataques cibernéticos contra ativos espaciais, especialmente satelitais. Pelo fato de o Tratado do Espaço ter sido confeccionado em um momento que a projeção global do ciberespaço sequer fora imaginada, as lacunas deixadas pelo Direito Internacional Espacial quanto à Segurança Cibernética atreladas à ausência de um tratado internacional sobre Guerra Cibernética ou operações militares cibernéticas criam uma espécie de corrida "ciberarmamentista" em que atores não-estatais e potências pequenas ganham capacidades assimétricas não vistas em outros ambientes. Portanto, levar em contar esses cenários pode ser algo a ser incorporado nos jogos de guerra e cenários prospectivos tanto na formação e pós-formação do militar brasileiro quanto nos programas de pós-graduação das FAs, a exemplo dos da UNIFA.

Assim como em qualquer evento realizado por uma OM da FAB, como é o caso da UNIFA, seus eventos têm de gerar, entre outras especificidades e pré-requisitos, *insights* e caminhos para o aperfeiçoamento da arte e da ciência da Estratégia voltada para as dimensões espacial e cibernética do Poder Aeroespacial. Nesse diapasão, pontuamos como caminhos sem volta a colaboração e a cooperação interagências e internacional nessa seara tanto do ponto vista tecnológico quanto prospectivo. Trata-se, pois, de duas questões a serem sempre estimuladas acadêmica e institucionalmente, como, inclusive, apregoaram muitos dos convidados em suas falas, a exemplo do Diplomata André João Rypl (MRE), da Dra Cristine Hoepers (CERT.br) e do Gen Bda Jomar Barros de Andrade (CDCiber), para citar alguns. Logo, pesquisar e estudar essas potencialidades nos parecem ser condizentes com as inspirações e aspirações para o desenvolvimento nacional do Brasil, bem como das suas relações exteriores.

Ainda, do ponto de vista do conteúdo, todos os temas inicialmente traçados para este II Seminário foram discutidos por civis e militares de referência teórica e/ou prática nos respectivos assuntos, bem como franqueada a palavra para a audiência, que, como se viu no Gráfico 1, aprovou, em grande medida, o evento. Agora, do ponto de vista da forma, acredita-se que o II Seminário foi uma experiência disruptiva para a UNIFA, pois, devido à imposição contingenciada da pandemia de Covid-19, o formato original do evento foi completamente reformulado para se encaixar na modalidade a distância.

Nesse sentido, para esta segunda versão do Seminário, a organização do evento utilizou, de forma pioneira, entre outros:

- a plataforma Zoom – com o Webex em redundância –, para transmitir um evento ao vivo via YouTube, em diálogo constante com uma equipe externa, no caso a FGV Projetos;
- sistema independente de perguntas da audiência, por meio do Slido;
- panos de fundos (*backdrops*) virtuais adaptados – em consonância com as equipes de *design* de comunicação social – para convidados e equipe;
- criação do canal da UNIFA a partir do já existente CEA-UNIFA, no que o principal desafio que isso constitui, agora, é alcançar 1.000 inscritos, para que, a partir dessa marca, possa-se realizar transmissões ao vivo, sem recorrer a terceiros;
- desenvolvimento de boas práticas virtuais – inspiradas em materiais do COMAER, FGV e Academia da Força Aérea (AFA) – especialmente para padronizar as apresentações dos trabalhos selecionados; e
- criação de uma sala completa de videoconferência, no Prédio do Comando da UNIFA, que, certamente, é um dos maiores legados deste evento.

Aqui vai mais um ponto em que adaptação a esses novos tempos ganhou ares de inovação: os quatro *webinars* que precederam os dois dias de Seminário apresentavam pequenas modificações, a título de experiência. Por exemplo, no primeiro *webinar*, o mediador fazia rodadas de perguntas aos palestrantes; no segundo *webinar*, as perguntas foram feitas em blocos únicos; e, no terceiro, o evento foi projetado para ter apenas um palestrante, no que o tempo dos comentários iniciais tiveram de ser aumentados de dois para 10 minutos e o papel do mediador teve de ser adaptado e ampliado para trazer mais dinamicidade e interatividade com a audiência. Enfim, acreditamos que, diante de tudo isso, o CEA conseguiu organizar um evento que cumpriu com sua função acadêmica, tecnológica e social.

