ESCOLA DE ARTILHARIA DE COSTA E ANTIAÉREA

1º TEN Art LEONARDO DE OLIVEIRA LOPES

A DEFESA CIBERNÉTICA NA SEÇÃO DE MÍSSEIS IGLA

Rio de Janeiro
2014

1º Ten Art LEONARDO DE OLIVEIRA LOPES

A DEFESA CIBERNÉTICA NA SEÇÃO DE MÍSSEIS IGLA.

Trabalho de Conclusão de Curso apresentado à Escola de Artilharia de Costa e Antiaérea como exigência curricular para fim de conclusão do curso de Pós-graduação de especialização nível latu sensu em Operações Militares de Defesa Antiaérea e de Defesa do Litoral.

Orientador: Cap Art Luciano Rovani

Rio de Janeiro
2014

LEONARDO DE OLIVEIRA LOPES

A DEFESA CIBERNÉTICA NA SEÇÃO DE MÍSSEIS IGLA

Trabalho de Conclusão de Curso apresentado à Escola de Artilharia de Costa e Antiaérea como exigência curricular para fim de conclusão do curso de Pós-graduação de especialização nível latu sensu em Operações Militares de Defesa Antiaérea e de Defesa do Litoral.

Aprovado em: _____/_____/_____

BANCA EXAMINADORA

_____
Cap **LUIZ CARLOS** BATISTA DE ALMEIDA JÚNIOR – Presidente
Escola de Artilharia de Costa e Antiaérea

_____
Cap LUCIANO **ROVANI** – Orientador
Escola de Artilharia de Costa e Antiaérea

_____
Cap DANIEL **TENEMBAUM** DA SILVA – Membro
Escola de Artilharia de Costa e Antiaérea

À minha noiva, uma homenagem pelo confiança em mim depositada nos momentos de maior incerteza.

AGRADECIMENTOS

Ao meu orientador meus sinceros agradecimentos pela orientação firme e objetiva na realização deste trabalho.

Aos meus pais Sergio Lopes e Sônia Maria de Oliveira Lopes, pelo amor com que me conceberam e educaram, pelas inúmeras horas que velaram meu sono, e pelas palavras de incentivo a cada tropeço de minha jornada, minha eterna gratidão.

A minha noiva pela compreensão, apoio e companheirismo nos momentos em que este trabalho foi priorizado.

A Deus, por me sustentar e fortalecer a cada dia de minha vida e a todos aqueles que direta ou indiretamente colaboraram para este projeto fosse concluído.

A nação que permanece em paz por muito tempo deveria mandar sempre alguns oficiais para áreas no exterior onde ocorrem guerras, a fim de familiarizarem-se com elas [...] (Clausewitz).

A DEFESA CIBERNÉTICA NA SEÇÃO DE MÍSSEIS IGLA

Centro de Instrução de Guerra Eletrônica (CIGE)[1]

Resumo: A guerra da informação é uma realidade nos dias atuais que encontra campo fértil no ciberespaço, constituindo a guerra cibernética. Esta vem sendo implementada com cada vez mais eficácia nos recentes conflitos mundiais, conforme exposto pela mídia. Neste caso o objetivo é reduzir ou neutralizar a capacidade combativa do oponente antes mesmo de se engajar no combate decisivo, atacando as infraestruturas críticas de Estado ou em conjunto com os demais vetores da guerra da informação. Além disso, todos os vetores da guerra da informação, tais como a guerra psicológica, a guerra de informações econômicas, a guerra de inteligência, e a própria guerra eletrônica, ganharam com o ciberespaço uma nova dimensão que potencializa sobremaneira seus efeitos. Neste ambiente, a informação é praticamente instantânea. Desta forma o uso do protocolo de internet nas comunicações de uma Seção de Mísseis IGLA torna-se um fator de vulnerabilidade à ações de Guerra Cibernética. Foi realizada uma pesquisa bibliográfica baseada em publicações de autores de reconhecida importância no meio acadêmico afim de Expor a necessidade da Defesa Cibernética na Seção de Mísseis IGLA, verificar os avanços ocorridos nos recursos tecnológicos voltados para o ataque cibernético, apresentar exemplos recentes de ataques cibernéticos à grandes instituições pelo mundo e verificar que aspectos devem se observados na defesa cibernética das informações de uma seção de mísseis IGLA.

PALAVRAS-CHAVE: guerra, ciberespaço, informação, Mísseis, vulnerabilidade e Defesa Cibernética.

[1] Centro de Instrução de Guerra Eletrônica (CIGE) – Departamento de Ciência e Tecnologia do Exército Brasileiro;

Abstract: Information warfare is a reality today which finds fertile field in cyberspace, constituting the cyberwar. This has been implemented with increasing effectiveness in recent global conflicts, as exposed by the media. In this case the goal is to reduce or neutralize the opponent's combative capacity even before engaging in a decisive battle by attacking critical infrastructure of State or jointly with the other vectors of information war. In addition, all vectors of information warfare, such as psychological warfare, information warfare economic war, intelligence and electronic warfare itself, won with the cyberspace a new dimension which greatly enhances its effects. In this environment, the information is virtually instantaneous. In this way the use of the internet communication protocol of an IGLA missile Section becomes a factor of vulnerability to Cyber War actions. A bibliographical research based on publications of authors of recognized importance in academia in order to Expose the need for Cyber Defence in section IGLA missile, check the advances that have occurred advances in technological resources geared to the cyberattack, presenting recent examples of cyberattacks at major institutions around the world and check what aspects should be observed on Cyber Defence of information from an IGLA missile section.

KEY WORDS: war, cyberspace, information, missiles, vulnerability and cyber defence.

SUMÁRIO

1 INTRODUÇÃO

O presente estudo pretende ampliar a gama de conhecimento a respeito das ameaças atuais contra a defesa do espaço cibernético no que tange as comunicações de uma seção de mísseis IGLA, servindo de base teórica para futuros estudos nesta mesma linha de pesquisa.

Pretende-se também conscientizar os artilheiros Antiaéreos sobre os riscos que essas ameaças podem ser ao futuro das atividades Antiaéreas no Brasil.

Deste modo, a fim de viabilizar a consecução do objetivo geral de estudo, foram formulados objetivos específicos, de forma a encadear logicamente o raciocínio descritivo apresentado neste estudo:

a. Verificar os avanços ocorridos nos recursos tecnológicos voltados para o ataque cibernético.

b. Apresentar exemplos recentes de ataques cibernéticos à grandes instituições pelo mundo.

c. Verificar que aspectos devem ser observados na defesa cibernética das informações de uma seção de mísseis IGLA.

A defesa da soberania nacional é dever constitucional das Forças Armadas. A atual conjuntura internacional, com os avanços na área de Tecnologia da Informação e Eletrônica, traz novas possibilidades e mais desafios para o Exército, Marinha e Aeronáutica. Em uma provável guerra cibernética que envolvesse o Brasil, alvos cruciais seriam as “infraestruturas críticas”, ou seja, os setores: energético, financeiro, bancário, de transportes, telecomunicações, fornecimento de água, rede hospitalar, órgãos de defesa, segurança pública e polos tecnológicos. Mesmo para os dirigentes desses setores, seria difícil garantir que já há o preparo necessário para evitar que as ameaças virtuais tenham efeitos reais num conflito. Portanto, são setores que se constituem em vulnerabilidades.

Ciberguerra, também conhecida por guerra cibernética, caracateriza-se como uma modalidade de guerra onde a conflitualidade não ocorre com armas físicas, mas através da confrontação com meios eletrônicos e informáticos no chamado ciberespaço. No seu uso mais comum e livre, o termo é usado para designar ataques, represálias ou intrusão ilícita num computador ou numa rede.

No entanto, uma genuína ciberguerra, situação que, em total rigor, até agora nunca ocorreu, implica, de um ponto de vista legal, o enquadramento da conflitualidade no âmbito do Direito dos Conflitos Armados ou Direito Internacional Humanitário. Tais situações poderão surgir ligadas a conflitos políticos, econômicos ou militares no mundo real, ou seja, ocorrer ao mesmo tempo de uma conflitualidade física, ou de forma totalmente autônoma. Por outro lado, estas ações poderão ter origem diretamente em estados, ou, então, ser protagonizadas por atores não estaduais atuando de forma autónoma.

Diante desse contexto, cabe ao Exército Brasileiro a responsabilidade específica sobre a Guerra Cibernética, segundo a Estratégia Nacional de Defesa (BRASIL, 2008). Nesse sentido, a presente pesquisa - resultado do presente trabalho justifica-se pela necessidade premente de desenvolver um trabalho investigativo com objetivo de Expor a necessidade da Defesa Cibernética na Seção de Mísseis IGLA tendo em vista o uso do protocolo de internet nas comunicações de uma Seção de Mísseis IGLA o que torna um fator de vulnerabilidade à ações de Guerra Cibernética.

