CÉLIO BORGES TAQUARY SEGUNDO

A DEFESA CIBERNÉTICA EM AMBIENTES DE INFRAESTRUTURA CRÍTICA E OS RISCOS DOS ATAQUES CIBERNÉTICOS

Trabalho de Conclusão de Curso – artigo científico apresentado à Comissão de Avaliação de TCC da Escola Superior de Guerra – Campus Brasília como exigência parcial para obtenção do certificado de Especialista em Altos Estudos em Defesa.

Orientador:Prof. Dr. Darcton Policarpo Damião

Brasília
2019

_____

CÉLIO BORGES TAQUARY SEGUNDO

A defesa cibernética em ambientes de infraestrutura crítica e os riscos dos ataques cibernéticos

Célio Borges Taquary Segundo[1]

RESUMO

Com o advento de novas tecnologias o espaço cibernético trouxe a conexão e celeridade ao mundo moderno e ainda, as vulnerabilidades existentes nesse ambiente. Além do aumento de usuários, verificou-se que existe um crescente número de ataques no ciberespaço, dentre eles, contra o próprio Estado, o que poderá afetar a infraestrutura crítica de um país, que são os meios de telecomunicações, energia, finanças, água e transporte, por exemplo, trazendo grandes riscos, prejuízos e impactos na vida do cidadão. Diante do exposto, o estudo procura evidenciar a segurança cibernética no Estado Brasileiro concomitantemente com o Sistema de Defesa Cibernética e as infraestruturas críticas, com aspectos conceituais que se relacionam ao tema, além de breves comentários às normatizações que regem o ciberespaço e segurança cibernética, citando riscos as infraestruturas críticas e meios que possam trazer soluções para as questões tratadas no referido estudo.
Palavras-chave: Segurança Cibernética. Defesa Cibernética. Infraestrutura crítica. Segurança da Informação.

Cyber defense in critical infrastructure environments and the risks of cyber attacks

ABSTRACT

With the advent of new technologies The cyberspace has brought the connection and celerity to the modern world and yet the vulnerabilities existing in this environment. In addition to increasing users, it was found that there is a growing number of attacks in cyberspace, among them, against the state itself, which could affect the critical infrastructure of a country, which are the means of telecommunications, energy, finances, water and transportation, for example, bringing great risks, losses and impacts on the life of the citizen. In view of the above, the study seeks to highlight cybersecurity in the Brazilian state concomitantly with the cyber defense system and critical infrastructures, with conceptual aspects related to the theme, as well as brief comments to Standardization that govern cyberspace and cyber security, citing risks to critical infrastructures and means that can bring solutions to the issues dealt with in the aforementioned study.
Keywords: *Cyber security. Cybernetic defense. Critical infrastructure. Information security.*

[1] Mestre em Informática (UFRJ), Profissional Petrobras de Nível Superior Master - Petrobras. Trabalho de Conclusão do Curso de Altos Estudos em Defesa (CAED) da Escola Superior de Guerra (ESG) – Campus Brasília (2019).

1 INTRODUÇÃO

Nos últimos anos, os serviços baseados em novas tecnologias trouxeram muitos benefícios aos usuários, mas também aumentaram em muito a complexidade e a diversidade dos ambientes e consequentemente o aumento de vulnerabilidades e ameaças de segurança cibernética.

O espaço cibernético é o novo ambiente da humanidade e não possui fronteiras claramente definidas e há uma dificuldade de atribuição de responsabilidades. Neste cenário, os ataques cibernéticos estão em crescente escalada.

Mas que tipos de ameaças existem nesse novo espaço? Geralmente os ataques se enquadram em uma das seguintes categorias: a interceptação, a modificação ou a negação da informação (MORESI, 2012). Eles podem ser dissimulados ou assumidos e podem trazer impactos físicos ou não, que variam desde desfiguração de *websites*, perdas financeiras, parada de um serviço ou ainda a indisponibilização de uma infraestrutura crítica para o país.

No Brasil, consideram-se Infraestruturas Críticas – IFCs, as instalações, serviços e bens que se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional. Os serviços prestados por essas infraestruturas, energia, telecomunicações, finanças, transporte, águas e outros também compartilham do espaço cibernético, alguns deles suportando a sua própria existência. Esses serviços possuem dimensão estratégica pois são essenciais para cidadãos, organizações e para o Estado, uma vez que desempenham papel tanto para a segurança e soberania nacional como para a integração e o desenvolvimento econômico sustentável do País (SANTOS; CARVALHO; CAVALCANTE, 2011). Dessa forma, problemas no fornecimento desses serviços podem acarretar transtornos e prejuízos ao Estado, à sociedade, à população e ao meio ambiente.

Neste sentido, a última versão da Estratégia Nacional de Defesa – END do Brasil, publicada em 2012, priorizou o setor cibernético como um dos três setores estratégicos essenciais para a defesa nacional. Dentre as prioridades deste setor, destaca-se a proteção das infraestruturas estratégicas/críticas. Sob a coordenação do Exército, foi elaborado em 2012 um programa para a implantação do Sistema de Defesa Cibernética.

No ano seguinte, em 2013, após as denúncias de espionagem conduzidas contra o País por agentes internacionais, o Ministério da Defesa – MD também criou um Grupo de Trabalho para elaborar propostas que contribuíssem com a potencialização da defesa cibernética nacional em face de ameaças externas e internas.

Neste sentido, percebe-se que o uso do ciberespaço para realização de ataques cibernéticos vem preocupando os responsáveis pela segurança estratégica, principalmente devido algumas características como:

- Baixo custo de acesso aos recursos, basicamente um microcomputador e uma conexão com a internet;

- Dificuldade de identificar precisamente um atacante;

- Capacidade de originar múltiplos ataques simultaneamente, independentemente da localização do alvo ou do atacante;

- Dificuldade de delimitar fronteiras na realização de operações para proteção;

- Deficiência de normatizações específicas.

Considerando o contexto acima, este artigo objetiva analisar como a segurança cibernética das IFCs brasileiras é tratada no âmbito da Política Nacional de Defesa, buscando com isso compreender melhor como é delineada a governança cibernética pelo Governo Federal. A análise desenvolvida procura responder as seguintes questões: Um ataque cibernético a uma infraestrutura crítica poderia desencadear alguma crise que geraria impactos maiores ou até mesmo em outros setores? Como a segurança e a defesa cibernética podem atuar nestas condições? Para isso, é apresentando os normativos e legislações pertinentes, um breve diagnóstico da maturidade da capacidade de cibersegurança do Brasil e impactos de ataques cibernéticos em IFCs.

O método de abordagem empregado à realização do trabalho foi o dedutivo, o qual, segundo Prodanov (2013) utiliza premissas gerais já afirmadas buscando novas proposições. A partir da discussão sobre o tema, será possível adotar ou discordar de ideias e afirmações tecidas no texto. A conclusão do estudo apresentará a linha de pensamento adotada por seu autor utilizando-se a revisão bibliográfica desenvolvida.