Não apenas a audiência como um todo, mas especialmente aqueles que se debruçam acadêmica e/ou profissionalmente com as dimensões cibernética e/ou espacial do Poder Militar Aeroespacial (PMA), puderam observar, ao longo desses seis dias de debates, que há vários desafios a serem superados e levados em conta na condução das atividades militares brasileiras, incluindo os mais diversos aspectos e perspectivas, como doutrinário, econômico, político, jurídico e acadêmico. Em relação, por exemplo, ao nível de atuação – político,

estratégico, operacional e tático –, os debates apontaram para a solidificação da ideia de que Defesa Nacional e Desenvolvimento Nacional devem andar *pari passu*, de modo que a Tríplice Hélice efetivamente rode também nos assuntos afetos à defesa da Nação brasileira.

Agência Força Aérea / © Sgt Johnson

APÊNDICE A – EDITAL PARA SUBMISSÃO DE TRABALHOS CIENTÍFICOS

1 INFORMAÇÕES GERAIS

1.1 As instruções aqui contidas se referem aos trabalhos científicos (artigos) que serão inscritos, analisados pela Comissão Científica do evento e, caso selecionados, apresentados e publicados no **II SEMINÁRIO DE SEGURANÇA E DEFESA CIBERNÉTICA: Desafios da Defesa Cibernética na Projeção Espacial Brasileira**, organizado pela Universidade da Força Aérea (UNIFA). Podem participar da seleção trabalhos de autoria de discentes e docentes de cursos de pós-graduação e pesquisadores ligados a outras instituições ou autônomos.

1.1.1 **Eixo Temático 1: Convergência estratégica entre os setores cibernético e espacial**: A Estratégia Nacional de Defesa (END) brasileira, não à toa, elegeu os Setores Cibernético e Espacial como Estratégicos para a Defesa Nacional: em seus respectivos domínios, ambos requerem alto grau de desenvolvimento tecnológico e aperfeiçoamento militar. As tecnologias de informação e comunicação (TIC) jogam papel fundamental nos assuntos de Defesa Nacional e Segurança Internacional relacionadas ao espaço exterior. Assim, o objetivo aqui é levantar debates sobre áreas de convergência estratégica entre esses dois Setores. Subtemas:

- O "novo" Direito internacional face aos desafios da segurança cibernética no espaço cósmico
- A recente legislação brasileira que trata de aspectos relativos à segurança cibernética
- Os desafios da Tecnologia da Informação no tratamento e resposta aos incidentes de segurança da Informação

1.1.2 **Eixo Temático 2: A dimensão da cibernética no Poder Aeroespacial perspectivas para a FAB:** A defesa contra ataques cibernéticos e a salvaguarda digital de dados sensíveis são algumas das facetas que envolvem a proteção de infraestruturas críticas, sistemas de comando e controle e satélites a serviço da Projeção Espacial Brasileira. É nesse sentido que o presente debate busca desvelar os principais desafios cibernéticos que envolvem a segurança da atividade espacial. Subtemas:

- O setor aeroespacial brasileiro
- A indústria de Defesa no setor aeroespacial brasileiro

1.2 Ao inscrever seu trabalho científico, o proponente estará automaticamente autorizando a UNIFA a utilizar a obra de sua autoria, em publicação impressa, digital, internet, em seus veículos institucionais, documentos editados, ou qualquer outra mídia.

1.3 Os artigos deverão ser inéditos em relação a outros eventos (simpósios, congressos ou *webinars*) ou publicações técnicas ou científicas, nacionais e internacionais, e representar uma contribuição real ao desenvolvimento dos temas aqui descritos, nos eixos do Seminário, levando-se em conta os aspectos a seguir.

1.3.1 Categorias de artigos aceitos para publicação:

Os artigos submetidos não podem conter plágio. Qualquer citação ou trecho de outros autores, devem ser referenciadas de acordo com as normas da ABNT, em respeito à ética, bem como para evitar problemas judiciais. Os artigos submetidos destinam-se a estimular a discussão e introduzir o debate sobre aspectos relevantes e inovadores, e devem ser sustentados por padrões científicos e apresentar relevância quanto aos temas abordados. Poderão ser submetidos artigos de todas as áreas científicas – Ciências Humanas, Ciências Exatas e da Terra, Ciências da Saúde etc. –, desde que relacionadas ao tema do evento. Os artigos poderão ser dos seguintes tipos:

a) Artigos originais: como o próprio nome indica, trata-se de artigos que resultam depesquisas inéditas e que possuem **conteúdo inédito**. Os mais reconhecidos são resultado de pesquisa experimental, e podem incluir novos experimentos e descobertas para o conhecimento humano. São bastante utilizados para pesquisas na área de saúde.

b) Artigos de revisão: são resultados de pesquisa recente e original do(s) autor(es). Trazem a proposta de rever, analisar e discutir conteúdos já publicados, podendo tais conteúdos serem outros artigos científicos já escritos. Adotam o método de revisão. Dentre os métodos, incluem-se: revisão integrativa (RI), revisão tradicional, revisão narrativa, revisão sistemática, metanálise, metassíntese, *scoping review*, *mapping review*, entre outros.