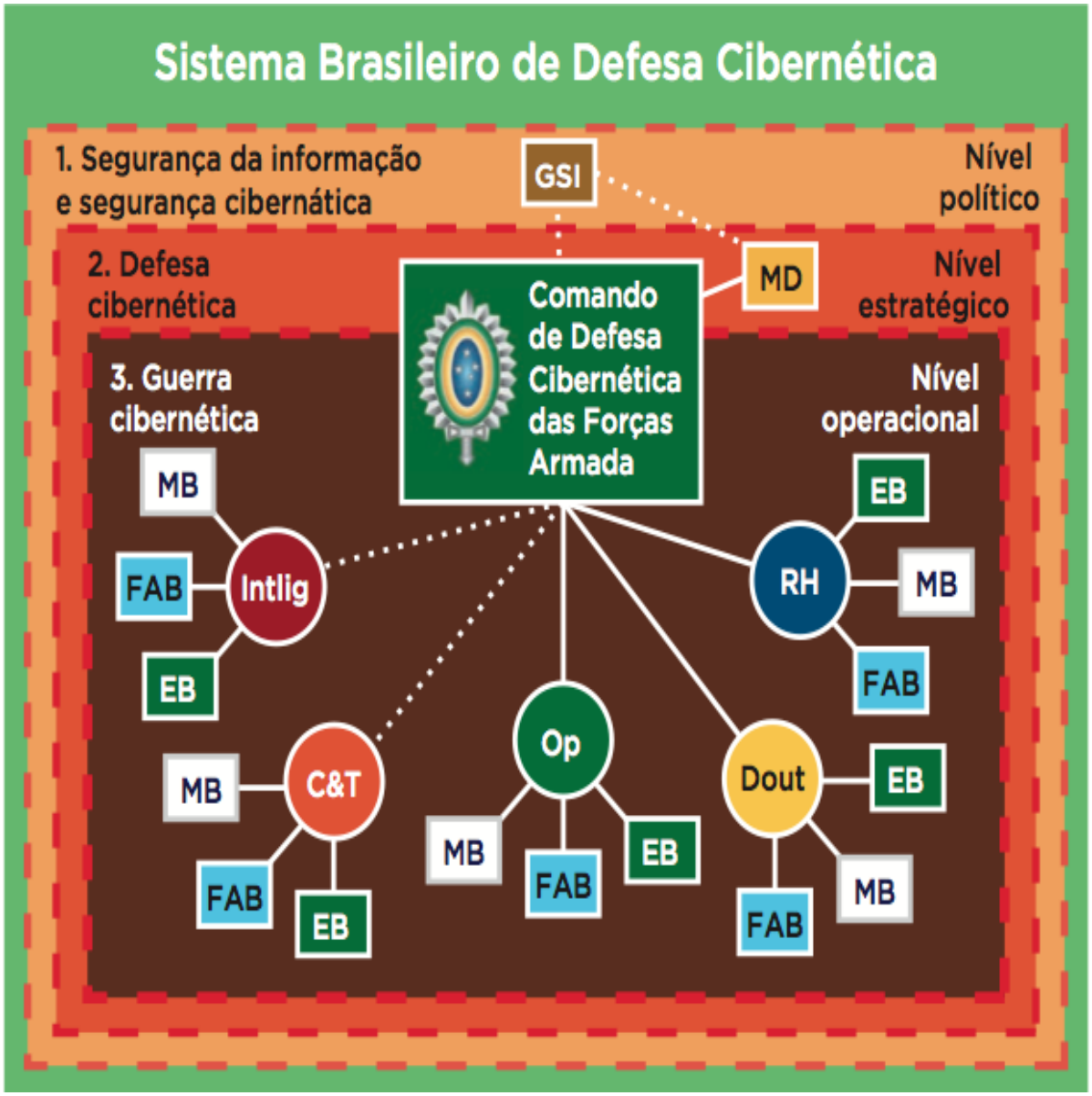
Viegas Nunes (1999) situa a guerra cibernética como parte da guerra eletrônica, sendo definida como “a utilização de todas as ferramentas disponíveis ao nível da eletrônica e da informática para derrubar os sistemas eletrônicos e de comunicações inimigos e manter os nossos próprios sistemas operacionais” (VIEGAS NUNES, 1999).

Muitos sistemas de armas e de comunicações militares dependem da velocidade e funcionalidade oferecidas pelas redes de computadores para garantir sua operacionalidade. A expressão “cibernética” foi criada por Wiener (1965), pesquisador da área de computação que decidiu designar “todo o campo das teorias de controle e comunicação, seja na máquina ou no animal”. O termo vem de uma adaptação da palavra grega para “timoneiro”, o piloto ou alguém que controla o timão das embarcações.

A Estratégia Nacional de Defesa (**END**), aprovada pelo Decreto no 6.703, de 18 de Dezembro de 2008, considera que existem três setores estratégicos de Defesa: o Nuclear, o Cibernético e o Espacial. A partir de então, a defesa do setor Cibernético foi considerada prioritária para o Exército Brasileiro. Entende-se por **Defesa Cibernética** o "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." (EME, Brasília,

2010). A fim de se atender os objetivos da END referentes à defesa cibernética, vizualiza-se a implantação do Sistema Brasileiro de Defesa Cibernética, conforme ilustrado no organograma exposto na figura 1 (Autor: Gen Bda Paulo Sergio Melo de Carvalho).

Com estas informações fica claro que o uso do protocolo de internet nas comunicações de uma Seção de Mísseis IGLA torna-se um fator de vulnerabilidade à ações de Guerra Cibernética, dentro deste contexto o presente trabalho tentará expor a necessidade da Defesa Cibernética na Seção de Mísseis IGLA, exemplificando os avanços ocorridos nos recursos tecnológicos voltados para a Guerra Cibernética, apresentando exemplos recentes ataques cibernéticos à grandes instituições pelo mundo.



Fonte: http://defesacibernetica.ime.eb.br/

O Exército Brasileiro ainda não possui uma doutrina que aponte para o correto gerenciamento da manutenção da performance cognitiva do militar em operações continuadas, o que faz crescer em importância iniciativas neste sentido, tornando este estudo altamente relevante para a otimização do desempenho cognitivo do militar em combate.

Dessa forma, o presente estudo justifica-se por promover uma discussão embasada em pesquisa bibliográfica, a respeito de um tema atual e de suma importância para a defesa das informações de uma Seção de Mísseis IGLA, das quais depende o sucesso das estratégias em operações militares, bem como por buscar identificar mecanismos que permitam diminuir vulnerabilidade frente a um ataque cibernético, estimulando o avanço nos estudos sobre Defesa Cibernética e sua rápida aplicação nas atividades de Defesa Antiaérea, em especial na Seção de Mísseis IGLA.

Pretende-se ainda, ampliar o cabedal de conhecimento acerca das possíveis consequências a uma seção de Mísseis IGLA caso sofra um ataque Cibernético, e particularmente no contexto de operações militares de Defesa Antiaérea, servindo como pressuposto teórico para outros estudos que sigam nesta mesma linha de pesquisa.

Pretende-se, também, buscar a conscientização das autoridades militares em todos os níveis, sobre os riscos admitidos quando da má gestão da Defesa Cibernética de nossas informações, tanto do ponto de vista geral, em todas as esferas da informação atinentes as atividades do Exercito Brasileiro, quanto no específico, como proposto na Seção de Mísseis IGLA.

Nesse sentido, o presente estudo pretende integrar os conceitos básicos e a informação científica relevante e atualizada, a fim de fornecer subsídios para a melhor compreensão de como se realiza a Defesa Cibernética, e de que maneira um ataque cibernético pode afetar as atividades de uma Seção de Mísseis IGLA.

2 DESENVOLVIMENTO

A fim de viabilizar e organizar a consecução do objetivo geral de estudo, serão abordados os objetivos específicos: Verificar os avanços ocorridos nos recursos tecnológicos voltados para o ataque cibernético, Apresentar exemplos recentes de

ataques cibernéticos à grandes instituições pelo mundo e Verificar que aspectos devem se observados na defesa cibernética das informações de uma seção de mísseis IGLA, de forma a encadear logicamente o raciocínio descritivo apresentado neste estudo:

2.1 AVANÇOS OCORRIDOS NOS RECURSOS TECNOLÓGICOS VOLTADOS PARA A GUERRA CIBERNÉTICA

As revoluções tecnológicas sempre inovaram a arte da guerra. O uso da pólvora e do radar, por exemplo, foram decisivos em diversas batalhas da nossa história. Com a invenção da Internet, aparentemente surgiu uma nova modalidade de guerra: a guerra cibernética.

A dependência mais e mais crescente da rede mostra que a segurança cibernética é a saída para a prosperidade, competitividade e segurança da sociedade brasileira. Quanto mais as infraestruturas críticas do Brasil, como energia elétrica e principalmente as comunicações, passam a ser mais dependentes de redes, tanto públicas quanto privadas, o provável impacto generalizado resultante da interrupção ou falha da internet também aumentou. A articulação de meios de segurança e defesa cibernética, necessários frente a um ataque cibernético, tem sido uma prioridade do governo brasileiro, por meio de ações concretas, podendo ser dado como exemplo para confirmar tal prioridade a criação do Centro de Defesa Cibernética do Exército, em 2010.

A crescente e acelerada evolução tecnológica torna complicada a classificação da segurança cibernética. Em uma ideia mais ampla, a segurança cibernética refere-se à proteção contra interferência ou ataque às atividades, aos serviços e, principalmente, às informações no âmbito digital e das redes.

Há, no ambiente cibernético, assimetrias que dificultam essa questão. De forma geral, o custo de ataques cibernéticos, através de robots e vírus é baixo, enquanto a proteção das redes de um determinado sistema tem um custo elevado de operação. Além disso, novas formas de ataques, baseados em software, surgem a cada dia, de forma rápida e perigosa, o que torna vulnerável a proteção com base apenas em ataques já ocorridos no passado.

Está claro que a segurança cibernética não é “comodity”, não esta à venda no mercado internacional aberto, pelos países que já avançaram no setor cibernético. Sendo assim, é necessário pensar de forma positivista, inovar nas formas de se enfrentar as mazelas da defesa do espaço cibernético.

E nesse aspecto entra a importância do conhecimento cientifico e tecnológico. A base natural de crescimento desse setor é, naturalmente, o avanço tecnológico, que cria novos conhecimentos e possibilidades, necessários para explorar desafios ainda não mensurados, como foi realizado com a exploração do espaço, da agricultura, do petróleo.