A próxima seção dedica-se a apresentação de alguns conceitos e definições acerca do tema. A seção 3 aborda os principais normativos nacionais relacionados à segurança cibernética. Na seção seguinte é realizado um diagnóstico da segurança cibernética e evidenciado os principais riscos de segurança cibernética com ênfase nas infraestruturas críticas. Por fim, nas conclusões, são apresentadas algumas ações estruturantes, necessárias para melhorar a proteção das IFCs, bem como sugestões para trabalhos futuros.

2 CONCEITOS E DEFINIÇÕES

Com intuito de nivelar o entendimento sobre os principais termos relacionados à temática de segurança cibernética e consequentemente deste artigo, será apresentada uma breve descrição destes termos.

2.1 ESPAÇO CIBERNÉTICO

O espaço cibernético pode ser definido como um espaço virtual, composto por dispositivos computacionais conectados em redes ou não, no qual transitam, processam-se e armazenam-se informações digitais, essenciais para garantir o funcionamento dos sistemas de informações, de gerenciamento e de comunicações, dos quais depende parcela significativa das atividades humanas. A natureza dinâmica do ciberespaço se baseia na conectividade.

Diferentemente dos espaços terrestre, marítimo e aéreo, que são físicos e concretos, o espaço cibernético é uma dimensão virtual da realidade, uma dimensão intangível e abstrata. Além disso, o ciberespaço se distingue dos demais pelo fato de ter sido criado pelo próprio homem, constituído de forma a atender as demandas e necessidades do ser humano, enquanto os espaços tradicionais foram ao longo do tempo sendo modificados à medida que as necessidades eram demandadas.

Outra característica do espaço cibernético é a transversalidade, o qual transpassa todos os demais espaços geográficos, por exemplo, por ele controlamos os satélites, os trilhos de metrô e os radares marítimos e tudo isso torna esse espaço mais vasto amplo do que a própria Internet e utilizado pelos seres humanos (OLIVEIRA et al., 2017).

2.2 SEGURANÇA DA INFORMAÇÃO

Em um nível mais elevado sobre a segurança no espaço cibernético está a Segurança da Informação, área sistêmica e diretamente relacionada à proteção de um conjunto de informações e ao valor que estas possuem para um indivíduo ou para uma organização. Desse modo, a Segurança da Informação abrange a Segurança Cibernética, a Defesa Cibernética, a segurança física, a proteção de dados e objetiva viabilizar e assegurar a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações (E-CIBER, 2019).

2.3 SEGURANÇA CIBERNÉTICA

A segurança Cibernética visa assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação (redes de comunicações e de computadores e seus sistemas informatizados) e suas

infraestruturas críticas (BRASIL, PORTARIA Nº 45 SE-CDN, 2009; BRASIL, GSI/PR, 2010). O termo abrange também a interação com órgãos públicos e privados envolvidos no funcionamento das IFCs nacionais, especialmente os órgãos da Administração Pública Federal – APF.

2.4 DEFESA CIBERNÉTICA

A defesa cibernética, no âmbito militar, constitui-se de atuações de defesa, de exploração e de ofensividade, ocorridas no espaço cibernético. O intuito dessas operações é a proteção dos sistemas de informações, levantamento de informações para fins de inteligência, bem como a neutralização dos recursos dos adversários, ou seja, uma Guerra Cibernética propriamente dita (CARVALHO, 2011).

2.5 RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

É o potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização (NC 10 – GSI-PR, 2012).

2.6 INFRAESTRUTURAS CRÍTICAS

O conceito de infraestrutura crítica no Brasil é definido, precisamente, pelo art. 2º da Portaria nº 2 do Gabinete de Segurança Institucional da Presidência da República – GSI/PR de 8 de fevereiro de 2008. Segundo a referida portaria, “Consideram-se Infraestruturas Críticas – IFCs, as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional” (PORTARIA Nº 45 GSI/PR, 2009).

O art. 3º da citada portaria elenca, entre os incisos I e V, as áreas prioritárias das infraestruturas que estão relacionadas à energia, à água, à rede de transporte, às telecomunicações e às finanças, sem prejuízo de outras que porventura vierem a ser definidas.

A “Segurança das Infraestruturas Críticas” é definida como o conjunto de medidas, de caráter preventivo e reativo, destinadas a preservar ou restabelecer a prestação dos serviços relacionados às IFCs.

2.7 ATAQUES CIBERNÉTICOS

Um ataque cibernético é qualquer tipo de manobra ofensiva para invadir um computador ou sistema. Abaixo é citado alguns dos principais tipos de ataques cibernéticos:

Negação de serviço é um ataque que inunda um servidor, um computador ou uma rede com um volume de tráfego de dados grande o suficiente para que os mesmos não consigam realizar suas funções, ficando indisponíveis para o usuário.

Ransomware é um tipo de ataque cibernético que restringe o acesso pelo atacado ao sistema ou informação afetados, cobrando um resgate para que o acesso seja restituído.

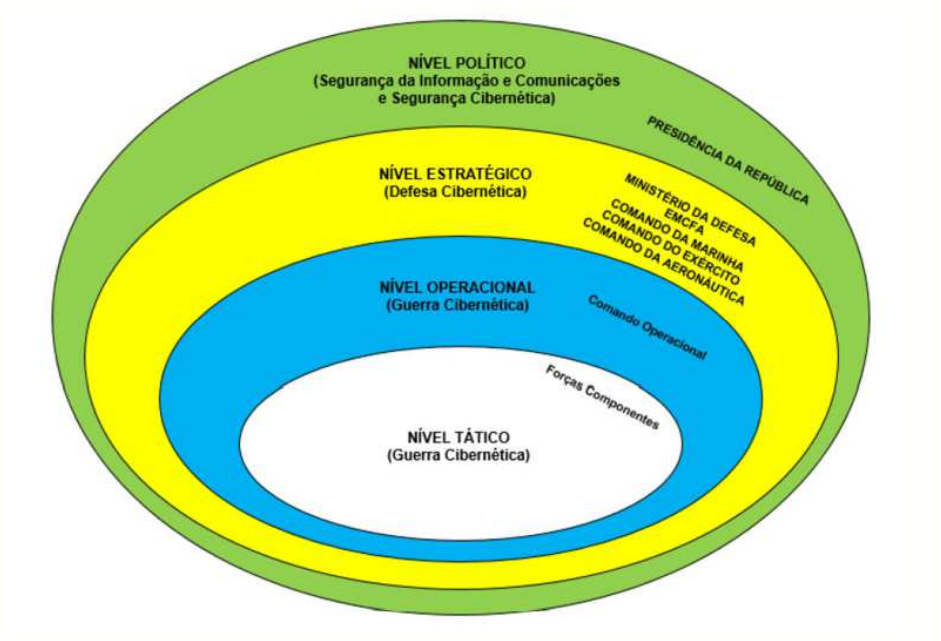
Ciberespionagem ou espionagem cibernética são ações que fazem uso não autorizado de meios de comunicação, principalmente a internet, para realizar espionagem. A espionagem é a prática ou ação para obtenção de informações secretas de competidores, rivais ou inimigos, sem autorização destes, com objetivo militar, político ou econômico. A ciberespionagem envolve tanto Estados quanto organizações e entes privados. De acordo com Möckly (2012), também pode ser considerado ciberespionagem as ações com finalidade de se testar a configuração e os sistemas de defesa de um determinado computador.