1.3.2 Quanto aos critérios de seleção, a priorização adotada resultará da busca pelo artigo que:

a) Mostre o avanço de conhecimento científico;
b) Contribua para o avanço de pesquisas técnico-científicas na área abordada;
c) Apresente qualidade científica, com método e análise apropriada para responder à questão de pesquisa;
d) Apresente rigor, originalidade e criatividade na apresentação dos resultados;

e) Apresente relevância e interesse global; e

f) Siga as boas práticas recomendáveis para reportar os diferentes tipos de estudos técnico-científicos, bem como a ética na pesquisa.

1.4 Não serão aceitos traduções e/ou trabalhos que se constituam em promoção comercial de determinada marca, produto ou empresa.

1.5 Cada trabalho científico poderá ser submetido com no máximo 03 (três) autores. Dentre esses 03 (três) autores, 01 (um) deverá inscrever-se como autor principal (1º autor). O autor principal (1º autor) poderá submeter no máximo 03 (três) trabalhos para avaliação.

1.6 Será excluído o proponente que não cumprir o previsto em qualquer das etapas deste Edital, independente do fato motivador. Não havendo 2ª chamada para qualquer uma das etapas deste Edital.

1.7. O resultado da avaliação dos trabalhos, em cada uma das etapas do processo de avaliação, será expresso por meio dos critérios **SELECIONADO** ou **NÃO SELECIONADO**.

1.8 A publicação dos trabalhos SELECIONADOS estará disponível no *site* do evento, que conterá, na íntegra, todos os trabalhos selecionados.

1.9 Os arquivos da documentação enviados pelos proponentes NÃO SELECIONADOS serão eliminados pela Comissão Científica Avaliadora, após a homologação do resultado deste Edital.

1.10 Características do e-mail de envio do Resumo:

1.10.1 No assunto do e-mail deverá constar: "[RESUMO]"

1.10.2 Qualquer dúvida em relação ao envio do resumo (Ex.: inclusão ou exclusão de autores, alteração no título do resumo), entrar em contato por meio do e-mail: seminario.unifa@fab.mil.br.

2 SUBMISSÃO DE TRABALHOS

2.1 A submissão de trabalhos será realizada mediante o preenchimento da ficha de inscrição de Resumo, disponível no *site* da UNIFA, e seu envio deve ser realizado até as 23h59min do dia **05 de outubro de 2020**, horário de Brasília, para o *e-mail* informado no item 6 deste Edital.

2.2 São documentos necessários para inscrição de Resumo:

a) Ficha de Inscrição: o modelo se encontra disponível no *site* do evento, deverá ser preenchida e encaminhada para o *e-mail* do evento: seminario.unifa@fab.mil.br (conforme item 6), sendo mandatório o preenchimento de todos os itens da ficha.

b) Currículo Lattes: deve ser preenchido diretamente no site do CNPq, no link http://lattes.cnpq.br. Não serão aceitos currículos em outros formatos. O link para acesso ao currículo Lattes do candidato deverá ser informado no campo específico existente na Ficha de Inscrição de Resumo. Caso o proponente não disponha de Currículo Lattes, deverá indicar seu endereço de ORCID.

c) Resumo: a ser elaborado segundo as características abaixo (item 3.2).

2.3 Todos os documentos especificados no item 2.2, nas alíneas de “a”, “b” e “c”, são obrigatórios e de responsabilidade do próprio proponente, devendo ser enviados à Comissão Científica Avaliadora do evento, pelo e-mail seminario.unifa@fab.mil.br, no prazo definido neste Edital. A não apresentação dos documentos exigidos acarretará a não homologação da inscrição e consequente exclusão do proponente.

2.4 A Comissão Científica Avaliadora do evento enviará uma mensagem padronizada, a cada candidato, acusando o recebimento da mensagem de inscrição, num prazo de até 72 (setenta e duas) horas, para posterior conferência e possível homologação.

2.4.5 O proponente que não receber a confirmação de recebimento de sua mensagem de inscrição, no prazo de 72 (setenta e duas) horas, deverá entrar em contato com a Comissão Científica Avaliadora do evento no prazo de um dia útil para receber as instruções de comprovação do envio.

3 APRESENTAÇÃO DO RESUMO

3.1 Somente serão aceitos resumos que forem enviados no formato pdf. Todos os demais formatos de arquivos, inclusive compactados, não serão aceitos.