Desta forma, conclui-se que para se ter defesas eficazes de informações no campo cibernético, é necessário um grande investimento nos setores de ciência e tecnologia, bem como na adaptação destas à aplicação militar especificamente na defesa das informações cibernéticas das comunicações dentro da Seção de Mísseis IGLA

É fato que a defesa cibernética não depende apenas de evoluções tenológicas, mas se baseia da mesma forma em parâmetros educacionais, econômicos e regulatórios, que são de suma importância para a construção de um sistema Militar de Defesa Digital.

O Marco Civil da internet é a **Lei de Proteção de Dados Pessoais e a atuação do Comitê Gestor de Internet.** São os pilares fundamentais da esfera legal do espaço cibernético. Por exemplo, por meio de ações técnicas articuladas pelo Comitê Gestor da Internet e adotadas pelas empresas de internet e telecomunicações, o Brasil conseguiu reduzir de forma acentuada a geração de spam. Desta forma, o Brasil, que já se encontrou entre os cinco maiores geradores de spam do mundo, não se encontra mais na lista nem dos 15 países que mais geram spam, mesmo assim, fica claro que não nos encontramos no grupo dos países que possuem o maior nível de possibilidade de defesa cibernética, o que gera um alerta quando se pensa na questão da vulnerabilidade de nossas informações frente a um ataque cibernético.

A seguir está exposta a Lei de Proteção a Dados Pessoais, que consiste na primeira medida legal com intuito de legalizar a utilização da troca de informações utilizando a rede mundial de computadores no Brasil, o que em diferentes países essa regularização já se encontra em estágios mais avançados.

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:

I - o reconhecimento da escala mundial da rede;

II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;

III - a pluralidade e a diversidade;

IV - a abertura e a colaboração;

V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VI - a finalidade social da rede.

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

IV - preservação e garantia da neutralidade de rede;

V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

VII - preservação da natureza participativa da rede;

VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:

I - do direito de acesso à internet a todos;

II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;

III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e

IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Art. 5º Para os efeitos desta Lei, considera-se:

I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

II - terminal: o computador ou qualquer dispositivo que se conecte à internet;

III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;

IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;

V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;

VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e

VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Art. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

CAPÍTULO II
DOS DIREITOS E GARANTIAS DOS USUÁRIOS

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;

V - manutenção da qualidade contratada da conexão à internet;

VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e

XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no **caput**, tais como aquelas que:

I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

CAPÍTULO III
DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET

Seção I
Da Neutralidade de Rede

Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

§ 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso

IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:

I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e

II - priorização de serviços de emergência.

§ 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º, o responsável mencionado no **caput** deve:

I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei nº 10.406, de 10 de janeiro de 2002 - Código Civil;

II - agir com proporcionalidade, transparência e isonomia;

III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e

IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.

§ 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

Seção II
Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput**, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.

§ 3º O disposto no **caput** não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a

legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o **caput** sua filial, sucursal, escritório ou estabelecimento situado no País.

Subseção I
Da Guarda de Registros de Conexão

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no **caput**.

§ 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no **caput**.

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º.

§ 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Subseção II
Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Conexão

Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.

Subseção III
Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no **caput** a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no **caput**, observado o disposto nos §§ 3º e 4º do art. 13.

§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:

I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

Art. 17. Ressalvadas as hipóteses previstas nesta Lei, a opção por não guardar os registros de acesso a aplicações de internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.

Seção III
Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros

Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.

Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

§ 1º A ordem judicial de que trata o **caput** deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

§ 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal.

§ 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.

§ 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.

Art. 20. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, caberá ao provedor de aplicações de internet comunicar-lhe os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário.

Parágrafo único. Quando solicitado pelo usuário que disponibilizou o conteúdo tornado indisponível, o provedor de aplicações de internet que exerce essa atividade de forma organizada, profissionalmente e com fins econômicos substituirá o conteúdo tornado indisponível pela motivação ou pela ordem judicial que deu fundamento à indisponibilização.

Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Parágrafo único. A notificação prevista no **caput** deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material

apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

Seção IV
Da Requisição Judicial de Registros

Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I - fundados indícios da ocorrência do ilícito;

II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III - período ao qual se referem os registros.

Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro. [1]

CAPÍTULO IV
DA ATUAÇÃO DO PODER PÚBLICO

Art. 24. Constituem diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da internet no Brasil:

I - estabelecimento de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica;

II - promoção da racionalização da gestão, expansão e uso da internet, com participação do Comitê Gestor da internet no Brasil;

III - promoção da racionalização e da interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e âmbitos da Federação, para permitir o intercâmbio de informações e a celeridade de procedimentos;

IV - promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes âmbitos federativos e diversos setores da sociedade;

V - adoção preferencial de tecnologias, padrões e formatos abertos e livres;

VI - publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada;

VII - otimização da infraestrutura das redes e estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no País, promovendo a qualidade técnica, a inovação e a difusão das aplicações de internet, sem prejuízo à abertura, à neutralidade e à natureza participativa;

VIII - desenvolvimento de ações e programas de capacitação para uso da internet;

> IX - promoção da cultura e da cidadania; e
>
> X - prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso, inclusive remotos.
>
> Art. 25. As aplicações de internet de entes do poder público devem buscar:
>
> I - compatibilidade dos serviços de governo eletrônico com diversos terminais, sistemas operacionais e aplicativos para seu acesso;
>
> II - acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, sensoriais, intelectuais, mentais, culturais e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais;
>
> III - compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações;
>
> IV - facilidade de uso dos serviços de governo eletrônico; e
>
> V - fortalecimento da participação social nas políticas públicas.
>
> Art. 26. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.
>
> Art. 27. As iniciativas públicas de fomento à cultura digital e de promoção da internet como ferramenta social devem:
>
> I - promover a inclusão digital;
>
> II - buscar reduzir as desigualdades, sobretudo entre as diferentes regiões do País, no acesso às tecnologias da informação e comunicação e no seu uso; e
>
> III - fomentar a produção e circulação de conteúdo nacional.
>
> Art. 28. O Estado deve, periodicamente, formular e fomentar estudos, bem como fixar metas, estratégias, planos e cronogramas, referentes ao uso e desenvolvimento da internet no País. [1]

Vale ressaltar que a lei de proteção de dados pessoais em nada protege as informações contidas no espaço cibernético, pois com os avanços dentro da gama de possibilidades que se dispõe de meios de ataque cibernéticos ela se constitui em uma remediação, porém para que não se sofra tais ataques é necessário que se invista em meios de proteção contra ataques cibernéticos.

---

[1] CAPITULOS I, II, III e IV; da Lei Nº 12.965, de 23 de abril de 2014 que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.

A Lei de proteção de Dados pessoais e o Comitê Gestor de internet, são mecanismos criados com a intenção de regularizar, fiscalizar e controlar o trafego de informações no espaço cibernético.

> Em Nota Conjunta de maio de 1995, o Ministério das Comunicações (MC) e o Ministério da Ciência e Tecnologia (MCT) afirmaram que, para tornar efetiva a participação da Sociedade nas decisões envolvendo a implantação, administração e uso da Internet, seria constituído um *Comitê Gestor da Internet*, que contaria com a participação do MC e MCT, de entidades operadoras e gestoras de espinhas dorsais, de representantes de provedores de acesso ou de informações, de representantes de usuários, e da comunidade acadêmica.
>
> O Comitê Gestor foi criado pela Portaria Interministerial Número 147, de 31 de maio de 1995. Seus integrantes foram nomeados pela Portaria Interministerial Número 183, de 3 de julho de 1995, sofrendo alterações através das Portarias subsequentes .
>
> No dia 4 de setembro de 2003, foi publicado no Diário Oficial da União o Decreto Nº 4.829, de 3 de setembro de 2003, que estabelece as normas de funcionamento e atribuições do Comitê Gestor da Internet no Brasil. O decreto foi alterado por Portarias subsequentes.
>
> De acordo com esse decreto, são atribuições do CGI.br:
>
> I - estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil;
>
> II - estabelecer diretrizes para a organização das relações entre o Governo e a sociedade, na execução do registro de Nomes de Domínio, na alocação de Endereço IP (Internet Protocol) e na administração pertinente ao Domínio de Primeiro Nível (ccTLD - *country code Top Level Domain*), ".br", no interesse do desenvolvimento da Internet no País;
>
> III - propor programas de pesquisa e desenvolvimento relacionados à Internet, que permitam a manutenção do nível de qualidade técnica e inovação no uso, bem como estimular a sua disseminação em todo o território nacional, buscando oportunidades constantes de agregação de valor aos bens e serviços a ela vinculados;
>
> IV - promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade;
>
> V - articular as ações relativas à proposição de normas e procedimentos relativos à regulamentação das atividades inerentes à Internet;
>
> VI - ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;
>
> VII - adotar os procedimentos administrativos e operacionais necessários para que a gestão da Internet no Brasil se dê segundo os padrões internacionais aceitos pelos órgãos de cúpula da Internet, podendo, para tanto, celebrar acordo, convênio, ajuste ou instrumento congênere;
> VIII - deliberar sobre quaisquer questões a ele encaminhadas, relativamente aos serviços de Internet no País; e
>
> IX - aprovar o seu regimento interno. [2]

---

[2] Fonte: http://pt.wikipedia.org/wiki/Comit%C3%AA_Gestor_da_Internet_no_Brasil

O Desenvolvimento de capacitação tecnológica para defesa cibernética passa diretamente pelas ações de apoio á pesquisa e desenvolvimento do Ministério da Ciência, Tecnologia e Inovação, que tem trabalhado em conjunto com outros ministérios, em especial o da Defesa. O Programa TI maior – Programa estratégico de softwere e Serviços de Tecnologia da Informação, Lançado em 2012, já havia elegido a área de defesa cibernética como prioritária.

