EXERCÍCIO GUARDIÃO CIBERNÉTICO 5.0

CENÁRIO FICTÍCIO DO EXERCÍCIO

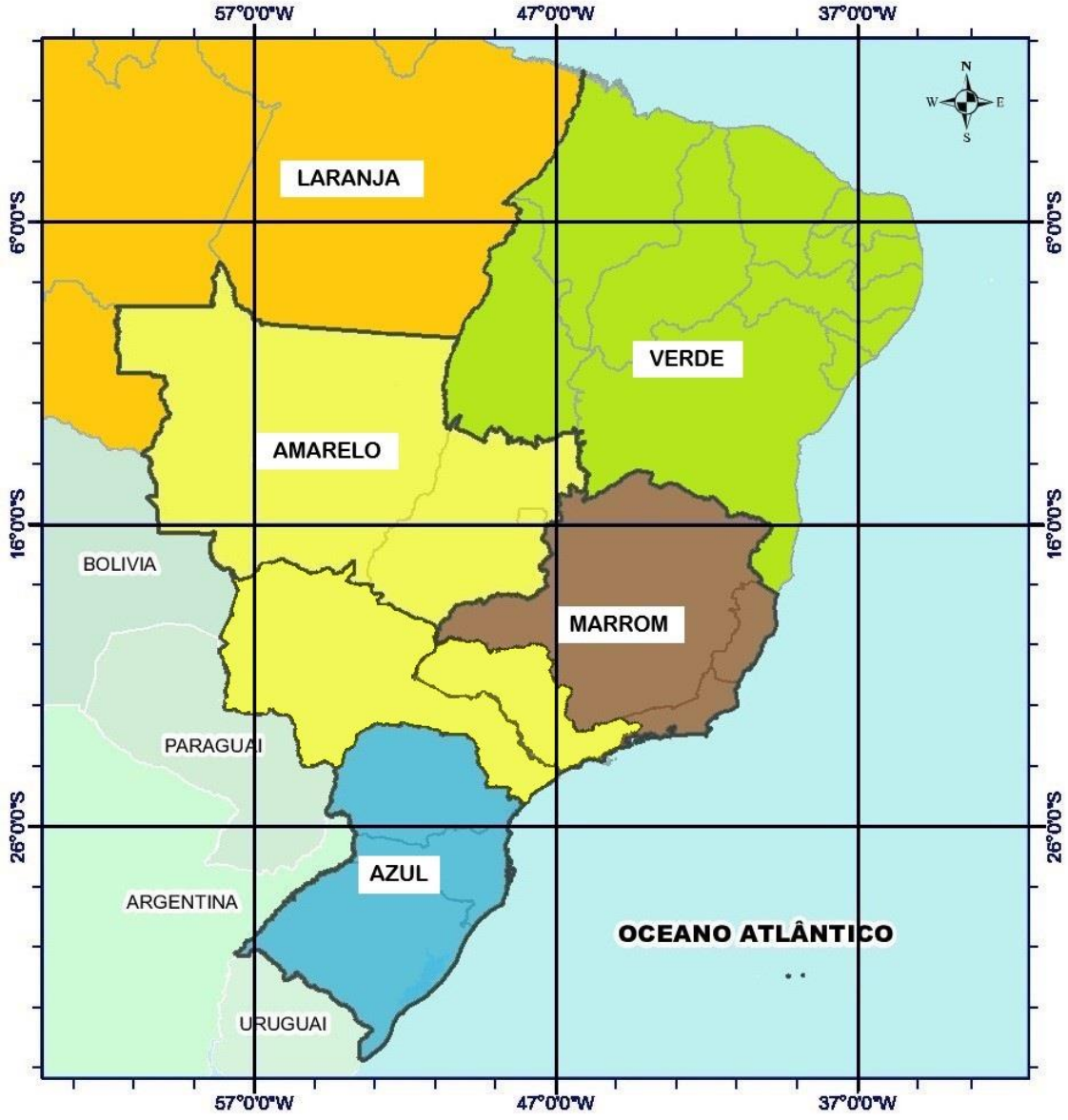
BASEADO NA CONJUTURA DO ADESTRAMENTO CONJUNTO MERIDIANO (EXERCÍCIO REALIZADO PELO MINISTÉRIO DA DEFESA)