3.2 Características do Resumo:

3.2.1 Deverá ser redigido em até 500 palavras, no idioma português ou inglês, em que o texto for submetido, em espaçamento um entre as linhas e com a fonte Times New Roman tamanho 12 (sem espaço entre parágrafos, em texto corrido). Não deverá conter: citações de autores, local e ano da coleta de dados e siglas.

3.2.2 O Resumo deverá conter: Objetivo, Metodologia utilizada, Resultados (quando for o caso) e Conclusões/Recomendações/Considerações finais. O Objetivo deve ser claro, conciso e descrito no tempo verbal infinitivo. A Metodologia utilizada deve expressar o tipo de estudo, amostra, variáveis, instrumentos utilizados na pesquisa e o tipo de análise. Os Resultados, quando aplicáveis, devem ser concisos, informativos e apresentar os principais resultados

descritos e quantificados, inclusive, se houver pesquisa de campo, informar as características dos participantes e análise final dos dados. As Conclusões/Recomendações/Considerações finais devem responder estritamente ao objetivo, expressar as considerações sobre as implicações teóricas ou práticas do estudo e as suas principais contribuições para o avanço do conhecimento científico e/ou para conhecimento/desenvolvimento do tema tratado.

3.3 Nenhuma referência aos nomes dos autores, suas entidades ou endereços poderá ser feita em nenhuma página do Resumo.

4 AVALIAÇÃO, SELEÇÃO E PRAZOS

4.1 A relação dos resumos SELECIONADOS será disponibilizada no *site* do evento **até 20 de outubro de 2020**.

4.2 Os autores dos trabalhos selecionados deverão enviar para o *e-mail*: **seminario.unifa@fab.mil.br**, até as 23h59min, horário de Brasília, do dia **04 de novembro de 2020**, a versão completa de seus trabalhos, considerando que os(as) autores(as) poderão ajustar seus resumos inicialmente apresentados, devido às observações dos(as) professores(as) avaliadores(as).

4.3 Somente serão incluídos, na programação oficial e programados para apresentação, os trabalhos completos que atenderem aos critérios constantes no presente Edital.

4.4 Autores que não atenderem aos critérios acima não terão seus trabalhos incluídos no programa oficial e nem programados para apresentação.

4.5 Autores que tiverem seus trabalhos selecionados comprometem-se a elaborar e encaminhar a versão completa (conforme critérios definidos no item 5), bem como sua apresentação para o e-mail seminario.unifa@fab.mil.br.

4.6 Os trabalhos que não forem encaminhados em sua versão completa (conforme características definidas no item 5), e com sua respectiva apresentação, não serão incluídos no registro impresso/digital do evento, que poderá ser disponibilizado em formato de anais.

5 INSTRUÇÕES PARA A VERSÃO COMPLETA DOS TRABALHOS E SUA RESPECTIVA APRESENTAÇÃO

5.1 O trabalho em sua versão completa deverá conter:

5.1.1. TÍTULO do trabalho (o mesmo informado na ficha de inscrição): máximo de 12 palavras, em negrito, centralizado.

5.1.2. AUTOR(ES): no caso de 02 (dois), ou 03 (três) autores, posicionar o autor principal primeiro, alinhado à direita, espaço interlinear 1,0. Na referência do tipo “nota de rodapé”, correspondente a cada autor, indicar: nome, formação, instituição e e-mail de contato; experiência/títulos principais do autor e e-mail. Máximo de 03 (três) linhas por autor.

5.1.3. INTRODUÇÃO: Deve ser breve, definir claramente o problema estudado, justificando sua importância e as lacunas do conhecimento. As referências devem ser o mais atualizadas possível, em especial aquelas dos últimos três anos e cuja abrangência seja nacional e internacional. Descrever as hipóteses do estudo, quando aplicável. O objetivo deverá constar desta seção, ao final dela. O objetivo deve ser idêntico no resumo e ao final da introdução. As siglas deverão ser descritas por extenso na primeira vez em que aparecerem no texto e acompanhadas de sua abreviatura.

5.1.4. DETALHAMENTO ou DESENVOLVIMENTO DA ANÁLISE (com subtítulos associados ao detalhamento do tema eleito). Consiste no desenvolvimento em si do trabalho, com os respectivos subtítulos necessários para seu detalhamento. Esta seção não tem título definido e fica a cargo do(s) autor(es) sua denominação, bem como dos subtítulos.

5.1.5. METODOLOGIA UTILIZADA: descrição do tipo de metodologia adotada no trabalho. Se houver pesquisa de campo, deverão ser abordados: tipo ou delineamento do estudo; Local ou situação em que ocorreu a coleta de dados; Período; População; Critérios de seleção; Definição da amostra, se for o caso, ou Participantes; Variáveis do estudo; Instrumentos utilizados para a coleta das informações; Coleta de dados; Tratamento e Análise dos dados.