> O Ministério da Ciência, Tecnologia e Inovação lançou recentemente em São Paulo o Programa TI Maior para estimular o desenvolvimento de softwares no Brasil. Com investimento de R$ 500 milhões até 2015, o programa terá como meta desenvolver a tecnologia da informação no país.
> "Queremos que a produção de software cresça no Brasil a uma taxa muito alta. Queremos que esse crescimento represente divisas para o Brasil, geração de renda para as empresas e criação de postos de trabalho qualificados para os brasileiros", disse o ministro, Marco Antonio Raupp.
>
> Para estimular a produção de softwares em território nacional, o governo utilizará legislações já existentes como a que trata da margem de preferência em licitações, que oferece adicional de preferência de até 25% para produtos com tecnologia desenvolvida no país, e o Decreto 7.174 que regulamenta a contratação de bens e serviços de informática pela administração pública federal.
>
> As empresas beneficiárias dessas leis não precisarão ser, necessariamente, brasileiras. Basta que os softwares desenvolvidos por elas sejam considerados nacionais, mesmo que parte da criação tenha ocorrido no exterior. Os casos serão analisados pelo Centro de Tecnologia da Informação Renato Archer (CTI), localizado em Campinas (SP), que oferecerá o Certificado de Tecnologia Nacional em Softwares e Serviços aos produtos. De acordo com o ministro, o CTI partilhará sua atividade com outras autoridades certificadoras pelo país, de modo a evitar o surgimento de gargalos burocráticos. "Será uma rede", definiu. Os critérios dessa certificação passarão ainda por consulta pública durante 30 dias.
>
> Outro ponto do Programa TI Maior é a criação de quatro empresas aceleradoras, que ainda serão selecionadas a partir de editais públicos. Segundo Virgílio Almeida, secretário de Políticas de Informática do Ministério da Ciência, Tecnologia e Inovação as aceleradoras se diferem das incubadoras por terem funções adicionais que agilizam a comercialização das tecnologias. Cada uma dessas empresas trabalhará com oito a dez startups, núcleos criados em parcerias com universidades. O programa das startups terá investimento de R$ 40 milhões e deve ter início dentro de 60 dias.
>
> O modelo de startups é usado nos Estados Unidos, em Israel, no Chile e em Cingapura. Países como a Índia e Coreia do Sul também adotam programas de estímulo à tecnologia da informação. "A análise das políticas públicas desses países nos inspirou a formular as políticas que aqui fazem parte desse programa estratégico", disse Virgílio Almeida. O plano brasileiro levou 15 meses para ficar pronto e recebeu sugestões de consultores do mercado, entidades setoriais, do setor privado e da academia. De acordo com Almeida, o Programa TI Maior está em consonância com outros planos do governo federal. "Esse programa nada mais é do que uma agenda de tópicos para o futuro, em que o governo atua como um maestro tentando orquestrar as várias ações". [3]

Um desses setores é o da educação, já que haverá estímulo da capacitação de novos profissionais de TI no Brasil. Segundo o ministro Raupp, um portal feito em colaboração com a Associação Brasileira de Empresas de Tecnologias da Informação de Comunicação estará no ar em breve, trazendo informações sobre capacitação no segmento. O objetivo é formar 10 mil estudantes em cursos com

> duração de seis meses a um ano. Além disso, serão criados no país novos centros globais de pesquisa, desenvolvimento e inovação, tanto públicos quanto privados. Já existem no Brasil centros de empresas internacionais como a International Business Machines (IBM), General Electric (GE), Google e Hewlett-Packard (HP). E o país buscará ainda se relacionar com centros de localidades avançadas no segmento de TI. O Vale do Silício, nos Estados Unidos, será o primeiro deles.
>
> Outra meta do ministério é incentivar as empresas a aumentar a participação na balança comercial de modo a reverter os déficits anuais crescentes do setor. “Temos a expectativa de que as empresas estrangeiras instaladas no Brasil também passem a exportar o software que elas desenvolverem aqui”, destacou o ministro.
>
> Em 2011, segundo Raupp, o saldo negativo chegou a US$ 3 bilhões. “Para um país com a nossa capacidade intelectual, criativa e empreendedora, a reversão desse déficit deve ser apenas uma questão de tempo”. [3]

Dentre todas as medidas realizadas pelo Governo Federal que dizem respeito ao espaço cibernético, o Programa TI Maior é o único que constitui uma medida que realmente se torna eficaz no que tange a medidas de proteção cibernética, por estimular a criação de defesas cibernéticas dentro do território nacional.

No primeiro semestre de 2013 a Financiadora de estudos e projetos (Finep) fez um edital de subvenção econômica de um elevado valor para empresas de softwere nas áreas do Programa TI Maior e a defesa cibernética foi a área que recebeu o maior número de propostas.

As tecnologias ligadas ao espaço cibernético fazem parte das chamadas tecnologias duais, que podem ser usadas tanto para fins civis quanto para fins governamentais e militares. Dessa forma, essas questões tornam-se interesse estratégico, pois os ataques cibernéticos não se restringem apenas às instalações governamentais, pois sua possibilidade abrange todo o espaço cibernético.

Segundo pesquisas de mercado, o Brasil perde quase R$ 16 bilhões por ano com ataques de ciber criminosos, que cada vez mais buscam atacar os smartphones, tablets e rede sociais. No mundo, o prejuízo causado pelos crimes cibernéticos chega a US$ 110 bilhões por ano. Tais dados mostram o crescimento nas atividades cibernéticas e a vulnerabilidade que se tem caso não seja realizada a proteção cibernética de nossas informações.

---

[3] Fonte: http://www.softwarepublico.gov.br/4cmbr/xowiki/news-item289

O Ministério da Ciência, Tecnologia e Inovação planeja uma série de outras iniciativas para fortalecer a estratégia brasileira de defesa e segurança cibernética, visando a criar tecnologias de proteção do ciberespaço brasileiro.

Grandes investimentos vão apoiar ações que visam a aumento da autonomia tecnológica para o setor, desenvolvimento de tecnologias avançadas para proteção do espaço cibernético, atualização da capacidade de supercomputação do Brasil e formação de técnicos e pesquisadores nas áreas relacionadas à defesa a segurança do espaço cibernético. Recursos deverão ser colocados para fomentar a pesquisa científica nas universidades em problemas relacionados à segurança do espaço cibernético. Além disso, novos editais serão lançados para apoiar iniciativas na área de segurança cibernética e para financiar o desenvolvimento de produtos e tecnologias para segurança das redes e dos dispositivos digitais.

Para alguns pesquisadores, a guerra cibernética é a mais nova forma de guerra na era da Informação: período que se caracteriza pela capacidade do homem de comunicar-se através da Internet. Devido à possibilidade de a Internet simular o espaço físico no espaço cibernético, a Internet também foi reconhecida pelos Estados Unidos como o mais novo espaço da sua infraestrutura: ademais do mar, do ar, da terra e do espaço sideral, conclui-se então que os avanços ocorridos nos recursos tecnológicos constituem-se como grande fator de risco para grandes instituições. Tal situação deixa clara a existência de vulnerabilidade nas comunicações de uma Seção de Mísseis IGLA, caso sofra um ataque cibernético.

2.2 EXEMPLOS RECENTES DE ATAQUES CIBERNÉTICOS À GRANDES INSTITUIÇÕES PELO MUNDO

A guerra cibernética ressuscitou a espionagem no cenário mundial. Na Era da Informação, cada vez mais há a existência de conflitos no espaço cibernético, os quais muitas vezes são caracterizados como guerras cibernéticas. Este artigo objetiva retratar alguns cenários de guerra cibernética com o escopo de analisar a possibilidade de prevenção contra tais guerras através do uso de políticas de dissuasão.

Existem exemplos concretos e recentes de Ataques Cibernéticos sofridos por grandes instituições pelo mundo que comprovam a preocupação de se deve ter com esse

aspecto, podemos cintar: o Sistema de Vigilância Global Americano e ciberataques a Estônia em 2007.

2.2.1. ATIVIDADES DO SISTEMA DE VIGILÂNCIA GLOBAL AMERICANO

O exemplo mais famoso e recente que temos de ataques Cibernéticos foi o revelado pelo ex-funcionário da Agência de Inteligência Norte Americana Edward Snowden, que tornou público detalhes de vários programas que constituem o Sistema de Vigilância Global Americano.

> Reportagens do jornal "O Globo" publicadas a partir de 6 de julho, com dados coletados por Snowden, mostraram que milhões de e-mails e ligações de brasileiros e estrangeiros em trânsito no país foram monitorados. Ainda segundo os documentos, uma estação de espionagem da NSA funcionou em Brasília pelo menos até 2002. Os dados apontam ainda que a embaixada do Brasil em Washington e a representação na ONU, em Nova York, também podem ter sido monitoradas.
>
> Outros países da América Latina também são monitorados, segundo os dados. De acordo com o jornal, situações similares ocorrem no México, Venezuela, Argentina, Colômbia e Equador. O interesse dos EUA não seria apenas em assunto militares, mas também em relação ao petróleo e à produção de energia.
>
> A revista "Época" também publicou reportagem sobre documento secreto que revela como os Estados Unidos espionaram ao menos oito países – entre eles o Brasil – para aprovar sanções contra o Irã.
>
> No dia 1º de setembro, o "Fantástico" exibiu reportagem com base em documentos obtidos com exclusividade. Os arquivos classificados como ultrassecretos, que fazem parte de uma apresentação interna da Agência de Segurança Nacional dos Estados Unidos, mostram a presidente Dilma Roussef, e o que seriam seus principais assessores, como alvo direto de espionagem da NSA. Um código indica isso.
>
> Em novembro, foi revelado que o governo brasileiro monitorou as atividades de diplomatas da Rússia, do Irã e do Iraque em 2003 e 2004, época do governo Luiz Inácio Lula da Silva. O ministro da Justiça, José Eduardo Cardozo, disse que o tipo de espionagem praticada pelo Brasil e aquela que, segundo denúncias, é feita pelos Estados Unidos, são “completamente diferentes”.
>
> O Brasil recebeu com "grave preocupação" a notícia. Em 7 de julho, o então ministro das Relações Exteriores, Antonio Patriota, disse que o governo solicitaria esclarecimentos aos EUA e ao embaixador americano no Brasil. Questionado sobre as denúncias, o governo americano afirmou que não discutirá questões publicamente, mas intramuros diretamente com a estrutura diplomática do país.
>
> O vice-presidente americano, Joe Biden, telefonou no dia 19 para Dilma Rousseff para dar explicações sobre as denúncias de espionagem de cidadãos e instituições brasileiras, disse que lamentava a repercussão negativa e reiterou a disposição do governo americano de dar "informações complementares sobre o tema".
>
> Em 12 de julho, Dilma Rousseff disse, durante cúpula do Mercosul no Uruguai, que o bloco deve adotar "medidas cabíveis pertinentes" para evitar a