Defacement ou desfiguração de página é um tipo de ataque que consiste em alterar o conteúdo de um w*ebsite*. Este tipo de ataque é muito utilizado por hacktivistas para promover algum tipo de ideologia.

3 ARCABOUÇO NORMATIVO NO SETOR CIBERNÉTICO

No Brasil, a gestão sobre as ações no espaço cibernético é dividida em quatro níveis: o político, coordenado pela Presidência da República que abrange administração federal e os órgãos decisórios de caráter público, responsável pela segurança cibernética; o estratégico, coordenado pelo MD, Estado maior e conjunto de Comando das Forças Armadas, responsável pela defesa cibernética; e os níveis operacional e tático, sobre a coordenação exclusiva das forças armadas, responsável em caso de guerra cibernética. Os níveis podem ser representados conforme a figura 1. Serão discorridos nesta seção as principais normatizações e leis relacionadas ao setor cibernético.

Figura 1- Nível de Decisão das Ações no Espaço Cibernético



Fonte: Doutrina Militar de Defesa Cibernética (2014, p. 17).

3.1 POLÍTICAS E ESTRATÉGIAS

O planejamento para o setor cibernético começou a ser pensado com o desenvolvimento de alguns documentos que são de grande importância para a soberania tais como o Livro Verde: Segurança Cibernética no Brasil, o Livro Branco de Defesa Nacional, a Política Nacional de Defesa – PND e a Estratégia Nacional de Defesa – END, introduzindo então a questão cibernética como fonte de domínio para garantia de soberania do Brasil e definindo o setor cibernético como um dos três setores estratégicos para a Defesa e o desenvolvimento nacional.

O "Livro Verde: Segurança Cibernética no Brasil", foi um dos primeiros documentos oficiais a tratar o tema da Segurança Cibernética no Brasil. Ele foi publicado em 2010 pelo Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República – GSI/PR, e teve como objetivo expressar potenciais diretrizes estratégicas para o estabelecimento da Política Nacional de Segurança Cibernética (LIVRO VERDE, 2010).

Em 2012, foi lançado o Livro Branco de Defesa Nacional – LBDN. Ele trouxe em seu bojo as atividades ministradas para a proteção do País, inclusive, as relacionadas ao Setor Cibernético, com intuito de informar aos próprios cidadãos e as outras nações os procedimentos aplicados em prol da segurança e o uso das Forças Armadas como base de defesa do Estado.

No mesmo ano foram publicados a Política Nacional de Defesa – PND, uma atualização da Política de Defesa Nacional – PDN de 2015 e a respectiva Estratégia Nacional de Defesa –

END. A PND exterioriza os objetivos almejados para garantir a Defesa Nacional, definida como "o conjunto de atitudes, medidas e ações do Estado, com ênfase na expressão militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas" (PND-END, 2012).

Por sua vez, a END orienta os segmentos do Estado Brasileiro quanto às medidas que devem ser implementadas para que os objetivos da PND sejam alcançados. Para cada Estratégia de Defesa são incorporadas Ações Estratégicas de Defesa – AED, que visam orientar as medidas que deverão ser implementadas no sentido da consecução dos Objetivos Nacionais de Defesa. Dentre as mais de 80 AED, destacam-se 5 relacionadas ao setor cibernético:

AED-1 - Desenvolver os setores estratégicos de defesa (nuclear, cibernético e espacial);

AED-2 - Contribuir para o incremento do nível de segurança das Estruturas Estratégicas;

AED-9 - Desenvolver as capacidades de monitorar e controlar o espaço aéreo, o espaço cibernético, o território, as águas jurisdicionais brasileiras e outras áreas de interesse;

AED-10 - Incrementar as capacidades de defender e de explorar o espaço cibernético;

AED-69 - Promover o desenvolvimento da tecnologia cibernética.

A Portaria Normativa nº 3.389 do MD, aprovada em 21 de dezembro de 2012, instituiu a Política Cibernética de Defesa, que objetiva nortear, no contexto do MD, as ações de Defesa Cibernética, suportando o nível estratégico, e as ações de Guerra Cibernética, nos níveis operacional e tático, visando à consecução dos Objetivos Nacionais de Defesa (BRASIL, 2012).

Diante do exposto, vislumbra-se que o Estado deverá atuar em todas as instâncias para garantir a segurança nacional, entre eles, o Setor Cibernético, observando a proteção das IFCs, o aprimoramento de métodos e processos que diminuam a vulnerabilidade dos sistemas que estejam envoltos pela defesa nacional em face de ataques cibernéticos. Nesse aparato, sustenta-se que esse setor também deverá abranger a Tecnologia da Informação e Comunicações – TIC, assim, o Setor Cibernético deverá atuar no que tange a "Estrutura de comando, controle, comunicações, computação e inteligência [...] para a atuação operacional [...] das Forças Armadas, recursos de TIC e arquitetura matricial que viabilize o trânsito de informações em apoio ao processo decisório em tempo quase real (CARVALHO, 2011, p. 9).

Em 2015, a Presidência da República, juntamente com 16 órgãos da esfera federal, publicou o documento "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015/2018, versão 1.0" com o objetivo de fortalecer as ações de Segurança da Informação e de Segurança Cibernética na Administração Pública Federal – APF, melhorar a segurança das IFCs e dos serviços nacionais.

A estratégia trouxe uma compilação de objetivos estratégicos visando direcionar as ações referentes a segurança da informação, das comunicações e de segurança cibernética, enfatizando a atuação coordenada dos atores envolvidos para o aperfeiçoamento da área governamental e diminuição dos riscos que a sociedade e as organizações possam estar expostas (ESTRATÉGIA DE SIC, 2015).

No ano seguinte, em junho de 2016, por meio do decreto nº 8.793 foi publicada a Política Nacional de Inteligência. Esta política também enfatiza que os ataques cibernéticos são ameaças com potencial capacidade para pôr em perigo a integridade da sociedade e do Estado e a segurança nacional do Brasil e tem ainda como uma de suas diretrizes a expansão da capacidade operacional da Inteligência no espaço cibernético (BRASIL, 2016).

