AUREO RIBEIRO VIEIRA DA SILVA

A Segurança Cibernética no mundo corporativo: proposta de um Planejamento Estratégico de Segurança Cibernética Corporativa

Prêmio ABSEG

2014

R XXX AUREO RIBEIRO VIEIRA DA SILVA

A Segurança Cibernética no mundo corporativo: proposta de um Planejamento Estratégico de Segurança Cibernética Corporativa **. /**
Proponete-concorrente – 2014.
46. ; il.: 30 cm.

Artigo para concorrer no Prêmio ABSEG 2014, 2014.

. Bibliografia: f. 44.

1. Segurança Cibernética. 2. Planejamento Estratégico. 3. Cibernética.

CDD xxx.xxx x

A Segurança Cibernética no mundo corporativo: proposta de um Planejamento Estratégico de Segurança Cibernética Corporativa

Trabalho apresentado à ABSEG para concorrer ao prêmio ABSEG 2014.

ABSEG

2014

RESUMO

O presente trabalho apresenta, com base no histórico da Cibernética e do Planejamento Estratégico, uma sugestão de inclusão do tema nos Planejamentos Estratégicos das Organizações. Além de ressaltar os principais aspectos da cibernética, no mundo e no Brasil aponta para os riscos que essa atividade representa no meio da sociedade organizacional.

Iniciando com revisões sobre conceitos de cibernética, casos históricos, exemplos de governança e repassando os conhecimentos pertinentes a um Planejamento Estratégico, o trabalho busca no final despertar o mundo corporativo para a necessidade de implantar Planejamentos Estratégicos para a Segurança Cibernética em sua cultura organizacional.

Palavras Chaves: 1. Segurança Cibernética. 2. Planejamento Estratégico. 3. Cibernética

ABSTRACT

This paper presents, based on the history of cybernetics and Strategic Planning, a suggestion of inclusion of this topic in the Strategic Planning of the organizations. He points out the main aspects of cyber affairs, worldwide and in Brazil and it points to the risk that this activity represents to organizational society.

Starting with revisions on concepts of cybernetics, cases, and examples of governance and passing on relevant about the concepts of strategic planning, this job searches, in late, to awake the corporate world to the need to deploy Strategic Planning for Cyber Security in its organizational culture.

Keywords:1 Cybersecurity. 2. Strategic planning. 3. Cybernetics

LISTA DE ABREVIATURAS E SIGLAS

CIA	Central Intelligence Agency (EUA)
DHS	Department of Homeland Security (EUA)
END	Estratégia Nacional de Defesa
FBI	Federal Bureau of Investigation (EUA)
G8	Grupo dos Oito
ANSSI	L'Agence nationale de la sécurité des systèmes d'information (FRANÇA)
MCT	Ministério da Ciência e Tecnologia
MC	Ministério das Comunicações
NASA	National Aeronautics and Space Administration (EUA)
NCSD	National Cyber Security Division (EUA)
NTICs	Novas Tecnologias de Informação e Comunicação
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
ONU	Organização das Nações Unidas
ONS	Operador Nacional do Sistema Elétrico
PE	Planejamento Estratégico
SERPRO	Serviço Federal de Processamento de Dados
TI	Tecnologia da Informação
USCYBERCOM	United States Cyber Command (EUA)