> repetição dos episódios. Ela disse que a segurança do país e a privacidade dos cidadãos e empresas devem ser preservadas.
>
> Após reportagem do "Fanástico", o ministro das Relações Exteriores, Luiz Alberto Figueiredo, afirmou no dia 2 de setembro que, se comprovados, os atos de espionagem dos EUA sobre a presidente Dilma Rousseff são "inadmissíveis" e "inaceitáveis".
>
> No dia 3 de setembro, foi instalada no Senado Federal uma CPI que investigará denúncias de espionagem pelos Estados Unidos a e-mails, telefonemas e dados digitais no Brasil.
>
> Durante a 68ª Assembleia-Geral das Nações Unidas em Nova York, Dilma disse em discurso que as ações de espionagem dos Estados Unidos no Brasil "ferem" o direito internacional e "afrontam" os princípios que regem a relação entre os países. Ela também cancelou uma visita de estado que faria aos EUA em outubro e pediu satisfações para Obama. Os dois presidentes conversaram na ocasião e um pouco antes, durante a cúpula do G-20.
>
> A Polícia Federal abriu um inquérito e quer que sejam ouvidos fora do país os presidentes mundiais das empresas Yahoo, Microsoft, Google, Facebook e Apple - que forneceram informações para o governo dos EUA. A PF também pediu acesso ao interrogatório de Snowden.
>
> Em novembro, os governos de Brasil e Alemanha apresentaram à Assembleia Geral da Organização das Nações Unidas (ONU) uma proposta que prevê regras para garantir o "direito à privacidade" na era digital. [4]
>
> Em dezembro, em um texto publicado pelo jornal "Folha de S. Paulo" intitulado "Carta Aberta ao Povo do Brasil", Snowden disse que a Casa Branca iria continuar interferindo em sua "capacidade de falar" até que ele obtenha um asilo permanente de algum país.
>
> No texto, ele sugeriu que, se obtivesse o benefício no Brasil, pode auxiliar o Palácio do Planalto e o Congresso Nacional a investigarem a espionagem de Washington a cidadãos, autoridades e empresas brasileiras.
>
> Em resposta, a presidente Dilma Rousseff disse que não se manifestaria sobre o interesse de Snowden de obter asilo no Brasil e que não interpretaria a carta.
>
> Em janeiro de 2013, o ministro de Relações Exteriores, Luiz Alberto Figueiredo, foi a Washington para discutir os casos de espionagem com a conselheira nacional de Segurança dos Estados Unidos, Susan Rice. Ele disse ter saído "igual" do encontro e informou que as explicações dadas serão analisadas pelo governo brasileiro. [4]

Nesse caso de vulto internacional, fica claro que faz parte da política Norte Americana as atividades no Espaço Cibernético, e ficou claro mais ainda a fragilidade de nossas defesas cibernéticas, em se tratando de defesa das informações da Presidência da República.

---

[4] Fonte: http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html

As Informações da Presidência deveriam dispor dos recursos mais avançados e eficazes que um país possuir, no que tange a defesa de suas informações. Porem não foi somente o Brasil que sofreu com as ações do Sistema de Vigilância Global Americano.

Três semanas após a divulgação dos primeiros dados, a revista alemã "Der Spiegel" publicou reportagem afirmando que a União Europeia era um dos "objetivos" da Agência Nacional de Segurança (NSA). A publicação sustentou as acusações com documentos confidenciais a que teve acesso graças às revelações do ex-funcionário americano.

Da mesma maneira também foi vigiada a representação da UE na ONU. Segundo os dados, os europeus são classificados de "objetivos a atacar". Em 2003, a UE confirmou a descoberta de um sistema de escutas telefônicas nos escritórios de vários países, incluindo Espanha, França, Alemanha, Grã-Bretanha, Áustria e Itália.

Em 30 de junho, o presidente do Parlamento Europeu (órgão legislativo da União Europeia), Martin Schulz, exigiu dos Estados Unidos que esclareça se espionou a União Europeia (UE). Em resposta, a Direção Nacional de Inteligência (ODNI) afirmou que os EUA responderiam através da via diplomática ao pedido de explicações.

Ao longo do mês de outubro, novas revelações sobre espionagens feitas pelos EUA (e também pelo Reino Unido) contra chefes de estado europeus vieram à tona. Alemanha, Itália, e França tiveram seus presidentes e chanceleres espionados, segundo documentos revelados pelas imprensas locais. Os países pediram satisfações aos EUA e convocaram os embaixadores americanos em seus territórios.

Líderes da União Europeia divulgaram um comunicado no dia 25 de outubro dizendo que a desconfiança sobre o esquema de espionagem dos Estados Unidos poderá prejudicar os esforços mundiais no combate ao terrorismo. A declaração foi dada após o jornal "Guardian" revelear que 35 líderes mundiais tiveram conversas telefônicas monitoradas.

Um deles foi a chanceler alemã Angela Merkel, que exigiu explicações e disse que que "amigo não espiona amigo". O jornal "Bild am Sonntag" afirmou que Obama sabia da espionagem contra Merkel desde 2010. O governo dos EUA negou, e o diretor da NSA garantiu que Obama não sabia do programa. Logo depois, o jornal "Wall Street Journal"

afirmou em reportagem que Obama cancelou o monitoramento de Merkel logo após saber da espionagem - o que teria ocorrido em meados de 2013.

O presidente francês, François Hollande - que também foi espionado, segundo os documentos - disse que as revelações de Snowden poderão "finalmente ser úteis", conduzindo a uma "melhor eficiência" dos serviços de Inteligência e a mais proteção da privacidade dos cidadãos.

Nove membros da comissão de Liberdades Civis do Parlamento Europeu (PE) anunciaram uma viagem aos EUA para coletar informações sobre a suposta espionagem e analisar com as autoridades americanas o impacto de seus programas de vigilância sobre os direitos fundamentais dos europeus.

Em meio aos escândalos, Lisa Monaco, conselheira de Obama em segurança interior e luta antiterrorista, admitiu em um artigo publicado no jornal "USA Today" que o programa de vigilância do país criou tensões consideráveis com alguns de seus sócios mais próximos, mas garantiu que suas atividades são legítimas.

No dia 28 de outubro, o jornal espanhol "El Mundo" revelou que mais de 60 milhões de ligações na Espanha foram monitoradas em um período de 30 dias. O governo espanhol convocou o embaixador dos EUA no país para dar explicações.

No dia 30, uma publicação italiana revelou que o Vaticano e o Papa Francisco também teriam sido monitorados, inclusive durante o conclave que elegeu o Papa. Os EUA negaram as acusações.

Até a China passou a cobrar explicações dos norte-americanos, após a imprensa australiana revelar que os EUA usavam suas representações diplomáticas na China para coletar dados sobre o país. A Indonésia também teria sido espionada por meio de embaixadas australianas.

A informação a respeito dos serviços secretos desencadeou interminável debate nos Estados Unidos e no exterior sobre o crescimento do alcance da NSA, que expandiu seus serviços de vigilância na última década. Agentes americanos garantem que a NSA atua dentro da lei.

Mais de 80 fundações e ONGs americanas lançaram uma campanha para protestar contra o programa de vigilância online. As organizações, entre elas a American Civil

Liberties Union (ACLU), as fundações World Wide Web e Mozilla, e o Greenpeace colocaram no ar o site Stopwatching.us ("Parem de nos vigiar", em tradução livre) e pediram ao Congresso que divulgue mais elementos sobre o vasto programa de vigilância.

Obama disse que os parlamentares americanos estavam informados sobre as atividades de espionagem do governo, e afirmou que as conversas telefônicas dos americanos "não estão sendo ouvidas" e que as salvaguardas constitucionais estão sendo garantidas no processo de monitoramento.

Em 9 de agosto, o presidente Obama, em entrevista, prometeu agir para que o Congresso mudasse as medidas do Ato Patriota relativas ao monitoramento e manifestou preocupação com a transparência e o respeito à privacidade.

O chefe da Agência de Segurança Nacional, general Keith Alexander, disse que a revelação dos programas de vigilância da inteligência dos EUA causou "dano irreversível" à segurança nacional e ajudou os "inimigos da América". Ele anunciou implementação de novas medidas de segurança para impedir o vazamento de informações.

Após os vazamentos relacionados a aliados europeus, no fim de outubro, a Casa Branca admitiu a necessidade de "controles adicionais" sobre a atividade de coleta de inteligência. Obama prometeu uma "revisão".

O diretor da inteligência americana, James Clapper, disse no Congresso que os aliados também espionam os EUA, e negou as acusações feitas pelos jornais europeus. Segundo o jornal "Wall Street Journal", França e Espanha também ajudaram os EUA na espionagem. O "El País" afirmou que serviço de inteligência da Espanha transfere periodicamente grandes quantidades de metadados pessoais, como a origem ou o destino de chamadas telefônicas privadas, aos serviços de inteligência americanos.