Em 26 de dezembro de 2018 foi publicada por meio do Decreto nº 9.637 a Política Nacional de Segurança da Informação – PNSI, a qual dispõe sobre princípios, objetivos, instrumentos, atribuições e competências de segurança da informação para os órgãos e Entidades da Administração Pública Federal – APF, sob o prisma da governança. Dentre as suas diretrizes pode-se destacar o Art.8º, que trata da instituição do Comitê Gestor da Segurança da Informação e os Art.12º e Art. 13º que definem as competências acerca do tema, cabendo ao GSI/PR a gestão da segurança da informação e consequentemente da segurança cibernética e ao MD, atuar mais focado na defesa cibernética bem como apoiar o GSI/PR na segurança cibernética. O Art.15º aborda as atribuições dos órgãos da APF, que dentre várias destaca-se a ênfase que os mesmos devem realizar a governança da segurança da informação no âmbito de sua atuação.

No mesmo ano, foi constituído um grupo de trabalho para revisar a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal – 2015/2018, citada acima. Em cumprimento ao estabelecido na PNSI, a nova versão da estratégia, será composta por pelo menos cinco módulos: segurança cibernética, defesa cibernética, segurança das infraestruturas críticas, segurança da informação sigilosa e proteção contra vazamento de dados. Considerando a Segurança Cibernética como a área mais crítica e atual a ser abordada, o GSI/PR elegeu em janeiro de 2019, a Estratégia Nacional de Segurança Cibernética – E-CIBER, o primeiro módulo a ser elaborado para a nova Estratégia Nacional de Segurança da Informação – ENSI.

Ainda em 2018, por meio do Decreto nº 9.573 de 22 de novembro de 2018 foi instituída a Política Nacional de Segurança das Infraestruturas Críticas Nacionais – PNSIC. Ela tem como objetivo estabelecer diretrizes para salvaguardar as IFCs consideradas indispensáveis à segurança nacional. Essas diretrizes visam prevenir uma eventual interrupção, total ou parcial,

das atividades ou serviços relacionados às IFCs ou, no caso de ocorrer uma interrupção, minimizar os impactos resultantes. A PNSIC estabelece ainda, como instrumentos para sua operacionalização, a Estratégia Nacional de Segurança de Infraestruturas Críticas, o Plano Nacional de Segurança de Infraestruturas Críticas e o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas (BRASIL, 2018).

Em seus princípios e objetivos, a PNSIC menciona a salvaguarda do interesse da defesa e da segurança nacional bem como a prevenção e a precaução, com base em análise de riscos. Dessa forma, se pode deduzir que a segurança cibernética tem caráter fundamental para continuidade da prestação dos serviços dessas organizações, tão relevantes para a nação brasileira (BRASIL, 2018).

3.2 NORMATIVOS JURÍDICOS

No contexto jurídico, o Brasil avançou com a promulgação de algumas leis que possibilitam apenar grupos ou pessoas que cometem os ataques cibernéticos. Em 30 de novembro de 2012 foi publicada a Lei dos Crimes Cibernéticos, Lei nº 12.737, conhecida como "Lei Carolina Dieckmann". Ela traz a tipificação do agente infrator quanto a invasão de sistemas computacionais, roubo de senhas, invasão de computadores, quebra de dados e vazamento de informações pessoais de outros usuários. Adicionalmente, a Lei nº 12.735, de 30 de novembro de 2012 trouxe a criação de delegacias que atuem exclusivamente no combate aos crimes digitais (BRASIL, 2012).

Em 23 de abril de 2014, foi promulgada a Lei nº 12.965, Marco Civil da Internet, que traz em seu escopo a regulamentação do uso da Internet no Brasil baseando em princípios, garantias, direitos e deveres àqueles que utilizam a rede mundial de computadores. Além disso, dispõe sobre orientações das quais o Estado deverá atuar, como por exemplo, na segurança de dados pessoais e da privacidade de usuários que utilizam o ambiente virtual. Cabe ressaltar que essa normatização deixa abertura para a inclusão de dispositivos, sejam estes voltados a governança da rede, negócios eletrônicos, crimes cibernéticos, cidadania digital, dentre outros (BRASIL, 2014).

No ano passado, em 14 de agosto de 2018, foi publicada a Lei Geral de Proteção de Dados – LGPD, Lei nº 13.709, que disciplina sobre o tratamento dos dados pessoais, inclusive, pelos meios digitais. Ela trouxe alterações que acarretaram a necessidade de investimentos, por parte das organizações, em novas estruturas e criação de normas internas adequadas a segurança de dados pessoais. Recentemente, a lei supracitada recebeu novos dispositivos e alterações,

advindos da Lei nº 13.853, de 8 de julho de 2019, criando a Autoridade Nacional de Proteção de Dados (BRASIL, 2019).

Além dessas leis, o governo está elaborando um projeto de Lei Geral de Segurança da Informação, com pretensão de apresentá-lo até o final de 2019.

4 DIAGNÓSTICO DA SEGURANÇA CIBERNÉTICA

No ano de 2018, cerca de 4,1 bilhões de usuários acessaram a *internet*, o que representa 54% da população mundial e, dentre essa porcentagem, 93% dos usuários fizeram uso via dispositivo móvel (GLOBAL DIGITAL, 2019).

Em 2020, foi previsto que a rede mundial de computadores estará interligada com mais de 30 bilhões de dispositivos com internet das coisas (*Internet of Things – IoT*), da qual não se trata apenas de internet para pesquisa, e sim de uma infinidade de ações, como a produção de conteúdo, interação com objetos, entre outros apetrechos, o que trará maior variedade na oferta de produtos e serviços ao usuário (E-CIBER, 2019).

Se por um lado, toda essa interação cibernética traz conforto, multiplicidade e celeridade nos serviços *on-line*, por outro, o usuário poderá sofrer impactos com a possível fragilidade desses sistemas, que podem sofrer ameaças e ataques cibernéticos ocasionando prejuízos de várias escalas, seja para um usuário comum ou para grandes instituições e organizações, levando a repensar na confiabilidade que esses produtos podem realmente oferecer.

O Relatório da *Internet Organised Crime Threat Assessment – IOCTA*, de 2018, organizado pela Agência da União Europeia para a Cooperação Policial – Europol, afirma que na América Latina, o Brasil é a nação que mais sofre ataques cibernéticos e que 54%, supostamente, ocorrem dentro do próprio país. É também a principal fonte dos ataques *on-line* da América Latina. O Brasil está no rol dos dez países que dão origem a ciberataques, os quais duplicaram de 2017 para 2018 e uma das causas do crescente número de ataques é a normatização brasileira fragilizada quanto aos crimes cibernéticos (E-CIBER, 2019).

Em uma pesquisa desenvolvida pela Consultoria JLT no Brasil (2017), com o público-alvo de 200 empresas de grande e médio porte, constatou-se que 55,4% destas empresas são praticamente dependentes de tecnologia, enquanto 35% podem sofrer interrupções de seus serviços se acaso sofrer algum problema em seus processos que envolvem o uso de tecnológicas e sistemas de ordem tecnológica. Assim a pesquisa *Cyber Review* indicou que 80% do público informaram que, caso ocorra um ciberataque, a organização sofreria problemas na sua operacionalização, enquanto 34% afirmaram que já passaram por alguma forma de ataque no

último ano e desse total, 29% vivenciaram os problemas operacionais resultantes desses ataques, ou seja, 10% do total dos entrevistados.