AMBIENTAÇÃO

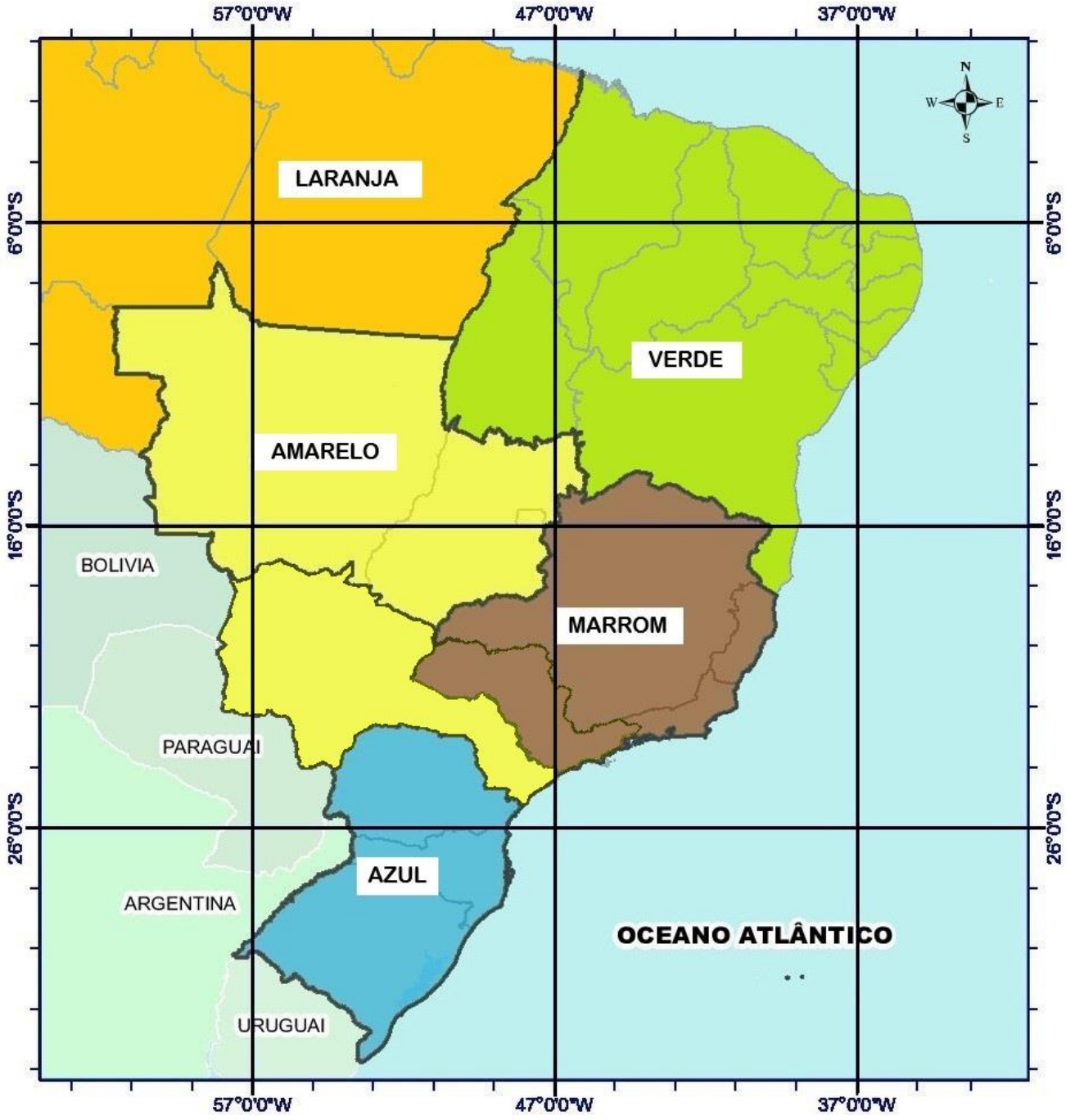
1 CARACTERIZAÇÃO GEOPOLÍTICA REGIONAL

O subcontinente MERIDIANO corresponde à porção do Continente Americano localizada abaixo do paralelo 10º N (excetuando-se o Panamá).

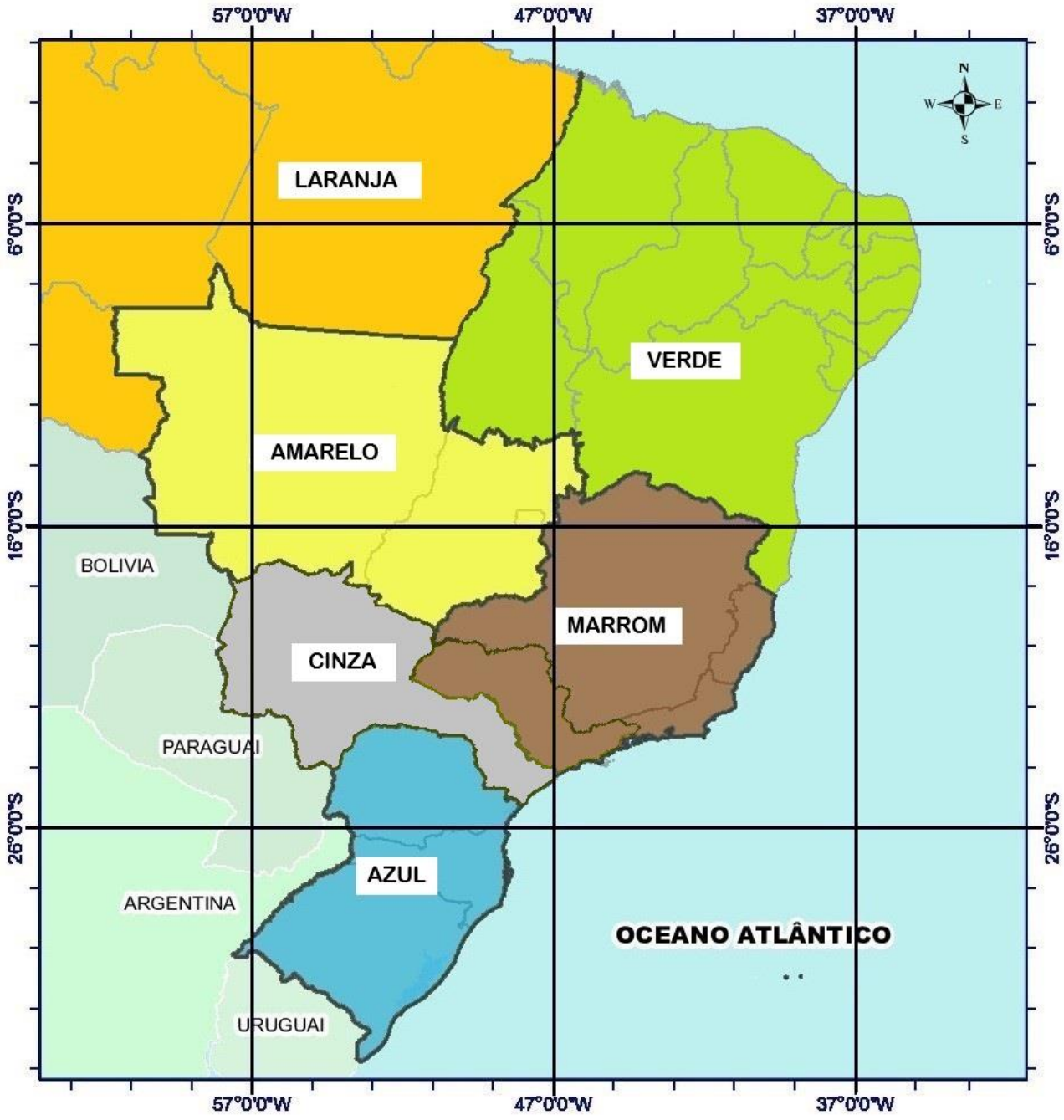
No século XX, a porção leste de MERIDIANO apresentava as fronteiras nacionais com a seguinte configuração.