No dia 31 de outubro, o secretário americano de Estado, John Kerry, admitiu que os Estados Unidos "foram longe demais" em alguns casos de espionagem, mas justificou as práticas de Inteligência e coleta de informações como parte da luta contra o terrorismo e a prevenção de atentados. Kerry também pediu que líderes europeus não deixem o escândalo da espionagem dificultar as negociações comerciais entre a União Europeia e os Estados Unidos para a criação de uma zona de livre comércio.

No mesmo dia, Obama ordenou que a NSA parasse de espionar ocasionalmente as sedes do Fundo Monetário Internacional e do Banco Mundial como parte de uma revisão das atividades de coleta de informações.

Em dezembro, uma autoridade da NSA informou que dezenas de mudanças foram feitas na agência para impedir o surgimento de um "novo Edward Snowden", incluindo eventual ação disciplinar. Ele reconheceu que o órgão teve uma má resposta para as denúncias iniciais de espionagem.

A principal medida, entretanto, foi anunciada em janeiro de 2014, quando o presidente Obama anunciou que as agências de inteligência vão interromper a prática de espionar as comunicações de dezenas de líderes internacionais considerados "amigos e aliados" dos EUA.

Pouco depois, a NSA confirmou que Snowden teve acesso a senha de colegas para acessar informações que ele não estava autorizado a ver.

Na mesma época, em entrevista a uma TV alemã, Snowden reiterou seu convencimento que os serviços secretos dos EUA espionaram as empresas de vários países.

Em fevereiro de 2014, o senador republicano Rand Paul, potencial pré-candidato presidencial às eleições de 2016 nos EUA, apresentou uma denúncia contra o presidente Barack Obama pelo programa de vigilância.

Com esse exemplo, fica claro que os Estados Unidos, realizavam atividades cibernéticas em nível global, não somente atacando no espaço cibernético outros países, mas também instituições dentro do seu próprio território, todas as atividades tinham a justificativa que eram atividades que visavam a segurança nacional Norte Americana. O fato é que a importância dada pelos Estados Unidos às atividades no espaço cibernético deixa claro que este não pode ser ignorado. Fica claro o entendimento por parte das nações que sofreram ataques cibernéticos, da importância que deve ser dada às atividades no espaço cibernético, pelo fato de todas, além de terem se manifestado negativamente frente a postura Norte Americana, terem passado a adotar medidas de proteção à ataques Cibernéticos.

2.2.2 CIBERATAQUES À ESTÔNIA EM 2007

Em 2007 a Rússia lançou um ataque cibernético sobre a Estônia, no que ficou considerado, para muitos, como a primeira Guerra Virtual em senário Mundial.

> Os ciberataques à Estônia em 2007 referem-se a uma série de ataques cibernéticos à Estônia, que teve início em 27 de abril de 2007 e deixou sites do governo fora do ar.
>
> O governo estôniano acusou a Rússia, que teria se motivado a realizar os ataques por conta da remoção de uma estátua que marcava a vitória russa contra o nazismo, a estátua do Soldado de bronze de Tallinn, porém confirmou-se que o governo russo não estava envolvido diretamente nos ataques, sendo sua origem desconhecida até hoje.
>
> Na Estônia, quase todos os serviços são integrados à Internet, o que torna o país vulnerável a esses ataques. Quase todas as tarefas cotidianas estão ligadas à rede, por isso a população do país foi atingida diretamente com o ataque.
>
> A Estônia foi o primeiro país a realizar votações para cargos públicos por meio da Internet, isso como um ciberataque representa perigo real ao país. Esse é considerado o primeiro ciberataque de grandes proporções.
>
> Os ataques à Estônia começaram logo no dia da remoção do Soldado de Bronze de Tallinn, no dia 27 de abril de 2007. Para os russos, a retirada da estátua significava o incentivo a ações neonazistas e por isso considera que a questão deveria ser olhada com atenção por todos os países do mundo. Sendo classificada por Serguei Lavrov, ministro dos Assuntos Exteriores da Rússia, como uma atitude desumana. A Rússia também reagiu economicamente em represália ao governo da Estônia.
>
> Uma minoria russa que vive lá desde a Guerra Fria, quanto o país foi ocupado pela União Soviética, reagiu violentamente às decisões quanto a remoção da estátua.
>
> Os sites do governo, a partir de então, sofreram vários ataques por semanas. Os crackers utilizaram computadores zumbis para que os servidores tivessem milhares de visitas por segundo, sobrecarregando-os.
>
> Após os ataques em DDoS, vários sites ficaram indisponíveis por algumas horas, não causando danos permanentes aos serviços da Estônia. Os ataques mostraram como os sistemas ligados à Internet são vulneráveis e deixou em alerta vários países com serviços virtuais que podem ser futuros alvos de ataques.
>
> Vários ataques se sucederiam e seriam creditados à ciberguerra, uma nova forma de guerra que estaria surgindo e motivando governos a se protegerem na Internet e aumentarem a segurança de todos os serviços.
>
> Preocupada com o assalto às suas instituições em 2007, a Estónia criou um exército cibernético de voluntários. A Liga de Defesa Cibernética (CDL) protegerá o país dessas ameaças no futuro, noticia o *Rzeczpospolita* na primeira página. Sendo o primeiro exército desta natureza no mundo, o CDL pertence à Liga de Defesa Total paramilitar da Estónia e, em caso de ataque, ficará sob comando militar.
>
> Neste momento, é composto por 80 especialistas e engenheiros de Informática, que se reúnem uma vez por semana para pôr em prática uma defesa a um ataque simulado. Líder no acesso à internet, a Estónia "*foi o primeiro país do mundo a ter votação pela Internet em eleições legislativas. É por isso que um novo ataque cibernético pode paralisar o país*", como afirmou ao jornal Vahur Made, membro da Academia Diplomática da Estónia. [5]

[5] Fonte: http://www.voxeurop.eu/pt/content/news-brief

Tais ocorrências tiveram como consequência uma reação imediata do governo da Estônia, a criação de um Exército Cibernético. Tanto a Atividade de Ataque da Rússia, como a consequência da Estônia criar o que se considera o primeiro Exército Cibernético do mundo, demonstram que a Guerra Cibernética entra na realidade dos conflitos mundiais.

Esses exemplos deixam claro que os conflitos cibernéticos são uma realidade e um quesito de suma importância no que tange a soberania nacional, sendo assim, é importante entender melhor a ideia geral de um ataque cibernético e seus objetivos.

> Ciberguerra, também conhecida por guerra cibernética, é uma modalidade de guerra onde a conflitualidade não ocorre com armas físicas, mas através da confrontação com meios eletrônicos e informáticos no chamado ciberespaço. No seu uso mais comum e livre, o termo é usado para designar ataques, represálias ou intrusão ilícita num computador ou numa rede.
>
> No entanto, uma genuína ciberguerra, situação que, em total rigor, até agora nunca ocorreu, implica, de um ponto de vista legal, o enquadramento da conflitualidade no âmbito do Direito dos Conflitos Armados ou Direito Internacional Humanitário. Tais situações poderão surgir ligadas a conflitos políticos, econômicos ou militares no mundo real, ou seja, ocorrer ao mesmo tempo de uma conflitualidade física, ou de forma totalmente autônoma. Por outro lado, estas ações poderão ter origem diretamente em estados, ou, então, ser protagonizadas por atores não estaduais atuando de forma autónoma. [6]

A possibilidade de ciberguerra resulta da existência de redes de computadores essenciais para o funcionamento de um país. Potenciais alvos são as infraestruturas críticas, nomeadamente as redes de energia elétrica, de gás e de água, os serviços de transportes, os serviços de saúde e financeiros.

Pelas suas possíveis consequências econômicas e danos que podem provocar ao normal funcionamento de um país, os ciberataques são motivo de crescente preocupação a nível internacional. Existem exemplos concretos do que poderão ser essas situações. Os ciberataques sofridos pela Estônia em 2007, mostraram como uma economia e serviços públicos da era digital podem sofrer graves anomalias de funcionamento ou até ficarem temporariamente indisponíveis.

Num outro plano, os danos sofridos pelo programa nuclear iraniano tornados públicos em 2010, devido ao vírus Stuxnet, evidenciaram as múltiplas potencialidades de uso de ciberarmas para os meios militares e de segurança.

---

[6] Fonte: http://pt.wikipedia.org/wiki/Ciberguerra

Naturalmente que as maiores e mais sofisticadas economias têm uma particular preocupação com este assunto, devido à crescente dependência da sua prosperidade face à tecnologia digital e às redes informática.

Todavia, as ações para prevenir e punir ciberataques estão longe de obter consenso internacional. Isto ocorre não só pela complexidade técnica e jurídica das questões levantadas, como porque o uso de ciberarmas pode ser uma opção interessante, de guerra assimétrica, para vários países.

A partir dai, é preciso que fique claro que os ataques cibernéticos tem, quase sempre, objetivos prioritários.

A empresa de segurança norte-americana, McAffee, no seu relatório de 2010 intitulado "Sob Fogo Cruzado". Infraestrutura Crítica na Era da Guerra Cibernética", fez uma avaliação global das ameaças que impendem sobre as infraestruturas críticas – redes elétricas, de gás e de água, telecomunicações, transportes, serviços financeiros e de saúde, etc.

O relatório baseou-se nos resultados de um inquérito efetuado a seiscentos executivos de Tecnologia da Informação (TI) responsáveis pela segurança em empresas de infraestruturas críticas de sete setores e catorze países. Estes responderam anonimamente a uma série de perguntas detalhadas sobre suas experiências com ciberataques e práticas de segurança.