5.1.6. RESULTADOS OBTIDOS OU ESPERADOS (não obrigatório): Quando se aplicar ao trabalho, deve descrever os resultados obtidos, dar ênfase aos aspectos considerados relevantes do estudo, discutir as concordâncias e as divergências com outras pesquisas científicas atualizadas, publicadas em periódicos nacionais e internacionais.

5.1.7. CONCLUSÕES/RECOMENDAÇÕES/CONSIDERAÇÕES FINAIS: Responder aos objetivos do estudo, de forma clara, direta e objetiva, sem a citação de referências.

5.1.6. REFERÊNCIAS. Apresentar exclusivamente as fontes citadas na obra. Aceitamse notas de rodapé, desde que não muito extensas, limitadas a 04 (quatro) linhas cada. Seguir estritamente as normas da ABNT.

5.1.7 Regras de Formatação: Os Artigos deverão conter até 10.000 (dez mil) palavras, sem considerar as referências. O texto deverá atender às seguintes instruções:

- Arquivo no formato .doc ou .docx (Microsoft Word); e pdf.

- Tamanho A4 (21 cm x 29,7 cm ou 8,27” x 11,7”);
- Margens: superior 3cm, inferior 2cm, esquerda 3cm e direita 2cm;
- Fonte: Times New Roman tamanho 12;
- Para destacar termos no texto, utilizar itálico. Não são permitidas no texto: palavras em negrito, sublinhado, caixa alta ou marcadores do Microsoft Word.
- Espaçamento entre linhas: 1,5 cm
- Notas de rodapé e referências: padrão ABNT

5.2 Apresentação do trabalho

Devido à especificidade da modalidade do evento (*online*), as apresentações dos trabalhos SELECIONADOS deverão ser:

a) gravadas em vídeo de 08 (oito) a 10 (dez) minutos de duração, pelo(s) próprio(s) autor(es), conforme roteiro disponível no *site* do evento; e
b) disponibilizadas em *link* do YouTube.

6 DISPOSIÇÕES GERAIS

6.1 Toda correspondência relativa ao conteúdo deste Edital deverá ser encaminhada para: seminario.unifa@fab.mil.br.

6.2 Endereço oficial do evento: http://www2.fab.mil.br/unifa/index.php/seminario.

6.3 A Comissão Científica Avaliadora do evento reserva-se o direito de resolver os casos omissos e as situações não previstas neste Edital de Chamadas.

Rio de Janeiro, 8 de setembro de 2020.

Comissão Científica Avaliadora

II Seminário de Segurança e Defesa Cibernética

APÊNDICE B – FICHA DE INSCRIÇÃO DE RESUMO

ESCREVA AQUI O TÍTULO DO TRABALHO (O MESMO ASSINALADO NO RESUMO SUBMETIDO)

1 Características do Resumo:

1.1 Texto do resumo

O Resumo do seu trabalho, a ser anexado no e-mail, juntamente com esta ficha de inscrição e, portanto, não deve conter nenhuma identificação dos autores ou quaisquer referências que possam identificá-los. Os nomes dos autores, sua qualificação e endereços deverão ser colocados **apenas na ficha de inscrição.**

O seu Resumo deverá ser redigido em parágrafos, totalizando até 500 palavras, no idioma português ou inglês em que o texto for submetido, em espaçamento um entre as linhas e com a fonte Times New Roman tamanho 12 (sem espaço entre parágrafos, em texto corrido). Não deverá conter: citações de autores, local e ano da coleta de dados e siglas.

O Resumo deverá conter: Objetivo, Metodologia utilizada, Resultados (quando for o caso) e Conclusões/Recomendações/Considerações finais. O Objetivo deve ser claro, conciso e descrito no tempo verbal infinitivo. A Metodologia utilizada deve expressar o tipo de estudo, amostra, variáveis, instrumentos utilizados na pesquisa e o tipo de análise. Os Resultados, quando aplicáveis, devem ser concisos, informativos
e apresentar os principais resultados descritos e quantificados, inclusive, se houver pesquisa de campo, informar as características dos participantes e análise final dos dados. As Conclusões/ Recomendações/Considerações finais devem responder estritamente ao objetivo, expressar as considerações sobre as implicações teóricas ou práticas do estudo e as suas principais contribuições para o avanço do conhecimento científico e/ou para conhecimento/desenvolvimento do tema tratado.

1.2 Palavras-chave:

No mesmo arquivo do Resumo, deverão constar, a seguir ao texto, 03 palavras-chave.