Ainda no século XX, MERIDIANO foi assolado pela GRANDE GUERRA MERIDIONAL (GGM), ao fim da qual **MARROM** anexou parte do território anteriormente pertencente a **AMARELO**, deixando a configuração fronteiriça na forma mostrada abaixo.



Após a derrota de **AMARELO**, separatistas localizados na porção sul do país aproveitaram-se do enfraquecimento do governo central e declararam sua independência, adotando o nome de **CINZA**. A independência foi rapidamente reconhecida por **ROXO**, uma potência extrarregional que sempre demonstrou interesse nas potencialidades comerciais do subcontinente, sem muito sucesso. Subsequentemente, a ONU reconheceu **CINZA** como nação independente e soberana, formalizando as fronteiras como mostrado abaixo:



Desde a independência, **CINZA** reclama a área anteriormente pertencente a **AMARELO** anexada por **MARROM** após a GGM. Recentemente, forças de **CINZA** invadiram uma porção litorânea ao sul do território de **MARROM**. Isso levou o Conselho de Segurança da ONU (CS/ONU) a encerrar negociações diplomáticas com **CINZA** e a aprovar a resolução Nº 4379/2021, que prevê uma intervenção militar dentro da área ocupada de **MARROM** e, se necessário, em território de **CINZA**. Foi então autorizada a formação de uma Força Militar Multinacional de uma coalizão de países da porção sul do subcontinente MERIDIANO, integrantes da Organização dos Estados Meridianos (OEM), com o intuito de restabelecer a integridade territorial de **MARROM**. A resolução atribuiu o comando da força de coalizão a **AZUL**.

2 DESENVOLVIMENTO DO CENÁRIO PARA O EGC

2.1 Contexto do Ciberespaço Azulino

A notável expansão do uso da Internet e dos telefones celulares, a partir da segunda metade dos

anos 1990, levou o governo de **AZUL** a criar políticas para democratizar o acesso às Tecnologias da Informação, de forma a permitir a inserção de toda sua população na sociedade da informação. Chamada de Inclusão Digital, essa iniciativa visava trazer mais benefícios para a vida pessoal e profissional dos cidadãos, simplificando a rotina diária, maximizando o tempo e as potencialidades das pessoas, melhorando suas condições de vida e trazendo novas oportunidades de emprego, meios de comunicação e formas de obtenção do aprendizado.

Como resultado dessa política, atualmente, 81% de toda a população de **AZUL** têm acesso à Internet. O principal meio é o telefone celular, presente em 99,5% dos lares azulinos, enquanto os computadores estão presentes em 45,1% deles.

Em paralelo, uma Estratégia de Governo Digital, centrada na plataforma Gov.az, fez com que **AZUL** disponibilizasse a seus cidadãos um grande volume de serviços digitais, levando o país a ser considerado o 2º melhor governo digital do mundo.

Entretanto, a popularização do uso de serviços on-line e da Internet em geral trouxe também a preocupação com questões relacionadas à Cibersegurança, envolvendo a confidencialidade, integridade, disponibilidade e autenticidade dos ativos cibernéticos (software, hardware e dados) envolvidos no processamento e comunicação de informações. AZUL amarga uma incômoda 18ª posição no ranking de cibersegurança da UIT, incompatível com o nível de serviços digitais ofertados.

Com o objetivo de coordenar e integrar todas as iniciativas de serviços de Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados, foi criado em meados dos anos 1990 o Comitê Gestor da Internet em **AZUL** (CGI.az) que mantém um Grupo de Resposta a Incidentes de Segurança para a Internet (CERT.az), que atua como um ponto central para notificações de incidentes de segurança em **AZUL**, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato.

Além do CERT, **AZUL** ainda conta com o CTIR.Gov (Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal) que é integrante da recém-criada Secretaria de Segurança da Informação e Cibernética (SSIC) do Gabinete de Segurança Institucional da Presidência da República e que tem como finalidade precípua o atendimento aos incidentes em redes de computadores pertencentes à Administração Pública Federal (APF).

Embora a segurança cibernética em **AZUL** siga padrões mundiais, o mesmo não se pode dizer do ordenamento jurídico para combater crimes cibernéticos. As leis que poderiam inibir a proliferação de tais crimes são defasadas e pouco abrangentes, abrindo espaço para que um número crescente de pessoas e grupos atue ilicitamente com relativa liberdade no ciberespaço, realizando *hacktivismo*, crimes cibernéticos (furto de dados bancários, perfis de redes sociais e invasão de privacidade), espionagem cibernética e terrorismo cibernético.

Nos dias atuais, a facilidade de acesso à Internet, a falta de legislação específica que puna severamente os crimes cibernéticos, a fiscalização governamental precária e a existência de um sistema econômico alternativo (que não tem uma entidade reguladora central), têm criado condições para a captação de talentos para atuar em atividades ilícitas na Internet.

Visando melhorar esse cenário, recentemente, **AZUL** iniciou o debate público de uma proposta de criação de sua Política Nacional de Cibersegurança, contemplando uma Agência Nacional de Cibersegurança que objetiva coordenar os esforços hoje dispersos de cibersegurança no país. A expectativa do governo é de que num universo temporal de 5 anos **AZUL** esteja mais bem preparado para enfrentar o crescente cenário global de ciberincidentes.

2.2 Ciberincidentes Recentes ao Redor do Mundo

2.2.1 Ransomware

Merecem destaque ciberataques do tipo *ransomware*, que criptografam arquivos do disco rígido,

ou até mesmo a tabela mestre de arquivos para que o sistema de arquivos se torne ilegível e o Sistema Operacional (Windows ou equivalente) não consiga sequer iniciar, e que exigem das vítimas um pagamento em *criptomoedas* para que o acesso aos arquivos seja devolvido ao usuário.

O primeiro a chamar a atenção, nessa categoria, foi o *worm Petya*, que atingiu diversos departamentos de Recursos Humanos em agências públicas e empresas privadas que utilizavam equipamentos com a mesma vulnerabilidade. Entretanto, ameaçava excluir os arquivos caso não houvesse pagamento de resgate.