As respostas evidenciaram que as redes e sistemas de controle de infraestruturas críticas estão constantemente sob o efeito de ciberataques. Frequentemente enfrentam também adversários de alto nível, existindo, em vários casos, suspeitas de envolvimento, não assumido, de países estrangeiros nos mesmos.

O tipo de ciberataque também varia, desde o ataque de negação de serviço (DoS na sigla em língua inglesa), perpetrado em massa e concebido para derrubar sistemas de informação, até iniciativas subreptícias de penetração nas redes, com o objetivo de espionagem.

Um outro tipo de ataque consiste na introdução de um software malicioso na infraestrutura crítica. O Stuxnet, considerado o mais poderoso virus até agora criado

reflete essa possibilidade. Comprovou, num caso concreto – o programa nuclear iraniano – como uma infraestrutura crítica de produção de energia pode ser alvo de um novo tipo de ato de ciberguerra, mostrando inovadoras possibilidades estratégicas para o atacante.

É consensual, entre os especialistas, o Stuxnet não poder ter sido produzido por um usuário doméstico até porque eram necessárias informações privilegiadas sobre o funcionamento das instalações nucleares iranianas, o que escapa, certamente, às possibilidades de hackers atuando isoladamente.

O impacto dos ciberataques também é bastante variável, mas algumas das consequências relatadas mostraram impactos negativos significativos. O custo reportado das paralisações decorrentes de grandes ataques excedeu US$ 6 milhões por dia. Fora esse custo, a perda mais amplamente temida com os ciberataques é o dano à reputação, seguido pela perda de informações pessoais dos clientes.

Em termos de identificação e responsabilização dos autores, há problemas técnicos e jurídicos delicados e difíceis de ultrapassar. As instruções de um ciberataque, que são transmitidas para as redes, costumam vir de outros computadores infectados, usualmente pertencentes a terceiros inocentes.

Quanto aos verdadeiros autores do ciberataque, normalmente ficam ocultos por detrás de barreiras e falsos vestígios. Esses fatores tornam difícil o rastreamento da sua verdadeira origem e limitam a possibilidade de punição legal pela incerteza quanto à autoria.

Assim, para os autores do relatório, o ciberespaço de hoje lembra muito o que Hobbes chamou de um estado de natureza – uma “guerra de cada homem contra cada homem”. Hobbes imaginava que apenas o governo e a lei poderiam por fim a essa “guerra”.

Todavia, em matéria de proteção e segurança das infraestruturas críticas o papel dos governos torna-se complicado quando a maioria das infraestruturas críticas está nas mãos de empresas privadas. O problema tende ainda a ser mais complexo, e a vulnerabilidade potencialmente maior, quando as infraestruturas críticas nacionais são detidas numa percentagem significativa por capitais estrangeiros.

Com esses exemplos, verificamos que ataques cibernéticos que envolvem segurança estão mais sofisticados através das mudanças decorridas dos avanços tecnológicos, o que consequentemente acarreta um aumento na taxa de sucesso das violações de segurança. Como resultado, as empresas e órgãos governamentais enfrentam novos desafios na avaliação, identificação e solução dessas atividades, o que demonstra que o nível que nos encontramos no que tange a defesa cibernética está longe de ser considerado ideal.

Sendo assim, é importante que toda atividade, dentro de uma Seção de Mísseis IGLA realizada dentro do espectro cibernético seja seguida de medidas de defesas cibernéticas, para que caso sofra um ataque cibernético, possa se defender e não sofrer perdas em suas informações, afim de que as atividades de defesa antiaérea sejam realizadas com o máximo de segurança e eficácia, tendo em vista os objetivos da Força Terrestre.

2.3 ASPECTOS QUE DEVEM SER OBESERVADOS NA DEFESA CIBERNÉTICA DAS INFORMAÇÕES DE UMA SEÇÃO DE MÍSSEIS IGLA

No campo cibernético, todo material que se encontre em uma rede está sujeito a um ataque cibernético. O uso da Radio Harris Falcon III nas comunicações de uma Seção de Mísseis IGLA a torna uma parte vulnerável à um ataque cibernético, por este rádio utilizar protocolo de internet em sua programação.

> Protocolo de Internet (em inglês: *Internet Protocol*, ou o acrónimo IP) é um protocolo de comunicação usado entre duas ou mais máquinas em rede para encaminhamento dos dados. Tanto no Modelo TCP/IP, quanto no Modelo OSI, o importante protocolo da internet IP está na camada intitulada camada de rede.
>
> Os dados numa rede IP que são enviados em blocos referidos como ficheiros (os termos são basicamente sinónimos no IP, sendo usados para os dados em diferentes locais nas camadas IP). Em particular, no IP nenhuma definição é necessária antes do nó tentar enviar ficheiros para um nó com o qual não comunicou previamente.
>
> O IP oferece um serviço de datagramas não confiável (também chamado de *melhor esforço*); ou seja, o pacote vem quase sem garantias. O pacote pode chegar desordenado (comparado com outros pacotes enviados entre os mesmos nós), também podem chegar duplicados, ou podem ser perdidos por inteiro. Se a aplicação requer maior confiabilidade, esta é adicionada na camada de transporte.
>
> Os roteadores são usados para reencaminhar datagramas IP através das redes interconectadas na segunda camada. A falta de qualquer garantia de entrega significa que o desenho da troca de pacotes é feito de forma mais simplificada. (Note que se a rede cai, reordena ou de outra forma danifica um grande número de pacotes, o desempenho observado pelo utilizador será pobre,

logo a maioria dos elementos de rede tentam arduamente não fazer este tipo de coisas - *melhor esforço*. Contudo, um erro ocasional não irá produzir nenhum efeito notável)

O IP é o elemento comum encontrado na Internet pública dos dias de hoje. É descrito no RFC 791 da IETF, que foi pela primeira vez publicado em Setembro de 1981. Este documento descreve o protocolo da camada de rede mais popular e atualmente em uso. Esta versão do protocolo é designada de versão 4, ou IPv4. O IPv6 tem endereçamento de origem e destino de 128 bits, oferecendo mais endereçamentos que os 32 bits do IPv4.

Talvez os aspectos mais complexos do IP sejam o endereçamento e o encaminhamento. O endereçamento define como os endereços IP dos nós finais são atribuídos e como as subredes dos endereços de IP dos nós são divididos e agrupados. O encaminhamento IP é feito por todos os nós, mas mais comumente por roteadores de rede, que tipicamente usam os protocolos IGP ou EGP para ajudar na leitura de datagramas IP que reencaminhem decisões através de IPs em redes ligadas.

No entanto, o protocolo IP em sua versão atual (a versão quatro, rotulada como IPv4) já é bastante antiga e tem muitos problemas. Os mais graves são falhas de segurança, que periodicamente são descobertas e não têm solução. A maioria dos ataques contra computadores hoje na internet só é possível devido a falhas no protocolo IP. A nova geração do protocolo IP, o IPv6, resolve grande parte dos problemas de segurança da internet hoje, herdados justamente do projeto antiquado do IPv4.

Mas o IPv4 tem um problema ainda mais premente do que sua inerente insegurança: já esgotou sua capacidade de expansão. Cada computador ligado à internet - seja um computador pessoal, uma estação de trabalho ou um servidor que hospeda um site - precisa de um endereço único que o identifique na rede. O IPv4 define, entre outras coisas importantes para a comunicação entre computadores, que o número IP tem uma extensão de 32 bits. Com 32 bits, o IPv4 tem disponíveis em teoria cerca de quatro bilhões de endereços IP mas, na prática, o que está realmente disponível é menos da metade disso. Se contarmos que o planeta tem seis bilhões de habitantes e que cada dispositivo ligado na internet (o que inclui smartphones, PCs, notebooks e afins) precisa de um número só dele, é fácil perceber que a conta não fecha. Esse número, sendo finito, um dia acaba.

Em cima disso, os endereços IP são "travados" geograficamente. Dois endereços próximos estão necessariamente na mesma cidade ou região. Se considerarmos que cerca de três quartos dos endereços IP disponíveis para a internet estão localizados nos Estados Unidos (mesmo que nunca usados), sobram apenas pouco mais de um bilhão de endereços para o resto do mundo - aumentando ainda mais o problema de escassez.

A entrada dos smartphones e outros dispositivos móveis (que são baratos e extremamente populares) na internet contribuiu para que o número de endereços IP disponíveis seja ainda mais escasso. De fato, algumas previsões pessimistas davam conta de que os endereços IP iriam acabar por completo em 2012, transformando a internet num verdadeiro caos.

O advento do IPv6, com 128 bits, resolveria todos esses problemas. Primeiro, porque dá fim a praticamente todos os buracos de segurança conhecidos do IPv4, tornando as comunicações muitíssimo mais seguras. O IPv6 provavelmente será uma dor de cabeça sem tamanho para os hackers criminosos.

Em segundo lugar, o IPv6 define 128 bits para endereçamento, e portanto conta com cerca de 3,4 × 10^38 endereços disponíveis (ou 340 seguido de 36

> zeros). Para quem não quiser fazer a conta, basta saber que são muitos bilhões de quatrilhões de endereços disponíveis, garantindo que não vai faltar números IP para os humanos por milênios.
>
> Pelo "draft" inicial de um documento proposto pelo IETF - Internet Engineering Task Force, órgão responsável pelo desenvolvimento tecnológico da internet, a migração de IPv4 para IPv6 deveria ter começado em algum momento entre 2009 e 2010, com migração total até o fim de 2011. O cronograma ainda está atrasado devido aos vários problemas da completa conversão. Google, Yahoo! e Facebook já começam a adotar o IPv6.
>
> Na Campus Party Brasil de 2011, em sua quarta edição brasileira, realizada em São Paulo, a Telefônica ofereceu aos campuseiros a oportunidade de se conectar à internet com IPv6. A companhia vem testando a tecnologia há dois anos e espera poder oferecê-la aos seus clientes ainda em 2011. [7]

Na internet e nas redes particulares que vemos hoje nas empresas ou mesmo nas residências, o protocolo de comunicação usado pelos computadores chama-se IP - sigla para Internet Protocol. Criado no fim dos anos 70, o protocolo IP tem como "missão" não só fazer dois computadores "conversarem", mas também possibilitar a interligação de duas ou mais redes separadas. Com raríssimas exceções, praticamente todas as redes do mundo acabaram, de uma forma ou de outra, sendo conectadas entre si e foi essa comunhão de redes que acabou formando o que conhecemos hoje por internet (nome que, em português, pode ser traduzido por "inter-redes" ou "redes interligadas"). Sendo assim os dados que são transmitidos pelo Rádio Harris Falcon III, circulam na mesma rede que qualquer pessoa pode ter acesso.