SUMÁRIO

1	**INTRODUÇÃO**	6
2	**BREVE HISTÓRICO DA SEGURANÇA E DEFESA CIBERNÉTICA**	9
2.1	EVENTOS QUE INFLUENCIARAM O MUNDO	9
2.2	SEGURANÇA E DEFESA CIBERNÉTICAS	14
2.3	UM GIRO PELO MUNDO	16
2.4	ATAQUES CIBERNÉTICOS NO MUNDO	18
3	**GOVERNANÇA CIBERNÉTICA – ÁREA GOVERNAMENTAL**	21
3.1	ALGUNS EXEMPLOS ATUAIS	21
3.2	BRASIL	28
4	**PLANEJAMENTO ESTRATÉGICO EM SEGURANÇA CIBERNÉTICA**	34
4.1	CONSIDERAÇÕES TEÓRICAS SOBRE PLANEJAMENTO ESTRATÉGICO	34
4.2	A ELABORAÇÃO DE UM PLANEJAMENTO ESTRATÉGICO	34
4.2.1	**O processo do planejamento estratégico**	34
4.2.2	**O que é planejamento estratégico**	34
4.2.3	**Quem faz o planejamento estratégico**	35
4.2.4	**Componentes do planejamento estratégico**	35
4.3	UM EXEMPLO SUCINTO DE PLANEJAMENTO ESTRATÉGICO EM SEGURANÇA CIBERNÉTICA	37
4.3.1	**Uma companhia global de TI**	37
4.3.2	**Principais tópicos do Planejamento Estratégico em Segurança Cibernética da Huawei (core)**	37
4.3.2.1	Estratégia, Governança e Controle	38
4.3.2.2	Construir os conceitos básicos de processos e padrões	38
4.3.2.3	Leis e Regulamentos	38
4.3.2.4	Pessoas	39
4.3.2.5	Pesquisa e Desenvolvimento	39
4.3.2.6	Verificação: não aceite nada, não acredite em ninguém, verifique tudo	39
4.3.2.7	Gestão de fornecedores terceirizados	39
4.3.2.8	Produção	40
4.3.2.9	Prestação de serviços de forma segura	40
4.3.2.10	Quando as coisas dão errado, o assunto é: defeito e vulnerabilidade	40
4.3.2.11	Rastreabilidade	40
4.3.2.12	Auditoria	40
5	**CONCLUSÃO**	41

1 INTRODUÇÃO

Atualmente, não existe espaço para novas gerações que não tenham contato, desde cedo, com telefones celulares, com tablets, smartphones, laptops e outros meios. Após o término da II Guerra Mundial, as telecomunicações foram associadas à computação e, com isso, iniciava-se um novo setor do conhecimento humano chamado de tecnologia da informação.

Essas novas tecnologias e métodos, chamadas de Novas Tecnologias de Informação e Comunicação (NTICs), surgiram no contexto da Revolução Informacional, "Revolução Telemática" ou Terceira Revolução Industrial, e foram desenvolvidas gradativamente desde a segunda metade da década de 70 do século passado e, principalmente, nos anos 90. Estas tecnologias utilizam a digitalização e a comunicação em redes para a captação, transmissão e distribuição das informações (texto, imagem estática, vídeo e som). O advento destas (e a forma como foram utilizadas por governos, empresas, indivíduos e setores sociais) possibilitou o surgimento do que se pode chamar de "sociedade da informação".

A partir daí, a tecnologia da informação se transformou na base de todos os ramos do conhecimento, criando uma dependência cada vez maior. Porém, além dos inúmeros serviços que presta, traz consigo vulnerabilidades em proporcional quantidade. Logo se percebeu a possibilidade de explorar os recursos e as vulnerabilidades da tecnologia da informação sobre as infraestruturas críticas de um Estado, a fim de se obter informações, segredos industriais, realizar sabotagens ou mesmo vantagem durante a ocorrência de conflitos, independentemente dos atores neles envolvidos. Essa exploração das vulnerabilidades pode ser realizada por individuo ou pelo Estado, sendo chamados de ataques cibernéticos ou guerra cibernética.

Uma consequência natural desse processo foi exatamente o reflexo que produziria, e produziu, no mundo corporativo. Ainda que incipiente, as corporações já sofrem por demasiado com os problemas na área cibernética, seja na gestão, na governança, nos processos e, principalmente, nas operações dos meios de TI.

Os ataques cibernéticos se apresentam em uma escalada mundial crescente, silenciosa e se caracterizam como um dos grandes desafios do século XXI. Todas as pessoas, empresas, governos e entidades que utilizam o espaço cibernético estão expostos a riscos. Na realidade, nos dias atuais, é praticamente inexistente empresas de grande porte que não possuem os meios de TI permeando seus processos.

Richard Clarke, autor de um estudo sobre ataques cibernéticos, cuidou da estratégia

de combate ao terrorismo cibernético dos Estados Unidos durante o Governo Bush. Recentemente, fez um estudo que levou o presidente Barack Obama a criar, em Washington, o comando cibernético para defender o país desse tipo de ataques.