Acredita-se que o *Petya* esteja por trás do imenso ataque de *ransomware* que afetou empresas e organizações em todo o mundo no final de junho de 2016. O país mais afetado nesse ataque foi a Ucrânia, atingindo o metrô de *Kiev*, o Banco Nacional da Ucrânia e vários aeroportos, para citar alguns de seus alvos mais chamativos. Muitas empresas multinacionais com sede em **AZUL** também relataram terem sido afetadas.

Outro *ransomware* de destaque, denominado *Wannacry*, destacou-se por explorar falhas no sistema operacional Windows que haviam sido descobertas pela ASO, a agência de segurança de **MARROM**, e tornadas públicas após um vazamento. O malware também ficou conhecido por ter atingido duramente o serviço de saúde pública do Reino Unido.

Logo em seguida, outro *ransomware*, batizado de *NotPetya* por diferir de seu irmão *Petya* na forma de ataque, foi considerado o mais devastador malware da história até o momento, tendo atingido duramente grandes empresas globais de logística, como a dinamarquesa Maersk, maior transportadora de contêineres do mundo, e a norte-americana FedEx, maior entregadora global de pacotes e encomendas.

Em maio de 2021, outro *ransomware* paralisou por 3 dias um importante oleoduto norte-americano, operado pela Colonial Pipeline, o que fez com que a companhia interrompesse a operação de todos os seus oleodutos de forma a evitar a propagação do malware, e levou o governo norte-americano a decretar estado de emergência em 17 estados daquele país.

Em março de 2022, no bojo da invasão da Ucrânia, uma onda de ataques combinando o uso de malwares até então desconhecidos com ataques cinéticos a hubs de redes de comunicação desabilitou as telecomunicações na Ucrânia, situação que só foi parcialmente contornada quando a empresa Starlink enviou centenas de kits de acesso à Internet por satélite para o país.

2.2.2 Wiper

Em 2022, no contexto da Guerra da Ucrânia e da popularização do ransomware, uma nova categoria de malware surgiu. Consiste em programa que "disfarçam-se" de ransomware, simulando terem criptografado os dados do usuário e por vezes até demandando resgate para sua restituição. No entanto, muitas vezes sequer dispondo de meios para a "devolução" do acesso aos dados ou para o recebimento do resgate, tendo apenas removido todo o conteúdo dos dispositivos infectados, numa atitude meramente destrutiva, que além de prejudicar o usuário pela ausência da informação ainda busca manter suas equipes de resposta a incidentes desnecessariamente ocupadas.

2.2.3 Ataques a Cadeias Logísticas Cibernéticas

Embora não seja novo, como casos conhecidos envolvendo hardware falso ou adulterado desde os anos 2000, nos últimos 5 anos ganhou impulso também um tipo de ataque que visa o comprometimento da cadeia de suprimento de produtos de software. Componentes maliciosos são inseridos em programas comerciais e são disseminados pelo próprio processo de atualização de versões do fabricante. Em 2017, o ransomware NotPetya foi disseminado assim, após ser inserido na cadeia de suprimento de um aplicativo de contabilidade usado por empresas ucranianas. Logo depois, em 2018, veio o caso do antivírus CCleaner. Mas o mais sofisticado foi, certamente, o caso software de gerenciamento de redes e serviços de TI SolarWinds, em 2020. A plataforma, amplamente utilizada nos EUS, foi infectada com uma backdoor que se disseminou para seus clientes, e que permitiu o acesso não autorizado a dados de

centenas de corporações, bem como do Departamento de Segurança Interna (DHS) e do Departamento do Tesouro (no qual trabalham os agentes do Serviço Secreto que fazem a segurança do Presidente daquele país) por meses.

2.3 Ciberataques Recentes no Contexto Regional

Nos últimos 3 anos, criminosos independentes e grupos organizados exploraram vulnerabilidades de serviços digitais que se tornaram essenciais na vida das pessoas de **AZUL**.

A situação se agravou após a resolução do CS/ONU autorizando uma intervenção militar comandada por **AZUL** destinada à desocupação de territórios de **MARROM** invadidos por **CINZA**.

Houve um significativo crescimento dos ciberataques reportados pelas empresas de cibersegurança. Em consequência da pandemia, observou-se que a utilização de equipamentos portáteis tanto para uso pessoal quanto em ambiente de trabalho, prática conhecida com BYOD (*Bring Your Own Device*), aumentou drasticamente, constituindo-se uma ameaça ainda mais preocupante nas empresas, instituições públicas, Forças Armadas de **AZUL** e em todas as entidades que possuam informações sigilosas.

Outrossim, tem crescido a quantidade de ciberincidentes envolvendo empresas e órgãos governamentais. Esses vazamentos têm ocorrido em virtude não apenas das ameaças internas, com elementos infiltrados, mas principalmente pela sofisticação crescente nos ataques de engenharia social direcionados aos funcionários dessas instituições, conhecidos como *spear-phishing*, utilizados por criminosos e por ameaças persistentes avançadas (APTs) a serviço de estados nacionais, as quais buscam estabelecer acesso às organizações a qualquer custo.

2.3.1 O Grupo Incognitus

O grupo hacker conhecido como *Incognitus*, financiado por **CINZA**, e que já causou severos prejuízos ao Sistema Bancário de **AZUL** no passado, voltou a se manifestar. Porém, desta vez, informando em mídias sociais que conseguiu acessar diversos sistemas de informações de Órgãos da APF e das Forças Armadas de **AZUL**. Adicionalmente, informes dão conta de que tal grupo possui elementos infiltrados nas Forças Armadas e em diversas outras organizações.

2.4 Ciberincidentes Envolvendo Serviços Essenciais de AZUL

Ao longo do ano passado, foram observadas em **AZUL** várias tentativas de ataques cibernéticos a infraestruturas críticas e a provedores de serviços essenciais, dos mais diversos setores.