O protocolo IP possui um esquema de endereçamento parecido com os números de telefone. Assim como qualquer telefone, no mundo todo, é único (considerando o DDD e o código de país), cada computador ligado na internet possui um número único, que é chamado de endereço IP ou número IP. Esse número serve para identificar o computador na internet. Se você precisar conversar com alguém pela internet, basta mandar mensagens endereçadas ao endereço IP do computador da pessoa, da mesma forma podemos entender que qualquer dado pode ser inserido no Rádio, desde que o Protocolo de Internet do Rádio Falcon III seja descoberto.

Para que um dado saindo do Rádio presente no COAAe fale com a UTir da Seção de Mísseis IGLA, por exemplo, é preciso que os dados (no caso, informações sobre a ameaça aérea) sejam divididos em “pacotinhos pequenos” (chamados de pacotes IP).

---

[7] Fonte: http://pt.wikipedia.org/wiki/Protocolo_de_Internet

Estes “pacotinhos” possuem marcados dentro de si o endereço IP de origem (ou seja, o número único do computador do COAAe) e o IP de destino (o número único do computador da UTir). A internet "se vira" para encontrar o caminho entre COAAe e UTir, sem que nenhum dos dois precise se preocupar com isso.

Desta forma toda a atividade que envolve a seção de mísseis IGLA deve ser vista como um campo de Guerra Cibernética em potencial, devendo ser adotadas todas as medidas de defesa cibernética possíveis.

> No campo de redes, a área de segurança de rede consiste na provisão e políticas adotadas pelo administrador de rede para prevenir e monitorar o acesso não autorizado, uso incorreto, modificação ou negação da rede de computadores e dos seus recursos associados. Segurança de rede envolve a autorização de acesso aos dados de uma rede, os quais são controlados pelo administrador de rede.
>
> Usuários escolhem ou são atribuídos uma identificação e uma senha, ou outra informação de autenticação que permite que eles acessem as informações e programas dentro de sua autorização. A segurança de rede cobre uma variedade de redes de computadores, tanto publicas quanto privadas, que são utilizadas diariamente conduzindo transações e comunicações entre empresas, agências governamentais e indivíduos.
>
> Redes podem ser privadas, como as de uma companhia, e outra podem ser abertas para acesso público. Segurança de rede está envolvida em organizações, empresas e outros tipos de instituições. Faz como seu nome sugere: torna a rede segura, assim como protege e supervisiona as operações sendo feitas. A maneira mais comum e simples de proteger um recurso de rede é atribuir um nome único e uma senha correspondente. Segurança de rede começa com autenticação do usuário, geralmente com um usuário e senha. Já que isto requer apenas um detalhe para autenticar o usuário — a senha, o que é algo que o usuário 'conhece' — isto algumas vezes é chamado de autenticação de um fator. No caso da autenticação de dois fatores, alguma coisa que o usuário 'tem' também é utilizada (por exemplo, um Token, um dongle, um cartão de crédito ou um telefone celular; já em uma autenticação de três fatores, alguma coisa que o usuário 'é' também é utilizada (impressão digital ou escaneamento de retina).
>
> Uma vez autenticado, um firewall aplica políticas de acesso, como os serviços que são permitidos a serem acessados pelas usuários da rede.[2] Embora efetivo na prevenção de acesso não autorizado, este componente pode falhar na checagem de conteúdo potencialmente perigoso, como worms ou Trojans sendo transmitido pela rede. Um software Antivírus ou um Sistema de prevenção de intrusos '(IPS - Intrusion Prevention System)'[3] ajudam a detectar e inibir as ações deste tipo de malwares.[8]

Um Sistema de Detecção de Intrusão baseado em anomalias também pode monitorar a rede e o trafego de rede, procurando por um conteúdo ou comportamento inesperado (suspeito) e outras anomalias para proteger os recursos de, mas não limitado a, um ataque de negação de serviço ou um empregado acessando arquivos em horários estranhos.

---

[8] Fonte: http://pt.wikipedia.org/wiki/Seguran%C3%A7a_de_rede

Eventos individuais que acontecem na rede podem ser registrados para serem auditados e para análises posteriores de alto nível. A comunicação entre dois hospedeiros utilizando uma rede pode ser encriptada para manter sua privacidade.

3 CONCLUSÃO

Analisado o tema, percebeu-se, portanto, uma nova filosofia de defesa nacional, qual seja: a Defesa Cibernética, que tem a responsabilidade de impedir o sucesso de ataques virtuais que visam como alvo os sistemas públicos e militares do país.

A formação de recursos humanos na área de segurança cibernética no Brasil ainda é muito lenta, problema esse compartilhado com outras nações. O governo norte-americano saiu à frente na busca de soluções, incentivando financeiramente seus cidadãos a buscar formação em segurança cibernética.

No Brasil, apesar dos recentes esforços governamentais, as ações de capacitação em segurança cibernética ainda são incipientes e isoladas. A formação em massa de mão de obra é uma necessidade urgente. O incentivo à formação acadêmica de graduação e pós-graduação deve ser considerado para o atendimento das necessidades, de forma a, pelo menos, atender as medidas previstas na legislação.

Para se enfrentar o desafio da formação de mão de obra em segurança cibernética no Brasil, as políticas públicas devem focar na capacitação de gestores, de técnicos e de novos pesquisadores.

Devem ser consideradas ações urgentes de curto prazo para a capacitação de servidores públicos em médio e longo prazo, visando à formação de mão de obra especializada para atender às demandas do Estado, da sociedade e especialmente do Exército.

Demonstrada a relevância do tema num contexto nacional, detectou-se que o Estado Brasileiro deverá atuar em duas vertentes para conseguir cumprir com suas responsabilidades: primeiramente terá que continuar a legislar no sentido de tipificar determinadas condutas virtuais como criminosas, para elas cominando penas; bem como preparar, modernizar e equipar o Exército Brasileiro para atuar na linha de frente, sempre que necessário.

Dentro desta perspectiva, depreendeu-se a necessidade de implemento da defesa cibernética e sua aplicação desta dentro da Seção de Mísseis IGLA, por esta utilizar o protocolo IP em suas comunicações, fazendo com que seja vulnerável a qualquer tipo de ataque cibernético. Observou-se, também, que o Estado Brasileiro criou a Estratégia Nacional de Defesa (END) e, por conseguinte, o Exército Brasileiro criou o Centro de Defesa Cibernética (C D Ciber), inaugurado em agosto de 2010, adquirindo e desenvolvendo novas tecnologias com o propósito de defender o Brasil em caso de ataque cibernético.

Por fim, torna-se imperioso que o Exército Brasileiro, mais especificamente a Artilharia Antiaérea, desenvolva a mentalidade de preocupação com a segurança e difunda a importância da defesa cibernética para a segurança das atividades atinentes a defesa antiaérea realizada pelas Seções de Mísseis IGLA. Ainda dentro deste preceito, é fundamental que o Governo disponibilize subsídios para que o Exército invista nessa nova categoria de combate moderno.

REFERÊNCIAS

1 - VIEGAS NUNES, Paulo F. Impacto das Novas Tecnologias no Meio Militar: A Guerra de Informação. Congresso Internacional da Imprensa Militar: Lisboa, 1999. Disponível em: <http://www.airpower.au.af.mil/apjinternational/apj-p/2000/2tri00/nunes.htm>. Acesso em: 30 jun 2014.

2 - EME, Brasília, 2010. Disponível em < http://defesacibernetica.ime.eb.br/>. Acesso em: 22 de julho de 2014.

3 - CAPITULOS I, II, III e IV da Lei Nº 12.965, de 23 de abril de 2014. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 22 de julho de 2014.

4- *Comitê Gestor da Internet* Disponível em <http://pt.wikipedia.org/wiki/Comit%C3%AA_Gestor_da_Internet_no_Brasil>. Acesso em : 22 de julho de 2014

5– Serviços de Tecnologia da Informação. Disponível em < : http://www.softwarepublico.gov.br/4cmbr/xowiki/news-item289/>. Acesso em: 03 de agosto de 2014.

6– G1 Mundo, Caso Edward Snowden. Disponível em <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html/>. Acesso em: 03 de agosto de 2014.

7 – CIBERDEFESA, Exercito Cibernético da Estônia. Disponível em < http://www.voxeurop.eu/pt/content/news-brief/462071-estonia-cria-um-exercito-cibernetico/>. Acesso em: 05 de agosto de 2014.

8 - CIBERGUERRA. Disponível em < http://pt.wikipedia.org/wiki/Ciberguerra/>. Acesso em: 05 de agosto de 2014.

9– PROTOCOLO DE INTERNET - IP. Disponível em < http://pt.wikipedia.org/wiki/Protocolo_de_Internet />. Acesso em: 22 de agosto de 2014.

10– SEGURANÇA DE REDE. Disponível em < http://pt.wikipedia.org/wiki/Seguran%C3%A7a_de_rede/>. Acesso em: 05 de agosto de 2014.