A guerra cibernética já começou. Potências rivais como a China e a Rússia já teriam colocado na rede dos Estados Unidos bombas lógicas, programas prontos para serem ativados e capazes de destruir parte da infraestrutura do país. Num exemplo recente de guerra cibernética, o vírus ***stuxnet*** danificou centrifugadoras do programa nuclear do Irã e as suspeitas recaem sobre Estados Unidos e Israel.

A Estratégia Nacional de Defesa do Brasil (END) define três setores estratégicos essenciais para a defesa nacional, atribuindo a cada uma das Forças Armadas a responsabilidade de coordenação de cada um deles, sendo o setor cibernético a cargo do Exército Brasileiro.

O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) tem como uma de suas competências a responsabilidade de coordenar as atividades de segurança da informação na administração pública federal.

Algumas definições e conceitos serão expostos ao longo do trabalho, mas faz-se necessário, antes de tudo, a definição de ***hacker***. Atualmente, não é difícil encontrar esse termo sendo utilizado na mídia como sinônimo de vandalismo. Para Dom (2003), ***hacker*** é uma palavra inglesa que não possui uma tradução exata para a língua portuguesa. A tradução mais próxima seria "fuçador" ou aquele que aprende "fuçando". Portanto, o termo *hacker* é usado para designar pessoas que criam e modificam software e hardware de computadores, não necessariamente com maus objetivos.

Comumente na mídia e em algumas populações, usa-se o termo *hacker* para designar *crackers*, ou seja, pessoas que praticam atos ilegais ou sem ética (atividades criminosas usando várias técnicas e tecnologias como: invasão de computadores, furto de informações e depredação de sites, etc).

De acordo com Cebrian (1998), em 1985, o termo cracker foi utilizado com uma nítida intenção em demonstrar que hackers e crackers eram seres diferentes e, assim, deveriam ser reconhecidos. Mas, essa tentativa mostrou-se frustrante diante da dificuldade em diferenciar um do outro.

Hackers são contratados por empresas para proteger seus sistemas contra o ataque de *crackers*. Esta talvez seja a melhor forma de diferenciar os dois tipos. Muitos termos foram criados para conceituar estes novos personagens do ciberespaço. Segundo o dicionário de Eric S. Raymond (2001), esses personagens (*lammer*, *phreaker*, *cracker etc*) se diferenciam dos

hackers pelas formas de atuação de cada um deles. Os *crackers* são classificados de acordo com suas especialidades podendo ser destacados:

WAREZ: São piratas, "crackers" que quebram a proteção de programas,como os que rodam somente com o CD original, os distribuídos com tempo de avaliação, e também distribuem pequenos programas, chamados "crackers", que quando executados geram senhas de programas ou modificam arquivos do sistema para fazer com que um determinado software instalado como demonstração, passe a funcionar por completo;

PHREAKER: especialista em telefonia móvel ou fixa. Eles conseguem invadir centrais telefônicas, o que lhes permite, entre outras coisas, efetuar ligações internacionais sem pagar, fazendo ataques a partir de servidores situados em outros países. Geralmente, um phreaker é um ex-funcionário de companhias, que usa exclusivamente seus conhecimentos para prejudicar as empresas de telefonia.

WHITE HAT: (aka "hacker" ético) "hacker" em segurança, utiliza os seus conhecimentos na exploração e detecção de erros de concepção, dentro da lei. A atitude típica de um White hat é, ao encontrar falhas de segurança, entrar em contato com os responsáveis pelo sistema, comunicando o fato. Geralmente, "hackers" de chapéu branco violam seus próprios sistemas ou sistemas de um cliente que o empregou especificamente para auditar a segurança. Pesquisadores acadêmicos e consultores profissionais de segurança são dois exemplos de "hackers" de chapéu branco;

GRAY HAT: Tem as habilidades e as intenções de um "hacker" de chapéu branco na maioria dos casos, mas por vezes utiliza seu conhecimento para propósitos menos nobres. Um "hacker" de chapéu cinza pode ser descrito como um "hacker" de chapéu branco que às vezes veste um chapéu preto para cumprir sua própria agenda. "hackers" de chapéu cinza tipicamente enquadram-se em outro tipo de ética, que diz ser aceitável penetrar em sistemas desde que o "hacker" não cometa roubo, vandalismo ou infrinja a confidencialidade. Porém, algumas pessoas argumentam que o ato de penetrar em um sistema por si é antiético;