Em um estudo da *Tempest/EZ- Security* (2019), em torno de 50% das empresas entrevistadas aduzem que têm gastos anuais quanto a segurança de seus sistemas de informação, de aproximadamente 2% de seu faturamento ao ano, enquanto 34,5% investem até 1% de seu faturamento anual com a segurança da informação.

Em outra pesquisa realizada pela *JLT CyberView*, no ano de 2017, 35% das empresas entrevistadas citaram que não possuem planos ou diretrizes a serem seguidas no que se refere a segurança cibernética. Em 2019, apenas 44,2% disseram que não incluíram em seus orçamentos uma previsão de gastos caso passem por alguma crise e, muito menos não possuem plano de contingência (*TEMPEST/EZ-SECURITY*, 2019)

A violação de sistemas de computadores se tornou uma constante e gera riscos para o sistema econômico brasileiro. A figura 2 ilustra o potencial desses riscos, apresentando uma consolidação estatística do Brasil em relação a Segurança Cibernética. Nos tópicos seguintes, são citados alguns exemplos de ataques reais em organizações internacionais, nacionais e a infraestrutura de defesa cibernética do Brasil e em seguida, alguns riscos de ciberataques em infraestruturas críticas.

Figura 2. Consolidação de dados estatísticos do Brasil em Segurança Cibernética

Fonte: Estratégia Nacional de Segurança Cibernética (2019).

4.1 ATAQUES CIBERNÉTICOS EM INFRAESTRUTURAS CRÍTICAS NO EXTERIOR

Entre alguns dos ataques cibernéticos ocorridos recentemente, em junho de 2017, o conglomerado de negócios dinamarquês *Maersk* sofreu ataques cibernéticos do *malware Not Petya*, um tipo de *ransomware*, que gerou cerca de US$ 300 milhões de prejuízo. O *ransomware* utilizado não permitia que os usuários acessassem seus próprios dados, o que afetou as operações da empresa. O ataque ocorreu devido a vulnerabilidades de segurança existentes no *Windows* em que o antivírus não protegeu o sistema (NOVET, 2017).

Em 2016, a Ucrânia sofreu ataques de hackers russos, conhecidos como *Fancy Bear*, comprometendo a própria infraestrutura do país. As ações desses ataques cibernéticos derrubaram as redes de energia, além de conseguirem rastrear a localização de armamentos ucranianos. Os ataques utilizavam *malwares* enviados por *e-mail*, que copiavam senhas e *logins*. Apesar dos ataques ocorrerem no Leste Europeu, o Ocidente não está isento de passar por este mesmo problema futuramente (CONDILIFFE, 2016).

Em agosto de 2012, um *cyber* ataque ocorreu na petrolífera *Saudi Aramco* atingindo trinta mil estações de trabalho. Após dez dias, a empresa conseguiu restaurar parte de seus serviços. O grupo *Cutting Sword of Justice* (Espada da Justiça) assumiu a responsabilidade pelos ataques e esclareceu que o ato foi uma retaliação contra o regime *Al Saud*. O grupo utilizou o *malware Shamoon*, o qual pode destruir arquivos dentro do sistema, impossibilitando a inicialização de máquinas *Windows* infectadas (LEYDEN, 2012).

No ano de 2010 ocorreu um ataque cibernético, reconhecido como *Stuxnet*, contra uma usina localizada em *Natanz*, no Irã, que manipulava urânio para fins médicos e produção de energia. O *malware* utilizado tinha uma configuração diferenciada e alcançou seus objetivos rapidamente, explorando falhas desconhecidas do sistema e se espalhando por toda a rede. O código do *malware* se copiava e infectava os computadores ligados ao compartilhamento dessa rede de forma quase imperceptível. O alvo do ataque foram os computadores de controle industrial e consistia em alterar a frequência das centrífugas de enriquecimento de urânio discretamente, o que foi descoberto posteriormente, provocando aquecimento das mesmas e acabando por inutilizar o maquinário devido as falhas geradas. O *malware Stuxnet* atuava de forma inteligente com capacidade de alto nível de alcance dentro do sistema (MASON, 2017).

O *Triton*, está entre um dos piores *malwares* criados para atacar os sistemas de segurança industriais. Sua função era parar uma indústria de energia no Oriente Médio em 2017. Com grande potencial ofensivo, o *malware* pode desabilitar os sistemas de segurança projetados para evitar acidentes industriais catastróficos, por exemplo os controladores do Sistema de Segurança Instrumentado Triconex (SIS), amplamente usado na indústria de energia para fazer

o monitoramento de sistemas críticos e promover ações imediatas caso algum problema seja detectado. O *Triton* se tornou uma ameaça real a infraestruturas de sistemas críticos pois pode ter acesso remoto e trazer danos físicos, além de acessar controles e desligar operações industriais, causando prejuízos de grande extensão (WEI, 2017).

No ocidente, os ataques cibernéticos aos EUA são constantes. A cidade de Atlanta, por exemplo, passou por ataques durante duas semanas, o que ocasionou um prejuízo de quase US$ 3 milhões. Além dessa cidade, Baltimore, Charllote, Dallas e São Francisco também foram alvos em 2017, episódio que ocorreu durante a implantação de novos sistemas operacionais, com estruturas inteligentes, que apresentaram falhas devido ao despreparo na aplicação das atualizações de segurança desses novos sistemas, resultando em vulnerabilidade (EREZ, 2018).

4.2 ATAQUES CIBERNÉTICOS NO BRASIL

Em junho de 2013, Edward Snowden, um ex-agente da *National Security Agency – NSA*, revelou que os Estados Unidos possuíam um programa de vigilância denominado *Prism* cujo objetivo era coletar comunicações da rede oriundas de grandes companhias de internet sediadas nos Estados Unidos. Entre as denúncias de Snowden, o governo e empresas do Brasil estariam entre os alvos da espionagem norte-americana (PIERRE, VITELLI, 2018).

Em 2014, *hackers* realizaram uma série de ataques ao sistema do Ministério das Relações Exteriores – MRE. Por meio da técnica de *phishing* (captação de informações de uma pessoa ou grupo através do envio de mensagens de correios eletrônicos fraudulentas) os *hackers* tiveram acesso a diversas mensagens sigilosas, comprometendo cerca de 1.500 diplomatas brasileiros.

Um outro caso ocorreu em 2015, quando *hackers* invadiram o sistema do Exército Brasileiro e divulgaram na internet dados de mais de 7 mil militares. Este caso teria sido motivado por uma represália às técnicas utilizadas pela instituição durante um exercício de jogos cibernéticos promovido pelo Centro de Defesa Cibernético – CDCiber, organização militar subordinada ao Comando de Defesa Cibernético – ComDCiber.