2.4.1 Ciberincidentes Envolvendo a Área de Finanças

Em julho do ano passado, o Sistema Bancário de **AZUL** ficou completamente indisponível por vários dias. Investigações preliminares indicam a participação de uma potência extrarregional com fortes indícios da utilização integrada de tecnologias avançadas, como supercomputadores e Inteligência Artificial (IA).

Recentes ações cibernéticas novamente levaram a reiteradas falhas no Sistema Bancário de **AZUL**, causando sérios danos à economia do País, com um impacto fortemente negativo nas Bolsas de Valores e perante seus parceiros e investidores internacionais.

A população tem enfrentado dificuldades em realizar transações com seus dispositivos móveis, gerando revolta e iniciando uma série de protestos, saques e destruição das poucas agências bancárias existentes, em virtude da falta de solução imediata para o problema apresentado.

2.4.2 Ciberincidentes Envolvendo a Área de Águas

2.4.2.1 Setor Abastecimento Urbano de Águas

Foram observados ciberincidentes em estações de tratamento de água de ao menos duas grandes cidades de **AZUL**, que visavam amplificar significativamente a quantidade de produtos químicos

misturados à água tratada, contaminando-a com índices elevados, e possivelmente tóxicos, de cloro e flúor, tornando-a insalubre e podendo afetar significativamente a saúde pública.

2.4.2.2 Setor Barragens

Desde 2015, quando foi revelada a ocorrência de um ciberataque na barragem Permanece sob investigação o incidente envolvendo a barragem Bowman Avenue Dam, na cidade de Rye Brook, logo ao norte da cidade de Nova York, há uma grande preocupação de AZUL com o controle das barragens.

A preocupação foi ainda mais ampliada quando, em novembro de 2021, a Austrália anunciou que a maior empresa de fornecimento de água da região de Queensland, que administra 19 barragens, foi vítima de uma violação de seus sistemas originada no exterior que permaneceu não detectada por 9 meses (de agosto de 2020 a maio de 2021).

2.4.3 Ciberincidentes Envolvendo a Área de Energia

2.4.3.1 Setor Elétrico

Há fortes indícios também de que a mesma potência extrarregional identificada nos ataques ao setor financeiro teria apoiado os ciberataques responsáveis pelas recentes quedas de energia na região central do país, principal região industrializada de **AZUL**, onde boa parte do Sistema Elétrico da região opera sob concessão da KPEL, multinacional que há dois anos adquiriu o controle acionário da antiga empresa estatal local.

A KPEL é uma multinacional sediada no continente **ORIENTAL** que tem investido pesado em suas subsidiárias, buscando aumentar seu poder de influência ao redor do mundo. As recentes quedas de energia têm sido atribuídas a ataques cibernéticos contra a KPEL, mas existem fontes de informação indicando uma ação orquestrada, por determinação de **CINZA,** que busca provocar o caos em **AZUL**.

Uma análise forense dos ciberataques, realizada por uma equipe especializada do Centro de Defesa Cibernética de **AZUL**, concluiu que o código malicioso (*malware*) encontrado na infraestrutura da operadora KPEL foi provavelmente projetado, instalado e controlado pelo serviço de inteligência de **CINZA**.

Estas ações, inclusive, levantaram algumas questões que ainda precisam ser mais bem estudadas e definidas, tais como:

1. Qual o grau de responsabilidade da empresa KPEL diante do incidente?
2. Como avaliar a conduta de **CINZA** nessas ações?
3. Quais legislações podem ser empregadas para imputar responsabilidade a **CINZA**?
4. As Operações Cibernéticas sem efeitos cinéticos podem representar um uso proibido da força?
5. Qual o entendimento para noção de força neste contexto?
6. O país **AZUL,** afetado, teria amparo legal para responder ciberneticamente ou cineticamente sob alegação de legítima defesa?

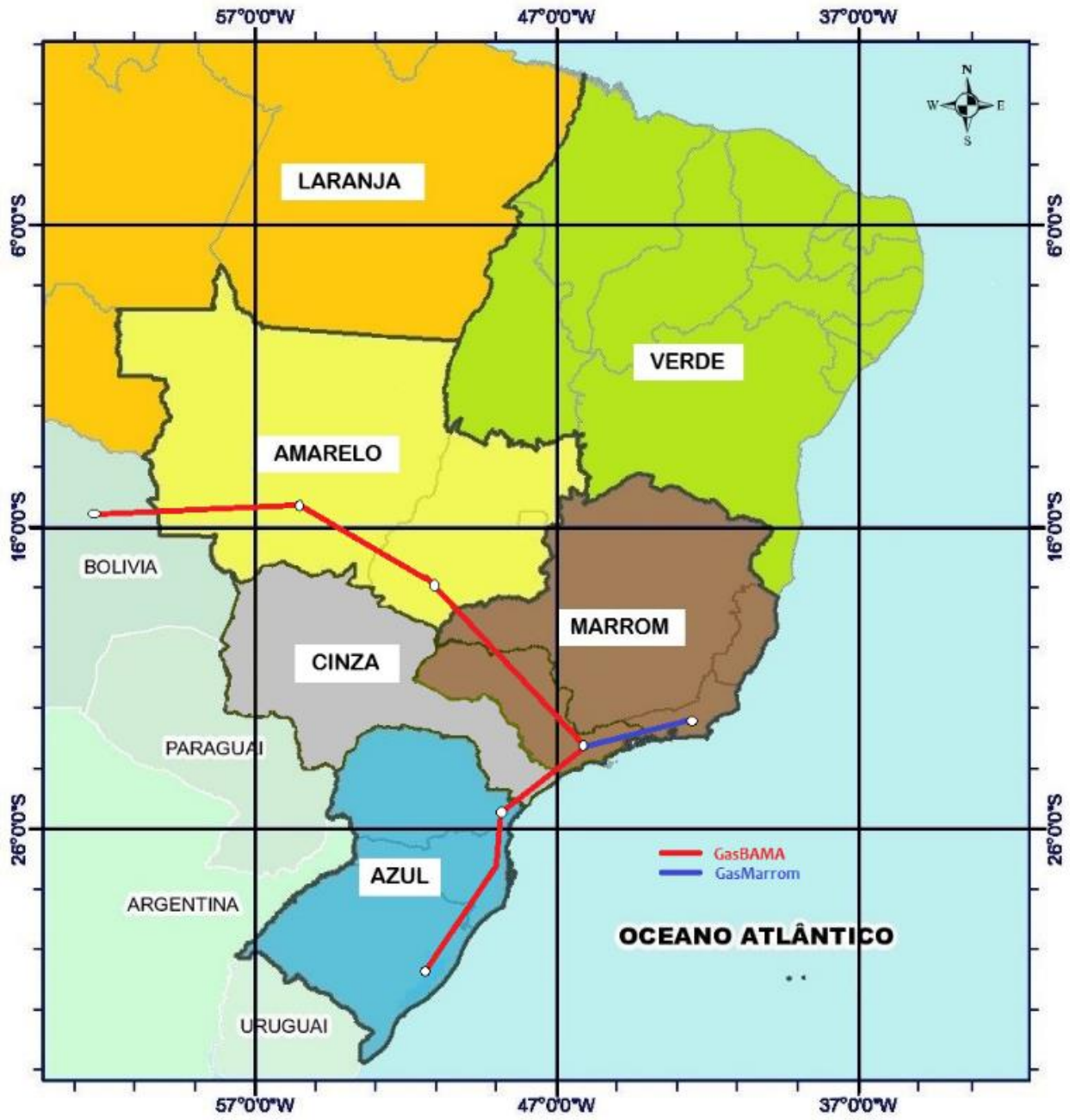
Também foram registrados diversos ataques às usinas hidrelétricas (UHs) azulinas, em particular à de Salto Osório (UHSO), empreendimento binacional de **AZUL** e do Paraguai responsável não apenas pelo suprimento de 50% da energia elétrica do país, como também de boa parte da eletricidade consumida por **MARROM**, **AMARELO** e **LARANJA**. Um número crescente de ataques também foi identificado no sistema integrado de distribuição de energia de **AZUL**, Não obstante o significativo (e preocupante) número de ataques, não foi registrado nenhum incidente de maior gravidade naquela usina. Nenhum grupo hacker reivindicou a autoria dos ataques, mas existem fortes indícios de que eles tenham sido realizados por membros do IPP e da organização criminosa local denominada Comando Geral de Ação (CGA), com apoio de hackers de **CINZA**.