BLACK HAT: (aka cracker ou dark-side hacker) criminoso ou malicioso "hacker", um "cracker". Em geral, "crackers" são menos focados em programação e no lado acadêmico de violar sistemas. Eles comumente confiam em programas de "cracking" e exploram vulnerabilidades conhecidas em sistemas para descobrir informações importantes para ganho pessoal ou para danificar a rede ou sistema alvo;

SCRIPT KIDDIE: Indivíduo que não tem domínio dos conhecimentos de programação, pouco experiente, com poucas noções de informática. Porém, tenta fazer-se passar por um "cracker" a fim de obter fama, o que acaba gerando antipatia por parte dos

“hackers” verdadeiros, cerca de 95% dos ataques virtuais são praticados por script kiddies;

LAMER: Uma pessoa inepta ou ineficaz. Também é empregado para designar uma pessoa que não possui conhecimentos técnicos sobre computadores, porém, faz-se passar por um especialista; e

NEWBIE: É aquele jovem aprendiz de “hacker” que possui uma sede de conhecimento incrível, pergunta muito e é ignorado e ridicularizado na maioria das vezes. Ao contrário do Lamer, não tenta se por acima dos outros, geralmente é muito simples e possui uma personalidade ainda fraca.

A trajetória percorrida durante este trabalho, os desafios impostos, o contato com diferentes conceitos e ideias, a preocupação com o alcance do objetivo proposto e o desejo de fazer desta pesquisa um apoio para o trabalho de segurança cibernética nas corporações privadas, em atendimento a uma necessária demanda atual, foram os motivadores para se chegar ao objetivo por mim mesmo proposto: uma sugestão de um Planejamento Estratégico de Segurança Cibernética.

Para tanto, a primeira parte deste trabalho traz uma explanação sobre conceitos e termos usados em segurança e defesa cibernéticas.

Na segunda parte, serão expostos os principais fatos e eventos ocorridos em telecomunicações e na computação, bem como a segurança e defesa cibernética no mundo e os principais ataques cibernéticos ocorridos nos últimos anos.

Logo depois, em uma terceira parte, serão abordadas as principais ações implementadas por governos em alguns países, inclusive o Brasil, para se protegerem desta nova ameaça.

Na quarta parte, revisaremos alguns conceitos de Planejamento Estratégico e será apresentada uma proposta de ideias para um Planejamento Estratégico de Segurança Cibernética.

Por fim, serão apresentadas, na conclusão, as principais medidas que devem ser adotadas pelas organizações, públicas ou privadas, para se proteger de ataques cibernéticos ou minimizar seus efeitos.

2 BREVE HISTÓRICO DA SEGURANÇA E DEFESA CIBERNÉTICA

2.1 EVENTOS QUE INFLUENCIARAM O MUNDO

O Brasil utilizou os sistemas de telecomunicações elétricas desde que foram inventados, no século XIX.

Já o primeiro computador no Brasil chegou em 1957, com o Univac 120, adquirido pelo governo do Estado de São Paulo, para calcular todo o consumo de água na capital. Em 1959, a empresa Anderson Clayton compra um Ramac 305 da IBM, que foi o primeiro computador do setor privado brasileiro.

As telecomunicações e a computação tiveram uma evolução vertiginosa a partir da segunda metade do século XX.

Os eventos a seguir apresentam os principais fatos de interesse para o presente trabalho ocorridos a partir do final do século XVII, até os nossos dias. Cabe salientar que cada fato aqui enumerado produziu reflexos nos sistemas públicos e privados do mundo, afetando direta ou indiretamente o mundo corporativo e suas relações com os colaboradores e clientes.