Outro ataque ocorreu em 2017 contra o setor energético, no qual foi feito um *defacement* (modificação da página) na *website* da Agência Nacional de Energia Elétrica – ANEEL, como forma de protesto devido ao aumento das tarifas de energia elétrica, expondo o poder de atuação do grupo de *hackers*.

4.3 ESTRUTURA DE DEFESA CIBERNÉTICA DO BRASIL

Em agosto de 2010 foi criado o Núcleo do Centro de Defesa Cibernética, vinculado ao Exército Brasileiro. Em setembro de 2012 foi ativado o Centro de Defesa Cibernética – CDCiber, que tem por finalidade a execução das atividades operacionais e de inteligência no âmbito do Sistema Militar de Defesa Cibernética. Atualmente o CDCiber é um órgão subordinado ao Comando de Defesa Cibernética – ComDCiber.

O ComDCiber é uma organização militar conjunta, na estrutura organizacional do Comando do Exército, ativada em 15 de abril de 2016 e soma esforços com as organizações governamentais já existentes. Tem como principais atribuições, dentre outras, planejar, orientar, supervisionar e controlar as atividades operacional, de inteligência, doutrinária, de ciência e tecnologia, bem como de capacitação no Setor Cibernético de Defesa.

Também subordinada ao ComDCiber, a Escola Nacional de Defesa Cibernética – EnaDCiber tem por missão fomentar e disseminar as capacitações necessárias à Defesa Cibernética, no âmbito da Defesa Nacional, nos níveis de sensibilização, conscientização, formação e aperfeiçoamento. Ela foi inaugurada oficialmente em fevereiro de 2019, apesar de já estar funcionando como núcleo desde 2015.

Como o objetivo de potencializar a Defesa Cibernética Nacional, foi lançado em 2011 o Programa de Defesa Cibernética na Defesa Nacional – PDCDN. Ele tem como premissas a atuação conjunta e a interoperabilidade entre as forças para assegurar o uso efetivo do espaço cibernético pelo MD e pelas Forças Armadas – FA e impedir ou dificultar sua utilização contra os interesses da Defesa Nacional. Objetiva ainda aglutinar as iniciativas do setor Cibernético na área de Defesa Nacional e contribuir para dotar a Defesa Nacional com a infraestrutura necessária para desenvolver todo o espectro de ações cibernéticas, visando proteger e defender os ativos de informação do MD e das FA.

A fim de contribuir com os objetivos da a Política Cibernética de Defesa, o ComDCiber estabeleceu um link direto com as Agências Reguladoras Nacionais, caracterizando a interação entre o Sistema Militar de Defesa Cibernética e o Sistema Nacional Integrado de Segurança das Infraestruturas Críticas, ampliando a capacidade de neutralização ou mitigação de ameaças cibernéticas.

Por ocasião do planejamento para a realização dos Grandes Eventos no Brasil, como a Conferência Rio+20 em 2012, a Jornada Mundial Juventude em 2013, a Copa do Mundo de 2014 e os Jogos Olímpicos de 2016, o Brasil teve uma experiência em securitização do problema da segurança cibernética, através de ampla atuação da defesa cibernética. Nesse contexto, as IFCs foram consideradas como objetivos a se proteger durante a realização desses

eventos, devido a percepção da realidade ameaçadora e da alta probabilidade de ocorrência. Para tanto, o propósito estabelecido foi garantir a continuidade da prestação dos serviços mesmo em situações de crise.

Ocorre que grande parte dos sistemas que compõe as IFCs são dependentes de evoluções tecnológicas computacionais e possuem interconexões com redes públicas e privadas de tal forma que são vulneráveis às diversas ameaças, entre elas: fraudes eletrônicas, espionagem, sabotagem, códigos maliciosos, *hackers,* vandalismo, fogo, inundação, *blackouts* e etc. Além disso, o processo de planejamento de uma IFC envolve diferentes atores como o governo em todas as esferas, a iniciativa privada como operadora e a população como usuária. Para lidar com essa complexidade, faz se necessário uma organização central para exercer o comando e controle, exigindo comprometimento e ações de todo os envolvidos. Em situações de crise e nos casos de securitização este papel no nível político é conduzido pelo GSI/PR, que coordena grupos técnicos formados com outros órgãos públicos, como por exemplo, ministérios, agências reguladoras, autarquias federais e etc., de acordo com o tema das IFCs. No caso dos grandes eventos a coordenação e integração da segurança e defesa cibernéticas ficaram a cargo do ComDCiber.

Já no âmbito das ações diplomáticas, e com base na experiência em grandes eventos, o Brasil, como apoio da equipe do ComDCiber, apoiou o Peru nas ações de combate aos crimes cibernéticos durante os Jogos Pan Americanos de Lima 2019. Este tipo de ação fortalece a cooperação entre países para investigação e combate a estes crimes.

4.4 RISCOS DE CIBERATAQUES PARA AS INFRAESTRUTURAS CRÍTICAS

Os riscos de ciberataques contra organizações são reais e de diversos tipos, como por exemplo, ataques de *phishing* (utilizam *e-mails* ou *websites* falsos para coletar informações do usuário), ataques de *ransomware*, negação de serviço em larga escala, vazamentos de dados, espionagem, terrorismo cibernéticos e a interrupção de serviços.

Quanto mais as organizações trabalham com estruturas interligadas, mais estarão sujeitas a serem alvos de ataques, pois uma interconexão global poderá apresentar maior fragilidade em sua segurança. Diante do aumento dos ciberataques, as empresas, principalmente as que fazem parte da IFCs, necessitam implementar maior segurança aos seus sistemas de informação diante da disseminação de *malwares*, ataques de *hackers* e hacktivistas e de ações estatais adversas (E-CIBER, 2019).

Os ataques cibernéticos são um dos problemas que um estado-nação pode enfrentar diante do atual cenário. Os níveis de ataques podem ser de pequena escala, advindos de fontes

imprecisas, por exemplo, por meio de redes sociais, mas que trazem grandes problemas aos interesses nacionais. Além disso, os ataques podem ser combinados e de grande escala, podendo derrubar serviços essenciais de um país. Portanto, os níveis e a gravidade em torno da guerra da informação podem ser variados. A capacidade de conter possíveis ataques e garantir sua própria segurança será colocado em prova diante dos "conflitos do futuro".

No contexto das novas guerras, um ataque não necessariamente pode ter o objetivo de gerar efeitos físicos. É interessante para o agressor restringir o uso da força de modo que permaneça abaixo do nível do conflito armado, uma vez que se acredita que a guerra armada clássica é arriscada e cara. Neste caso, a tecnologia cibernética permite que várias situações de atrito sejam criadas abaixo do limiar da violência, criando uma lacuna entre a paz e uma guerra declarada. Em vez de violência física, os conflitos no ciberespaço buscam o controle da população por coerção, com ações direcionadas contra civis. Essas mudanças têm contribuído para que os ataques cibernéticos aumentem cada vez mais (COLLIER, 2017).