Um apagão, que atingiu grande parte de **MARROM** em agosto, permanece sem explicação. E há rumores de que o mesmo poderia ter sido causado por um incidente cibernético. Considerando a

similaridade dos sistemas de controle de MARRON e de AZUL, a agência reguladora de energia elétrica de **AZUL** ofereceu-se para auxiliar as investigações junto à sua congênere de **MARROM**.

2.4.3.2 Setor PEGANBIO (Petróleo, Gás e Biocombustível)

Observou-se, também, a ocorrência de ciberataques exploratórios contra o Gasoduto Bolívia-AMARELO-MARROM-AZUL (ou GasBAMA). O gasoduto, de mais de 3.200km, é responsável por cerca de 30% de todo o gás natural utilizado em **AZUL**, dos quais cerca de 1/3 é usada na produção de energia elétrica em termelétricas. Ele entrou em operação pouco antes da independência de **CINZA**, e quando da emancipação houve muitas preocupações com a continuidade do suprimento a **AZUL**. A despeito de ameaças pontuais de interrupção do fornecimento no Ramo-Sul, **CINZA** manteve a operação regular do GasBAMA, que segue o trajeto mostrado no mapa abaixo.



Cresce a incerteza no tocante a essa continuidade diante da intensificação das divergências entre **CINZA** e **AZUL**. Do ponto de vista cibernético, esse aumento da incidência de ciberataques exploratórios é preocupante em decorrência do ciberataque que vitimou a Colonial Pipeline nos EUA.

2.4.4 Ciberincidentes Envolvendo a Área de Transportes

2.4.4.1 Setores Rodoviário e Ferroviário

Ciberincidentes foram registrados afetando a operação dos sistemas de pedágio nos dois principais acessos da Capital de **AZUL**, por ocasião do final de tarde do último dia de um feriado prolongado, provocando filas que, segundo a Concessionária, chegaram a 43 km numa rodovia e 37 km na outra, com espera estimada em até 5 horas nessas filas. O problema foi agravado pelas panes de veículos que ficaram sem combustível ou que tiveram problemas de superaquecimento. A grande concentração de smartphones em uso pelos passageiros nas filas também provocou a saturação do serviço nas antenas das pequenas cidades que margeavam os pontos de congestionamento, gerando grande insatisfação de seus moradores.

Não foram observados incidentes relacionados à operação do sistema ferroviário, mas cresce a preocupação de que essa relativa tranquilidade possa ser interrompida por um ciberataque que provoque complicações operacionais, a exemplo do que se observou quando hackers simpatizantes da Ucrânia atacaram os sistemas ferroviários da Bielorrússia que transportavam meios militares russos no início da invasão da Ucrânia.

2.4.4.2 Setor Aeroviário

Alguns relatos de ciberincidentes envolvendo operadores aeroportuários foram registrados, embora nenhum tenha efetivamente chegado a comprometer a operação de aeroportos importantes de forma significativa, ou ainda as principais companhias de transporte aéreo de passageiros ou de cargas. Não obstante, o grupo *Incognitus* sinaliza a possibilidade de ter obtido acesso a sistemas de uma concessionária (não nominada) que "opera um dos 3 maiores hubs aeroportuários de **AZUL"**.

2.4.4.3 Setor Aquaviário

Diferentes ciberincidentes envolvendo operadores portuários, navais, fluviais e de eclusas vêm sendo relatados ao CERT.az. Os incidentes envolvem tentativas de acesso não autorizado aos mais diversos sistemas e servidores computacionais. Em alguns casos houve o comprometimento de sistemas que levaram à paralização temporária da operação de contêineres, resultando em atrasos na atracação e desatracação de navios e enormes filas dos meios de transporte aguardando carga e descarga dos navios. Noutro caso, informações aduaneiras das cargas foram comprometidas, levando a atrasos no despacho aduaneiro. Há também dois relatos, ainda sob investigação, de "quase-colisão" de navios possivelmente provocada por interferência no sistema de navegação das embarcações.