Ano	**Evento**
1747	William Watson realizou a transmissão da eletricidade através de um fio.
1837	inventado o telégrafo e o código Morse.
1854	Charles Bourseul publicou seu ensaio sobre a transmissão elétrica do som.
1867	entrou em operação o primeiro cabo de telégrafo a cruzar o oceano Atlântico.
1874	lançamento do primeiro cabo submarino ligando Brasil e Europa.
1876	invenção do Telefone por Alexander Graham Bell.
1877	Bell Telephone Company - primeira companhia telefônica do mundo.
1880	é formada a Telephone Company of Brazil, primeira companhia telefônica do Brasil.
1888	Friedrich Hertz descobriu a onda eletromagnética.
1904	Roberto Landell de Moura inventou o rádio baseado nas ondas eletromagnéticas.
1922	os serviços de telegrafia e telefonia via rádio são introduzidos no Brasil, entre o Rio de Janeiro e Nova Iorque. Nesse mesmo ano foi inaugurada a primeira central telefônica automática do país, em Porto Alegre.
1927	a invenção da televisão, atribuída ao escocês James Hojie Baird.
1946	ENIAC- *Electronic Numerical and Calculator*, o primeiro computador eletrônico digital. O mesmo foi idealizado, inicialmente, para o cálculo de trajetórias balísticas e, posteriormente, para determinar se a bomba H poderia ser construída.

Ano	Evento
1947	criação da 1ª geração de computadores, baseados em tecnologia de válvula.
1952	conclusão do computador IAS, utilizando o conceito de programa armazenado. Foi o predecessor de todos os computadores de propósito geral subsequentes.
1955	criação da 2ª geração de computadores, baseados na tecnologia do transistor.
1957	a então URSS lançou o primeiro satélite do mundo, o Sputinik.
1960	lançados os primeiros satélites de comunicação comercial (INTELSAT e INMARSAT), sob os auspícios de organizações governamentais oficiais.
1962	J. C. R. Licklider, do MIT, foi o primeiro a pensar na possibilidade de uma comunicação global entre computadores.
1965	criação da 3ª geração de computadores, baseados na tecnologia do circuito integrado.
1969	primeira rede de computadores de longa distância. A ARPANET, patrocinada pela DARPA – Agência de Projetos de Pesquisa Avançada do Departamento de Defesa dos Estados Unidos da América (EUA).
1970	inventada a fibra ótica pelo físico indiano Narinder Singh Kapany, nos EUA.
1971	lançado o primeiro "computador pessoal" (PC), o Kenbak-1; o vírus **Creeper** foi uma das primeiras pragas a serem documentadas em computadores na Arpanet (rede fechada de uso militar dos Estados Unidos, que serviu de base para a internet).
1972	criação da 4ª geração de computadores, baseados na tecnologia de microprocessadores.
1975	lançado o PC com “Unidade Central de Processamento” (CPU), o Altair 8800. Bill Gates e Paul Allen desenvolveram uma versão da linguagem "Basic" para o Altair 8800 e fundaram a Microsoft.
1976	Steve Jobs e Steve Wozniak fundaram outra empresa que mudaria o rumo da informática: a Apple.
1977	foi lançado o primeiro microcomputador como se conhece hoje, o Apple II.
1980	introdução da tecnologia de banda larga.
1981	criação do PC-DOS, sistema operacional para as máquinas da IBM.
1982	o **Elk Cloner** foi o primeiro vírus de 'larga escala'. Ele, basicamente, mostrava um poema quando o computador (no caso o Apple II) era inicializado com o disquete infectado.