Dessa forma um ataque cibernético pode ser usado para invadir infraestruturas críticas de um Estado e afetar civis diretamente, como por exemplo, o ocorrido aos computadores dos operadores do sistema elétrico na Ucrânia, que provocou a interrupção do fornecimento de energia em grande parte da capital Kiev por algumas horas. O objetivo era deixar a população sem eletricidade em um dos períodos mais frios do ano. O blecaute poderia ter persistido por até uma semana se determinados recursos do *malware* tivessem sido executados. Os investigadores não conseguiram identificar claramente a origem dos ataques, mas na ocasião o presidente da Ucrânia acusou a Rússia de estar em Guerra Cibernética contra o seu país. Os pesquisadores supõem que os hackers estariam testando uma espécie mais evoluída de todos os *malwares* de sabotagem até hoje encontrados, e que sua adaptabilidade o torna uma ameaça não apenas à infraestrutura crítica ucraniana, mas também às redes de energia em todo o mundo (ARIMURA, 2016).

Empresas do setor de energia podem ser vítimas tanto de ataques cibernéticos gerais, que não tem como alvo uma empresa ou setor específico, como ataques bastante específicos, que tem como objetivo atingir o sistema elétrico ou uma empresa específica do setor. As consequências desses ataques virtuais vão desde roubos de dados e fraudes no faturamento até danos a equipamentos de infraestrutura, podendo inclusive comprometer o fornecimento de energia elétrica.

Além do risco para cada empresa específica, a interconexão do sistema elétrico pode multiplicar os danos causados por um ataque cibernético em uma delas. Um ataque bem coordenado, focado nos elos mais fracos do ponto de vista de segurança, pode causar um efeito

dominó amplificando as dimensões dos danos. Um ataque dessa natureza pode provocar a interrupção no fornecimento de energia de um país inteiro, causando transtornos para a sociedade, com impactos em serviços vitais, como escolas, hospitais e segurança pública,

Outra forma de ataque é o hacktivismo, que seria o ativismo *online* com a ação de *hacking,* com intuito de manifestar sobre determinado assunto que esteja se contrapondo ao interesse público, podendo desestabilizar a instituição que for alvo (ARIMURA, 2016).

Os hacktativistas no Brasil utilizam técnicas realizadas em ações ocorridas em outros países, não existindo indicativos de que os ataques cometidos por eles no país tenham sido financiados por outros Estados.

Diante do exposto, pode-se inferir que apesar dos crimes cibernéticos ocorridos no Brasil terem características de ataques menos impactantes, como *scan* (varredura de rede), *phishing* (envio de falsos *e-mails* e mensagens), *defacement* e até mesmo espionagem, as infraestruturas críticas do Brasil também estão expostas ao risco de ataques cibernéticos mais graves, podendo até desencadear uma crise sistêmica em todos os outros setores.

5 CONCLUSÃO

A segurança cibernética é vista de forma variada pela própria sociedade, em que não existe um nível de conscientização real sobre o problema face aos ataques, sendo por vezes menosprezado. A consequência é um baixo investimento em segurança cibernética pelas empresas.

No entanto, os ataques cibernéticos são uma realidade que se propaga ao redor do mundo e seu poder de atuação afeta grandes organizações que acumulam prejuízos milionários, alcançando ainda o próprio Estado. Atuam de forma silenciosa em alguns casos, tendo acesso aos dados, quebrando barreiras, controlando serviços essenciais, destruindo a imagem do Estado e colocando vidas em risco.

Uma forma de se apenar grupos ou pessoas que cometem tais ataques seria uma normatização internacional em que todos os países-membros de acordos e tratados aceitassem as medidas a serem impostas, fato que ainda não é acolhido por todos os países.

O Brasil é um exemplo de Estado que não possui uma normatização bem estruturada para conter o aumento incessante do número de ciberataques. O Estado possui diretrizes gerenciais para a contenção de ataques, mas, ainda tem aspecto fragmentado, sendo fragilizado quanto ao seu poder de ação, gerando retrabalho em processos que ocorrem rotineiramente. A aprovação da Lei Geral de Segurança da Informação, por exemplo, poderá trazer avanços neste sentido.

Diante do exposto, suscita-se a necessidade de um advento de legislação que se adeque a realidade brasileira no quesito de proteção dos sistemas, das redes governamentais e principalmente das infraestruturas críticas, visto que os serviços suportados por esses recursos não podem ser interrompidos.

No que se refere à Administração Pública e organizações públicas e privadas, essas entidades deveriam constituir processos de segurança cibernética com uma análise periódica de acordo com a evolução tecnológica, sendo necessário instaurar procedimentos aperfeiçoados, ofertar capacitação contínua e treinamento aos colaboradores.

Apesar de muitas empresas não adotarem investimentos em prol de sua segurança cibernética, esta é uma medida necessária, principalmente nas definidas como IFCs, além de gerenciamento de riscos e de ações contra incidentes, observando ainda, as próprias vulnerabilidades do sistema utilizado. O planejamento orçamentário adequado para a segurança cibernética poderá ser um meio de se estruturar e prevenir possíveis ataques nessas organizações.

Dessa forma, para se opor aos impactos de possíveis ataques cibernéticos, é essencial aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação ou mesmo aqueles que permitam seu pronto restabelecimento.

Ressalta-se, por fim, o quão fundamental para o Estado é o envolvimento de todas as instâncias para o incremento do nível de segurança das infraestruturas críticas e para o aperfeiçoamento de respectiva normatização, destacando-se a necessidade de fortalecimento da interação entre os órgãos e entidades da APF e setores envolvidos no funcionamento das infraestruturas críticas nacionais.

No presente, um dos arquétipos de segurança utilizados que podem atender as necessidades do setor seria a implantação de um modelo centralizado de governança de Segurança Cibernética, nos moldes do SISBIN (integrado por 39 órgãos do Estado), atuando com interoperabilidade, ou seja, implementando a capacidade de vários órgãos trabalharem com sistemas computacionais que interajam de modo eficiente.

REFERÊNCIAS

ARIMURA, Mayumi. Saiba a diferença entre *Hackers, Crackers, White Hat, Black Hat, Gray Hat*, entre outros. **Portal. E-GOV**, Junho, 2016. Disponível em: <https://egov.ufsc.br/portal/conteudo/saiba-diferen%C3%A7a-entre-hackers-crackers-white-hat-black-hat-gray-hat-entre-outros>. Acesso em 10 ago, 2019.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. **DOU** em 9 jul. 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1>. Acesso em 2 set.2019.

_____. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **DOU** em 15 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato 2015-018/2018/lei/L13709.htm>. Acesso em 12 set.2019.

_____. Lei nº 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres par o uso da internet no Brasil. **DOU** em 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 2 set.2019.

_____. 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. **DOU** em 3 dez 2012. Disponível em:<http://www.planalto.gov.br/ ccivil_03/_ato2011-2014/2012/lei/l12737.htm >. Acesso em 2 set.2019.