2. Eixo Temático e subtema:

Escolha o Eixo Temático no qual seu trabalho se encaixa

( ) EIXO 1: CONVERGÊNCIA ESTRATÉGICA ENTRE OS SETORES CIBERNÉTICO E ESPACIAL

Subtemas:
( ) O "novo" Direito internacional face aos desafios da segurança cibernética no espaço cósmico;

( ) A recente legislação brasileira que trata de aspectos relativos à segurança cibernética;

( ) Os desafios da Tecnologia da Informação no tratamento e resposta aos incidentes de segurança da 34Informação.

( ) EIXO 2: A DIMENSÃO DA CIBERNÉTICA NO PODER AEROESPACIAL - PERSPECTIVAS 37**PARA A FAB** 38**Subtemas:**
( ) O setor aeroespacial brasileiro;

( ) A indústria de Defesa no setor aeroespacial brasileiro.

3. *Link* do Currículo Lattes ou ORCID:

APÊNDICE C – FORMULÁRIO DE AVALIAÇÃO DO ARTIGO COMPLETO

CÓDIGO DE INSCRIÇÃO		CÓDIGO DO AVALIADOR	

ITEM DO EDITAL	ITENS A SEREM AVALIADOS	SIM	NÃO
5.1.1	O título do trabalho está em acordo com o Edital? (máximo de 12 palavras, em negrito, centralizado)		
5.1.2	O(s) autor(es) está(ão) devidamente identificados, inclusive com os dados solicitados no Edital, bem como a formatação de seus nomes está correta no texto?		
5.1.3	O trabalho dispõe de Introdução, que está em acordo com o item 5.1.3 do Edital?		
5.1.4	O detalhamento ou desenvolvimento da análise foi conduzido adequadamente?		
5.1.5	A metodologia utilizada no trabalho foi adequadamente definida?		
5.1.6 RESULTADOS	O trabalho apresentou resultados obtidos ou esperados? (item opcional)		
5.17 CONCLUSÕES	As Conclusões/Recomendações/Considerações finais respondem aos objetivos do estudo, de forma clara, direta e objetiva, sem a citação de referências?		
5.1.6 REFERÊNCIAS	As referências estão em acordo com o previsto no Edital e, ainda, em acordo com as regras da ABNT?		
5.1.7 Regras de Formatação	As Regras de Formatação estão de acordo com o Edital?		
5.2	Para a apresentação dos trabalhos foi disponibilizada aos autores as seguintes possibilidades: gravar um vídeo e/ou enviar uma apresentação em *slides*. Os *links* e/ou a apresentação estão em anexo (ou constam no corpo) do e-mail que encaminha o presente formulário.		
PARECER: ( ) Recomendações/sugestões ( ) Sem recomendações/sugestões			

Recomendações/sugestões:

_____

_____

_____

_____

_____

_____

_____

APÊNDICE D – ORIENTAÇÕES PARA APRESENTAÇÃO DOS TRABALHOS CIENTÍFICOS

As instruções aqui contidas se referem aos vídeos de apresentação dos trabalhos científicos (artigos) selecionados pela Comissão Científica do **II SEMINÁRIO DE SEGURANÇA E DEFESA CIBERNÉTICA: Desafios da Defesa Cibernética na Projeção Espacial Brasileira**, organizado pela Universidade da Força Aérea (UNIFA).

Tendo em vista as novas tecnologias e a transformação que o ambiente acadêmico vem vivenciando, além de ser uma tendência no nosso dia a dia, tornou-se usual que o pesquisador se depare com uma etapa de elaboração de um vídeo de apresentação profissional e/ou acadêmica. Em situações como esta, tenha em mente que você está sendo observado e que as outras pessoas vão analisar sua imagem e também o conteúdo da sua apresentação.

Neste sentido, algumas recomendações podem apoiar suas atividades na construção desta etapa. Lembre-se que se trata de mais uma oportunidade de apresentar sua pesquisa e divulgar seu trabalho. Assim, as recomendações a seguir visam contribuir para que sua apresentação seja bem-sucedida.

Realizar uma boa apresentação exige preparação, e o momento da criação é a fase mais delicada de todo esse processo; é quando você precisa refletir acerca do conteúdo que irá expor e os objetivos pretendidos. Seu bom desempenho diante da plateia depende da preparação. Além da criatividade, você poderá valer-se de métodos simples para cumprir esta etapa.

Lembre-se que, a partir de um bom roteiro, é possível criar uma comunicação que faça sentido!