Ano	Evento
1984	início da fabricação dos computadores pessoais Macintosh ou Mac pela Apple.
1987	a IBM lançou seu micro 386; criação do **vírus Jerusalém** que trazia consequências mais graves, pois apagava tudo o que estivesse rodando no computador nas sextas-feiras 13. O Jerusalém foi um dos primeiros vírus a causar 'malefícios' aos usuários e a ter repercussão global.
1992	surge a Internet; criação do vírus **Michelângelo,** um vírus 'em hibernação', que era uma praga programada para agir em todos os dias 6 de março (data de nascimento do pintor italiano renascentista de mesmo nome). Apesar da demora em agir, o Michelângelo apagava arquivos críticos do HD do computador.
1993	lançamento do Windows NT (significa *New Technology* em inglês) pela Microsoft.
1995	lançamento, em 24 de agosto, do Windows 95.
1998	lançamento do Windows 98.
1999	criação do vírus **Melissa** que infectava documentos do Word e os mandava para todos os contatos do Outlook do usuário.
2000	criação do vírus "I love you". Após abrir o arquivo anexo, o usuário infectava seu PC e o e-mail era mandado para todos os contatos de seu programa de e-mail.
2001	assinatura do pacto de Xangai entre China, Rússia e outros países centro-asiáticos; lançamento do Windows XP (a sigla **XP** deriva da palavra ***eXPe****rience*, em inglês) pela Microsoft; criação do vírus **Code Red,** que foi feito para infectar servidores web. Ele aproveitava uma falha dos sistemas operacionais da Microsoft utilizados em servidores (Windows 2000 e NT) e trocava a página da web por uma com os dizeres: "Hacked by Chinese" (Hackeado por chineses). Além da mensagem, outra característica do Code Red é que ele, ao infectar uma máquina, direcionava ataques de negação de serviço (DDOS) para o site da Casa Branca, sede do governo americano, sendo o primeiro caso de 'hackerativismo' (quando usuários utilizam ataques via web para atingirem governos ou pessoas por uma causa ideológica) em larga escala.
2003	lançamento da *National Strategy to Secure Cyberspace* (Estratégia Nacional para Segurança do Espaço Cibernético) pelos EUA.
2004	criação do vírus Sasser, que explorava uma falha em computadores com o sistema operacional Windows. Ele, simplesmente, fazia com que a máquina infectada desligasse durante certo intervalo de tempo (alguns minutos) ininterruptamente.

Ano	Evento
2005	criação do vírus MyTob, que muito mais que um vírus, o MyTob tornava os computadores membros de uma botnet (rede de computadores zumbis que podem ser controlados por criminosos para comandar ataques).
2007	criação do vírus **Storm,** que criou uma rede de computadores zumbis descentralizada chamada Storm botnet. Em sua melhor fase, estima-se que a Storm botnet tenha infectado cerca de 50 milhões de sistemas e que a rede zumbi era responsável por 8% de todos os malwares que circulavam no mundo.
2008	criação do vírus **Koobface,** que com o advento das redes sociais, recrutava computadores zumbis por meio delas. O Koobface (o nome foi inspirado no Facebook) usava uma falsa visualização do plugin flash para ver um vídeo. Ao baixá-la, o usuário instalava automaticamente o vírus em seu computador. A estimativa é que o Koobface conseguiu juntar mais de 500 mil estações zumbi online.
2009	lançamento do Windows 7; criação do vírus **Conficker**, que aproveitava brechas de segurança do sistema Windows. Ao todo, estima-se que a praga infectou sete milhões de usuários da internet, além de aviões de caça franceses , hospitais e bases militares. Além disso, removê-lo era uma tarefa árdua: de cara ele impedia a restauração do sistema e o acesso a algumas páginas de antivírus.
2010	criação do *U.S. Cyber Command* pelos EUA; liberado o vírus **Stuxnet** que é um vírus muito complexo e que explora várias falhas de sistemas Windows. Ele funciona da seguinte forma: após infectar um computador, o vírus busca na rede em que ele é instalado o software Skoda, feito pela Siemens. Este programa é responsável pelo controle de sistemas industriais, como o de uma usina nuclear, por exemplo.
2010	O Irã, uma das vítimas, acredita que o vírus foi feito por alguma nação que quer espionar o sistema nuclear iraniano. A iniciativa foi vista como um sinal de início da guerra cibernética. A problemática do Wikileaks começa a tornar preocupante devido ao

Ano	Evento
2010 continuação	vazamento de dezenas de informações que eram sigilosas. Ao longo do ano de 2010, o WikiLeaks publicou grandes quantidades de documentos confidenciais do governo dos Estados Unidos, com forte repercussão mundial. Em abril, divulgou um vídeo de uma fato de 2007, que mostrava o ataque de um helicóptero Apache estado unidense, matando pelo menos 12 pessoas - dentre as quais dois jornalistas da Reuters em Bagdá, no contexto da ocupação do Iraque. Outro documento polêmico mostrado pelo Wikileaks é a cópia de um manual de instruções para tratamento de prisioneiros na prisão militar estado-unidense de Guantánamo, em Cuba. Em julho do mesmo ano, WikiLeaks promoveu a divulgação de uma grande quantidade de documentos secretos do exército dos Estados Unidos, reportando a morte de milhares de civis na guerra do Afeganistão em decorrência da ação de militares norte-americanos. Finalmente, em novembro, publicou uma série de telegramas secretos enviados pelas embaixadas dos Estados Unidos ao governo do país.
2013	O ex-técnico da CIA Edward Snowden, de 29 anos, é acusado de espionagem por vazar informações sigilosas de segurança dos Estados Unidos e revelar em detalhes alguns dos programas de vigilância que o país usa para espionar a população americana – utilizando servidores de empresas como Google, Apple e Facebook – e vários países da Europa e da América Latina, entre eles o Brasil, inclusive fazendo o monitoramento de conversas da presidente Dilma Rousseff com seus principais assessores.