_____. Decreto nº 9.573, de 22 de novembro de 2018. Aprova a Política Nacional de Segurança das Infraestruturas Críticas. **DOU** em 23 nov. 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm>. Acesso em 4 mai.2019.

_____. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação. **DOU** em 27 dez. 2018. Disponível em: < http://www.planalto.gov.br /ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm>. Acesso em 4 mai.2019.

_____. Decreto nº 8.793, de 29 de junho de 2016. Fixa a Política Nacional de Inteligência. **DOU** em 30 jun. 2016. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/Decreto/D8793.htm>. Acesso em 6 mai.2019.

_____. Norma Complementar nº 10/IN01/DSIC/GSIPR. Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. **DOU** 10 fev. 2012. Disponível em: <http://dsic.planalto.gov.br/ legislacao/nc_10_ativos.pdf>. Acesso em 10 set.2019.

_____. Portaria Normativa nª 3.389, de 21 de dezembro de 2012, do Ministério da Defesa. **DOU** em 27 dez. 2012.

_____. Portaria nº 45 SE-CDN, de 8 de setembro de 2009. Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e dá outras providências. Brasília, **DOU** em 9 de set. 2009. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=2&data=09/09/ 2009>. Acesso em 10 set.2019.

_____. Presidência da República. Gabinete de Segurança Institucional. **Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018: versão 1.0 /** Gabinete de Segurança Institucional, Secretaria-Executiva, Departamento de Segurança da Informação e Comunicações. – Brasília: Presidência da República, 2015.

_____. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro Branco de Defesa Nacional**. Ministério da Defesa, Brasil, 2012.

_____. 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. Organização Claudia Canongia e Raphael Mandarino Junior. – Brasília: GSIPR/SE/DSIC, 2010.

_____. Política Nacional de Defesa (PND). **Estratégia Nacional de Defesa (END).** Versão sob apreciação do Congresso Nacional (Lei complementar nº 97, de 1999, art. 9º, § 3º. Ministério da Defesa, Brasil, 2016.

_____. Política Nacional de Defesa (PND). **Estratégia Nacional de Defesa**. Ministério de Estado da Defesa. Ministério. Brasília, 2012. Disponível em: <https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf>. Acesso em 6 mai.2019.

_____. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética**. MD31-M-08. 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 4 jun. 2019.

CARVALHO, P.S.M. O Setor Cibernético nas Forças Armadas Brasileiras. *In*: **Desafios Estratégicos para a Segurança e Defesa Cibernética**. 1ª. Ed. Brasília: Presidência da República, 2011, p. 13-34.

COLLIER, J. Proxy Actors in the Cyber Domain: Implications for State Strategy. ***St Antony's International Review***, 2017. v. 13, nº 1, pp.25-47.

CONDILIFFE, Jamie. Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks. **MIT Technology Review**. December, 2016. Disponível em: <https://translate.google.com/translate?hl=pt-BR&sl=en&u=https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/&prev=search>. Acesso em 12 set.2019.

CONSULTORIA JLT. Riscos de ciberataques vão aumentar em 2018. **Inseder**, 2017. Disponível em: < file:///C:/Users/WINDOWS/Downloads/JLT_Insider_mar_BR18005.pdf>. Acesso em 4 set.2019.

EREZ, Noam. Cyber attacks are shutting down countries, cities and companies. **World Economic Forum,** June, 2018. Disponível em: <https://translate.google.com/translate?hl=pt-

BR&sl=en&u=https://www.weforum.org/agenda/2018/06/how-organizations-should-prepare-for-cyber-attacks-noam-erez/&prev=search> Acesso em 14 ago.2019.

ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA (E-Ciber). **Participa**. 2019. Disponível em: <http://www.participa.br/seguranca-cibernetica/estrategia-nacional-de-seguranca-cibernetica-e-ciber> Acesso em 18 set.2019.

GLOBAL DIGITAL POPULATION AS OF JULY, 2019 (IN MILLIONS). **Statista**, 2019. Disponível em: <https://www.statista.com/statistics/617136/digital-population-worldwide/>. Acesso em 2 ago.2019.

LEYDEN, Jonh. Security Hack on Saudi Aramco hit 30,000 workstations, oil firm admits First hacktivist-style assault to use malware? **The Register**, 2012. Disponível em: <https://translate.google.com/translate?hl=pt-BR&sl=en&tl=pt&u=https%3A%2F%2Fwww.theregister.co.uk%2F2012%2F08%2F29%2Fsaudi_aramco_malware_attack_analysis%2F&anno=2&sandbox=1>. Acesso em 12 ago.2019.

MASON, Paul. STUXNET: The day industrial control systems became a target. Secarma. November, 2017. Disponível em: <https://www.secarma.com/stuxnet-the-day-industrial-control-systems-became-a-target.html>. Acesso em 14 ago.2019.

MÖCKLI, D. **Strategic trends 2012: key developments in global affairs**. Zurich: Center for Security Studies (CSS), 2012.

MORESI, Eduardo A. D. et al. Defesa cibernética: um estudo sobre a proteção da infraestrutura e o software seguro. **Universidade Católica de Brasília**, 2012.

NOVET, jordan. Shipping company Maersk says June cyberattack could cost it up to $300 million. August, 2017. **CNBC**. Disponível em: <https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html>. Acesso em 14 ago.2019.

OLIVEIRA, Marcos Aurélio Guedes de et al. **Guia de defesa cibernética na américa do Sul**. Recife: Editora UFPE, 2017.

PIERRE, Hector Luis Saint Pierre; VITELLI, Mariana Gisela (orgs.). **Dicionário de Segurança e Defesa.** São Paulo: Unesp, 2018.

PRODANOV, Cleber Cristiano. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico**. 2. ed. Novo Hamburgo: Feevale, 2013.

SANTOS, D. B. M.; CARVALHO, B. E. F. C; CAVALCANTE, S. P. P. Segurança de Infraestruturas Críticas no Brasil. **10º Simpósio de Hidráulica e Recursos Hídricos dos Países de Língua Oficial Portuguesa**. Pernambuco, 2011.

TEMPEST/EZ-SECURITY. A. Tempest apresenta primeiro estudo do mercado brasileiro de cibersegurança. **Crypto Id**, Disponível em: <https://cryptoid.com.br/pesquisas-seguranca-da-informacao-e-ciberseguranca/tempest-apresenta-primeiro-estudo-do-mercado-brasileiro-de-ciberseguranca/>. Acesso em junho de 2019.

TRICLOT, MATHIEU, **Le moment cybernétique: la constitution de la notion d´information**, Éditions Champ Vallon: Seyssel, 2008.

WANG, WEI. TRITON Malware Targeting Critical Infrastructure Could Cause Physical Damage. **The Rackers News**. Dezembro, 2017. Disponível em: <https://translate.google.com/translate?hl=pt-BR&sl=en&u=https://thehackernews.com/2017 /12/triton-ics-scada-malware.html&prev=search>. Acesso em 2 ago.2019.