Conforme dispõe o EDITAL PARA SUBMISSÃO DE TRABALHOS CIENTÍFICOS, em seu item 5.2, que trata da apresentação do trabalho,

"Devido à especificidade da modalidade do evento (*online*), as apresentações dos trabalhos SELECIONADOS deverão ser:

- *gravadas em vídeo de 08 (oito) a 10 (dez) minutos de duração, pelo(s) próprio(s) autor(es), conforme roteiro disponível no site do evento; e*
- *disponibilizadas em link do YouTube."*

1 QUANTO AO ROTEIRO DA APRESENTAÇÃO

a) título do trabalho;
b) nome completo do(s) autor(es) e respectivas filiações profissionais e/ou acadêmicas;
c) objetivos;
d) metodologia;
e) desenvolvimento;
f) resultados (opcional)
f) conclusões/recomendações/considerações finais; e
g) referências.

2 QUANTO AO CONTEÚDO DA APRESENTAÇÃO

2.1 Poderá ser realizada, adicionalmente, uma apresentação em slides, que é também um meio facultativo à apresentação. Utilizar como base o modelo de apresentação disponível no *site*, que deverá conter no mínimo 8 (oito) slides.

2.1.1 Fonte: Verdana na cor preta; se necessitar realçar algum termo, utilizar negrito, e para palavras de outra língua, o itálico; tamanho para os títulos 26 e para o texto 16.

2.1.2 No primeiro slide, devem aparecer o título do trabalho e o nome completo do(s) autor(es), com as respectivas filiações profissionais e/ou acadêmicas; posicionar o autor principal primeiro, alinhado à esquerda, com espaço interlinear 1,0.

2.1.2 O segundo slide, deve conter o Sumário.

2.1.3 O terceiro slide, deve apresentar o(s) objetivo(s) do trabalho, que deverá definir claramente o problema estudado, justificando sua importância e as lacunas do conhecimento a serem preenchidas.

2.1.4 Em seguida, o próximo slide deverá descrever a metodologia adotada no trabalho. Se houver pesquisa de campo, deverão ser abordados: tipo ou delineamento do estudo; local ou situação em que ocorreu a coleta de dados; período; população; critérios de seleção; definição da amostra, se for o caso, ou participantes; variáveis do estudo; instrumentos utilizados para a coleta das informações; coleta de dados; tratamento e análise dos dados.

2.1.4 O quinto slide deverá conter o detalhamento ou desenvolvimento da análise (com subtítulos associados ao detalhamento do tema eleito).

2.1.6 O slide de resultados obtidos ou esperados (opcional) deverá descrever os resultados obtidos, dar ênfase aos aspectos considerados relevantes do estudo, discutir as concordâncias e divergências com outras pesquisas científicas atualizadas, publicadas em periódicos ou livros nacionais e internacionais.

2.1.7 O slide de conclusões/recomendações/considerações finais responderá aos objetivos do estudo, de forma clara, direta e objetiva.

2.1.8 O último slide, das referências, deverá apresentar exclusivamente as principais fontes citadas na obra, limitadas a 04 (quatro).

3 QUANTO AO VÍDEO

3.1 O(s) autor(es), para atingir uma comunicação efetiva, deve(m) atentar para a boa coordenação entre respiração e fala; consciência do efeito das pausas para a melhor compreensão do ouvinte; qualidade vocal estável e agradável; articulação precisa dos sons; correto uso das ênfases; ritmo e velocidade variáveis e adequados ao discurso e ao ouvinte, e evitar maneirismos (né, tá, ok, etc.) e cacoetes.

3.2 Se não tiver um microfone portátil para capturar áudio (*headset*), lembrar sempre da boa acústica no ambiente interno.

3.3 Para a gravação do vídeo, a câmera utilizada pode ser a integrada no próprio notebook/desktop, celular ou *tablet*.

3.4 Certifique-se de que a câmera esteja na posição horizontal, evitando que a imagem fique com faixas pretas nas laterais.

3.5 Quanto ao enquadramento, evite olhar para a tela e sim para a lente da câmera, gerando mais conexão com o público; o enquadramento correto é manter a câmera com a lente à altura dos olhos.

3.6 Cômodos internos, caso estejam ao fundo do vídeo (*background*), necessitam de prévia organização dos elementos que aparecerão no vídeo.

3.7 Evitar lugares onde haja ruídos da rua, carros, pessoas conversando, música e ecos.

3.8 Não fique posicionado contra a luz e procure um ambiente bem iluminado.

3.9 Quanto à vestimenta, mesmo estando em casa, opte por usar as roupas que você usaria em um evento presencial; adeque sua vestimenta ao estilo da palestra e público.

3.10 Quanto às expressões corporais, evite gesticulações exageradas.

3.11 Em relação ao vídeo, sugere-se que, caso o tamanho não exceda o limite de capacidade do seu e-mail, poderá ser encaminhado diretamente para o e-mail: seminario.unifa@fab.mil.br.