2.2 SEGURANÇA E DEFESA CIBERNÉTICAS

Os termos segurança e defesa são, conceitualmente, distintos. Na prática, são extremamente difíceis de ser balizados. Esses conceitos estão já em discussão há alguns anos e ainda não se encontrou um consenso que defina de forma definitiva essas duas ideias. Uma concepção coerente é que **Segurança** é um estado, um sentimento de estar livre de ameaças ou longe delas e é decorrente de ações que buscam eliminar as vulnerabilidades. Para os Estados, essas ações têm a ver com os denominados campos do poder (político, psicossocial, científico-tecnológico, econômico e militar). Uma concepção de **Defesa** é que é um ato, um conjunto de medidas, ações e recursos orientados para a manutenção da segurança, cabendo à área militar a

responsabilidade primária por sua execução. Sem segurança não existirão condições para o desenvolvimento econômico e social de um país, portanto, as questões relativas à segurança devem sempre preceder o estabelecimento de uma política de defesa.

Portanto, quando se fala em mundo corporativo, mundo privado, o correto é se falar em segurança cibernética, ou governança para segurança cibernética.

Atualmente, tudo depende de computadores e da internet: a comunicação (celulares, email), entretenimento (TV a cabo digital, MP3), transporte (sistemas de carro motor, navegação de aeronaves, metrôs), shopping (lojas online, cartões de crédito), medicina (equipamentos, registros médicos) dentre outros. A vida diária das pessoas depende de computadores. Muitas informações pessoais são armazenadas em computadores. Defesa e segurança cibernética envolvem proteger essa informação por prevenção, detecção e resposta a ataques.

Existem várias definições de segurança cibernética, mas, para fins de padronização e uso neste trabalho, usar-se-á a da Secretaria Executiva do Conselho de Defesa Nacional, assim descrita na Portaria 45:

> é a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas (Portaria 45 SE-CDN, 2009).

Quanto a esse espaço cibernético, o seu domínio está entrando em uma fase potencialmente caótica e muito perigosa de sua evolução, razão pela qual se tornou um dos assuntos principais da pauta do G8 em Deauville, em maio de 2011, na França. Como é de conhecimento geral, apenas para relembrar, o G8 é um grupo internacional que reúne os sete países mais industrializados e desenvolvidos economicamente do mundo, mais a Rússia. Atualmente, com a crise da Ucrânia, a Rússia não deverá mais fazer parte do G8.

É lugar comum hoje em dia dizer que segurança das informações virou prioridade para empresas de todos os segmentos e portes. Dados não faltam para justificar essa crescente preocupação: 60.000 novos malwares (softwares maliciosos) por dia; 8 mil novos sites infectados por dia; mais de 100 bilhões de spam's disparados diariamente pelo mundo todo; além dos incontáveis danos causados às informações corporativas por imperícia ou negligências dos próprios funcionários, sabotagem, defeitos em equipamentos e outros. Como eu sempre digo e ensino, uma pequena falha em um sistema hoje, embora não parecendo ameaçadora, poderá ser o grande motivador de uma falência amanhã.

Um enorme mercado negro de ferramentas e produtos para crimes cibernéticos

prospera como uma espécie de submundo escondido da globalização, dirigindo tudo, desde o roubo de identidades até crimes de espionagem política e comercial.