2.4.5 Ciberincidentes Envolvendo a Área de Comunicações

2.4.5.1 Setor Telecomunicações

O Sistema Telecomunicações, similarmente ao Setor Financeiro, é um dos mais maduros no tocante à ciberdefesa e à cibersegurança, não obstante (ou talvez em decorrência de) geralmente ser um dos mais atacados. Dado este histórico, é relativamente surpreendente que nenhum grave ciberincidente tenha afetado diretamente as concessionárias do setor em **AZUL** nos últimos meses. Mas essa "calmaria" pode estar com os dias contados. A intensificação das ameaças de **CINZA** e do grupo *Incognitus* colocou o setor em alerta, em particular por conta do observado no setor durante a Guerra Russo-Ucraniana.

Destaques foram os ciberincidentes que afetaram os serviços dos aplicativos de mensagens WhatsOn e InstantOn, operados por empresas multinacionais, mas extremamente populares em **AZUL**. Embora os incidentes tenham ocorrido no exterior, usuários azulinos, diante da indisponibilidade do serviço, aderiram em números expressivos ao serviço TelegrOn, também estrangeiro, e então sem representação legal no país, para tentar suprir a falta dos outros serviços.

2.4.5.2 Setor Serviços Postais

Um ciberataque causado por *ransomware* atingiu duramente o serviço AzulEx, dos Correios de **AZUL**, responsável por cerca de 50% da entrega de pacotes e encomendas expressas do país, causando a

paralização desse serviço por 9 dias. Disso resultaram enormes prejuízos decorrentes da perda de produtos perecíveis, da perda de prazos para entrega de documentos e da falta de insumos para a produção de bens e serviços de pequenas empresas, além de um grande volume de reclamações e processos judiciais buscando o ressarcimento desses prejuízos.

2.4.5.3 Setor Radiodifusão

Depois do ciberataque à TV5 francesa, que afetou os 12 canais mantidos pela empresa em quase a levaram à falência, em 2015, parecia que o setor de radiodifusão estava livre de maiores ameaças.

As preocupações se reacenderam quando, em meados de 2021, diversas emissoras de TV dos EUA pertencentes ao Cox Media Group, nos estados da Flórida, Carolina do Norte e Pensilvânia foram vitimadas por ciberataques.

Então, em 2022, veio o ataque à azulina Rede Record, que teve quase todo o seu acervo de mídia digital indisponibilizado por um ransomware, levando a empresa e recorrer a mídias analógicas e a mudar sua grade de programação por vários dias. Até mesmo os noticiários ficaram limitados, sendo substituídos por reprises de filmes e programas de auditório. Adicionalmente, a empresa teve diversas informações sigilosas vazadas.

2.4.6 Ciberincidentes Envolvendo a Área de Biossegurança e Bioproteção

Começa-se a discutir o que se está chamando ciberbiossegurança, um campo emergente na interseção entre cibersegurança e biossegurança, abordando "a destruição potencial ou real maliciosa, o uso indevido ou a exploração de informações, processos e materiais valiosos na interface das ciências da vida e dos mundos digitais"[1].

O setor ganhou muita visibilidade durante a pandemia da Covid-19. Em 2020, o governo norte-americano indiciou dois cidadãos chineses por ciberataques contra a farmacêutica Moderna. Em 2021, no Reino Unido, o NCSC registrou ciberataques contra a Universidade de Oxford, onde a vacina da AstraZeneca era pesquisada. Nos EUA, o Departamento de Segurança Interna (DHS) divulgou um alerta quanto ao crescimento de ciberataques envolvendo 44 empresas de 14 países da Europa, América do Norte, América do Sul e Ásia engajadas nos processos de transporte, armazenamento a frio e distribuição de vacinas contra a Covid-19.

2.4.7 Ciberincidentes Envolvendo a Área de Defesa

Devido ao atraso no pagamento de compromissos financeiros, o ataque ao Sistema Bancário de **AZUL** impactou no pagamento dos militares e no fornecimento de peças sobressalentes, de medicamentos e de combustíveis para suas forças armadas.

Crescem na mídia informes de que **AZUL** pode ser vítima de ataques cibernéticos direcionados a seus sistemas de defesa. Esses informes dão conta de ameaças no sentido da possibilidade de interferência em, ou mesmo interrupção de, serviços como o controle do espaço aéreo, operação de bases militares e de sistemas de controle de armas.

O grupo hacker *Incognitus* anunciou ter obtido credenciais de militares de **AZUL** para acesso a sistemas do Ministério da Defesa. Isso poderia explicar o recente incidente de inserção de mensagens de cunho político na página na Internet e nas redes sociais do Ministério da Defesa de **AZUL**.

O recente anúncio de que o telefone funcional do Ministro da Defesa da Espanha foi infectado com o *spyware* Pegasus, possivelmente ativo ao longo dos últimos 6 meses, alarmou o Governo de **AZUL**, que determinou uma verificação em profundidade dos aparelhos das autoridades de primeiro e segundo escalão do governo, e dos quatro mais altos escalões da Defesa, em particular no tocante a este *spyware*. A preocupação é de que **CINZA** possa estar usando esse malware para obter informações sobre as defesas de **AZUL**.

[1] Richardson, Lauren; Connell, Nancy; Lewis, Stephen; Pauwels, Eleonore; Murch, Randy. *Cyberbiosecurity: A Call for Cooperation in a New Threat Landscape*, 2019.