Comissão Científica Avaliadora

II Seminário de Segurança e Defesa Cibernética

Referências

BRASIL. Comando da Aeronáutica. Diretoria de Ensino. Academia da Força Aérea. Ambientação à audiência. Pirassununga: AFA, [20--?].

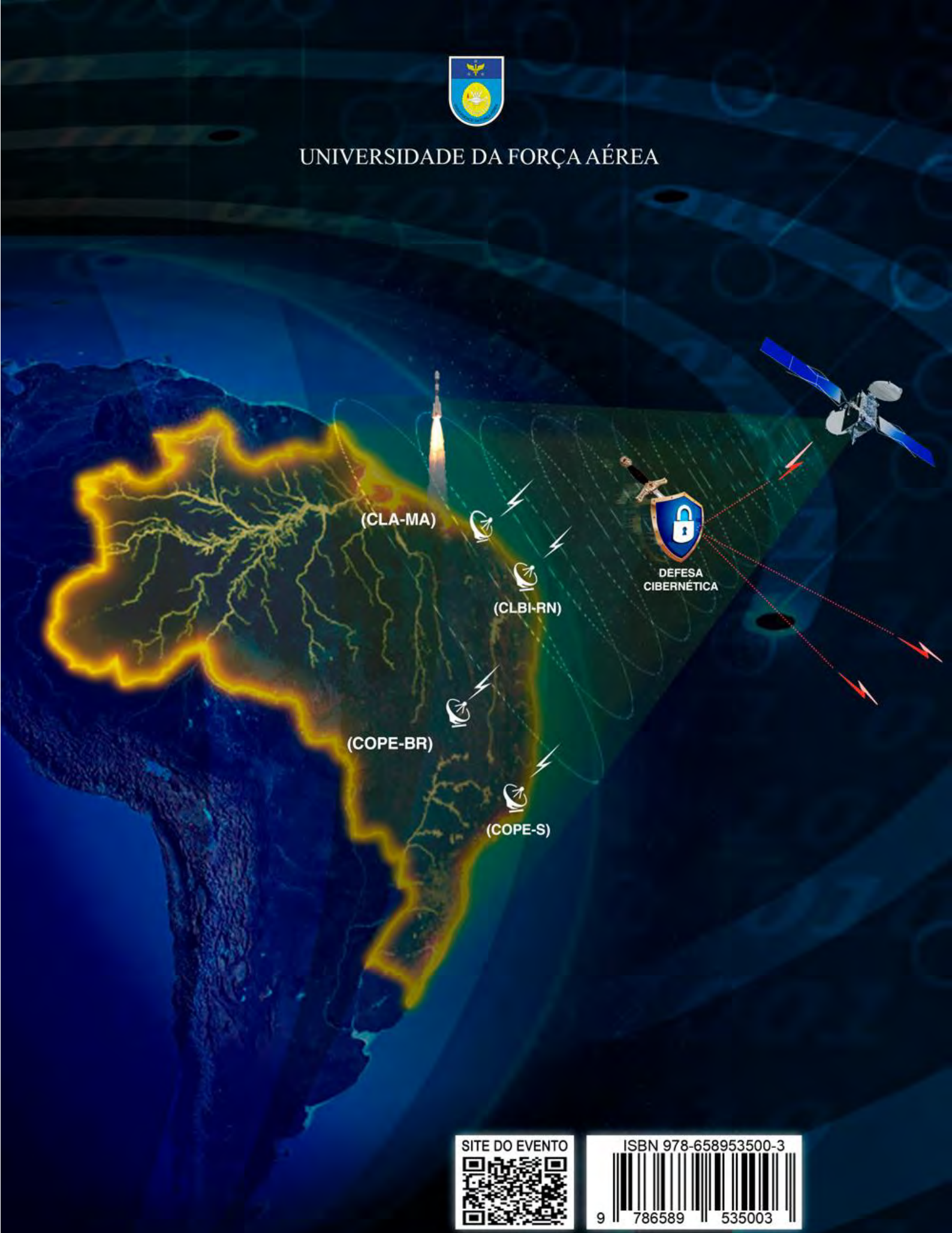
BRASIL. Comando da Aeronáutica. Diretoria de Ensino. UNIFA. Comunicação oral e escrita. CEAD, 2020.

BRASIL. Comando da Aeronáutica. Diretoria de Ensino. UNIFA. Comunicação: técnicas e recursos da exposição oral. CEAD, 2020.

FGV. **Webinar**: Guia de boas práticas. Rio de Janeiro: DICOM, [201-].

ÍNDICE REMISSIVO

UNIVERSIDADE DA FORÇA AÉREA



SITE DO EVENTO

ISBN 978-658953500-3

FGV

REDE CTIDC