2.4.8 Ciberincidentes Envolvendo Outras Áreas

2.4.8.1 Área de Justiça

Em fins de 2020 um ataque de grandes proporções à Corte Superior de Justiça de **AZUL**, oriundo de outro país, deixou indisponíveis quase todos os sistemas do tribunal, inviabilizando o funcionamento do mesmo e impactando em centenas de processos. O ataque do tipo *ransomware* utilizou credenciais legítimas de servidores e prestadores de serviço do tribunal, obtidas por *phishing*, para implantar um malware que explorava uma vulnerabilidade *0-day* ("de fábrica" ou "de origem") de um middleware de virtualização e atingiu mais de uma centena de "máquinas virtuais" da corte. No debate que se seguiu a ciberataque, pesquisadores observaram que há quase um século a Corte Internacional de Justiça, sediada em Haia, considera que um princípio básico de soberania regido pela Legislação Internacional, é a capacidade de prestação jurisdicional (aplicação da lei) de forma autônoma, e que um ataque que inviabiliza tal prestação jurisdicional, advindo de uma nação estrangeira, poderia ser considerado uma violação formal de soberania nacional.

Poucos dias depois, outro ciberataque, desta feita tendo como alvo a Corte Superior Eleitoral de **AZUL**, reacendeu o inflamado debate sobre a segurança do processo eleitoral azulino. Quando a corte reiterou que seus sistemas são "completamente seguros", dados internos daquele tribunal, em sua quase totalidade afetos a áreas administrativas, foram vazados para a mídia, levantando novamente questões sobre a "completa segurança" oferecida pela corte.

2.4.8.2 Área de Saúde

Um grande ciberataque ao Ministério da Saúde de **AZUL**, em fins do ano passado, comprometeu os sistemas de controle da vacinação da população do país, bem como a emissão de certificados de vacinação, em plena pandemia. O sistema ficou inoperante por vários dias. As origens do ataque e a extensão dos efeitos provocados ainda são investigadas.

Noutra linha de incidentes, que aparentemente envolve a chamada "cadeia cibernética de suprimentos" (*cyber supply chain*), a empresa que fornece os softwares de gestão hospitalar e gestão laboratorial mais usados no sistema de saúde de **AZUL** informou ter encontrado uma *backdoor* em seu sistema, que estaria no software ao menos há 4 anos. Não ficou clara a origem dessa vulnerabilidade. A empresa acredita que essa *backdoor* possa justificar a ocorrência de diversos casos de vazamento de informações confidenciais de saúde de pessoas de grande visibilidade pública. Ela também poderia ter sido o meio utilizado em diversos casos de emissão de laudos médicos com resultados falsos. Num desses casos, um político conservador de grande visibilidade teria desistido de concorrer à Presidência do país após realizar exames de rotina e receber dois laudos laboratoriais indicando que ele seria portador de uma grave doença sexualmente transmissível. O caso causou grande comoção no país, e abalou profundamente a credibilidade do partido conservador naquele pleito. Posteriormente, descobriu-se que ambos os laudos foram forjados.

2.4.8.3 Área de Educação

No âmbito da Educação foram observadas diversas tentativas de ciberataques, mas poucas tiveram resultados perceptíveis pelo público. Na mais significativa, a página de inscrição para o Exame Nacional de Admissão, pré-requisito para o acesso ao ensino superior em **AZUL,** e realizado apenas uma vez por ano, foi sobrecarregado nos últimos dias do prazo de inscrição, levando o Ministério da Educação a prolongá-lo. Conquanto o ministério tenha reputado o incidente a problemas técnicos, a mídia repercutiu a opinião de alguns pesquisadores que suspeitavam que a lentidão fora provocada por um ataque do tipo DDoS (Negação Distribuída de Serviços), com uma inundação de requisições falsas sendo disparadas contra o site.

Outra situação que provocou repercussões na mídia diz respeito a atrasos no pagamento de bolsas a pesquisadores de **AZUL**, no país e no exterior, provocada por falhas concomitantes nos dois sistemas de gestão da instituição de fomento à pesquisa científica de **AZUL**. Embora a versão oficial atribua o

problema a uma falha no sistema de armazenamento do antigo computador utilizado, que não dispunha de contrato de manutenção, a mídia também ventilou a possibilidade de as falhas serem decorrentes de ciberataques localizados. Em qualquer dos casos, as falhas dos sistemas tiveram repercussão muito negativa na opinião pública, e em particular junto à comunidade científica diretamente atingida.

2.5 Conclusão

Depreende-se que **AZUL,** além dos problemas já enfrentados no campo da segurança da informação, passou a sofrer com problemas isolados que, analisados em conjunto, indicam apossibilidade de uma campanha cibernética contra os Ativos Informacionais de suas infraestruturas estratégicas.

Os canais de mídia de **CINZA**, agora estatizados, realizam intensa campanha de desinformação junto à população local, enfatizando "a intenção dos países **AZUL, AMARELO e MARROM** de subjugar o povo cinzento, influenciar em sua autodeterminação e impedir o desenvolvimento regional".

Atribui, ainda, a responsabilidade pela situação precária que vive a população de **CINZA** às políticas econômicas agressivas e políticas imperialistas de **MARROM** e de **AZUL**, contribuindo para a crença popular de que a não exploração das reservas petrolíferas existentes na zona econômica exclusiva (ZEE) do Mar de **CINZA** é o grande mal que impede o desenvolvimento regional e a melhoria das condições de vida do seu povo.

O grupo hacker *Incognitus* é conhecido por possuir especialistas em acessar dispositivos portáteis para ganhar acesso a redes de grandes corporações. Os membros do grupo, uma vez em posse de informações sigilosas, as vendem no mercado negro. Quando não há a possibilidade de grandes lucros, o grupo age de forma a tentar causar caos sob o argumento de que toda informação deve ser livre, ou como forma de protesto contra a corrupção no Governo.

No mês passado, o grupo *Incognitus* lançou a campanha *#OpAdeus* que pretende, por meio de ciberataques sistemáticos, criar uma instabilidade econômica em **AZUL** e criar o caos em sua vida administrativa.

Em sua página na Internet, o grupo manifestou:

> *Suspendam o apoio a **MARROM**, e deixem o comando da força de coalizão ou a legião atuará contra **AZUL** levando o cibercaos a todos os setores estratégicos. Nós somos Incognitus. Somos uma legião. Nós não esquecemos. Nós não perdoamos. Esperem por nós.*

O cenário do EGC4.0 foi elaborado em conjunto pelo ComDCiber e pelo Instituto Vegetius, tendo por base o cenário do Exercício Meridiano, do Ministério da Defesa.