Atualmente, novos desafios são enfrentados dia após dia e, no mundo corporativo, tornam-se parte das políticas de negócios, pois se transformam em verdadeiros obstáculos na busca por mercados. A maioria desses obstáculos são, também, os maiores desafios do Estado, mas exercem grande influência no mundo corporativo: pobreza extrema e pessoas vivendo à margem da dignidade humana (não como óbice, mas desafio a ser vencido, pois há grande influência na mão de obra existente), terrorismo, crime transnacional, armas de destruição em massa, drogas, corrupção, tráfico de armas, lavagem de ativos, desastres naturais, tráfico ilícito de pessoas e ataques à segurança cibernética. Tudo isso tem um reflexo enorme nas empresas e pessoas que trabalham com segurança privada, seja pela legislação vigente, que acaba regulando a atividade profissional, seja pela influência que exerce, pelas ameaças, diretamente nos agentes que atuam nesse nicho profissional.

2.3 UM GIRO PELO MUNDO

Após os ataques aos EUA, em 11 de setembro de 2001, foi realizada a Convenção do Conselho Europeu, também chamada de Convenção de Budapeste, em 23 de novembro de 2001, na cidade de mesmo nome, na Hungria, para tratar de crimes cibernéticos. Na pauta estavam os seguintes assuntos: Segurança Cibernética (uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informações e redes de computadores), ações elaboradas para obtenção de vantagens (na área militar e civil) e guerras assimétricas (viabilidade com baixo custo x grande impacto).

A partir dessa convenção, foi elaborado um tratado que entrou em vigor no dia 1º de julho de 2004. Os Estados Unidos são o único país de fora do Conselho Europeu que o ratificou, sendo que 19 países europeus já ratificaram o tratado.

O Brasil não participou da convenção e, de acordo com o então Secretário-Geral do Ministério das Relações Exteriores, em 2007, Samuel Pinheiro Guimarães, o país só pode se tornar signatário do tratado se for convidado pelo Comitê de Ministros do Conselho Europeu.

O Brasil, se obrigado pelo Congresso Nacional, a aderir ao tratado, terá de legislar sobre os crimes tipificados na Convenção. O Ministério da Justiça, através do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional, o Gabinete de Segurança Institucional da Presidência da República, o Departamento de Polícia Federal, o Ministério de

Ciência e Tecnologia e o Ministério das Relações Exteriores, estão analisando a Convenção à luz do ordenamento jurídico brasileiro.

Na avaliação do Itamaraty, é um acordo complicado se aplicar, embora seja o único tratado internacional de combate aos crimes cibernéticos.

Atualmente, não existe um país que esteja preparado ou com melhores equipamentos para fazer frente a um ataque cibernético. Todos os países são extremamente frágeis e sabem disso. Uns mais, outros menos, mas a ameaça é um gigante adormecido, pronto para levantar e agir. Os países desenvolvidos, por seu turno, possuem tecnologia para poder atenuar suas vulnerabilidades.

Vários países estão fazendo acordos (EUA e Índia; França e Reino Unido; França e Estônia; EUA e Canadá, entre outros) e a cooperação bilateral é mais eficaz que a multilateral.

Entretanto, um problema enfrentado por qualquer país nos dias atuais são os investimentos em ciência e tecnologia. A mesma situação sofre a corporações, pois, inserida em um mercado de pouca expansão tecnológica, a empresa sofrerá, obviamente, as restrições que essa situação lhe imporá.

O desenvolvimento tecnológico cria vantagens que podem superar as vantagens comparativas tradicionais entre as nações. Neste contexto, investimentos em ciência e tecnologia são fundamentais para que o Estado possa ter condições de prover e manter a sua defesa. Isso se aplica também ao mundo empresarial, comercial, ou seja, privado.

Quando uma empresa não detém determinada tecnologia e seu país, por seu turno, também não domina essa tecnologia, certamente uma operação de importação será efetivada para que essa empresa tenha aquele produto, ferramenta ou instrumento que esteja buscando. Ocorre que, do mesmo modo que a dependência tecnológica cria rastros de busca para governos que vendem equipamentos de última geração, no mundo dos negócios, isso ocorre e eu diria: “mais abertamente ainda”.

Um concorrente que tenha relações com um determinado fornecedor, no caso do mundo cibernético, vai conseguir retirar dados de seu oponente comercial apenas pelo fato da dependência tecnológica que se estabelecerá entre o fornecedor (estrangeiro normalmente) e o comprador. Exemplo. A empresa A italiana vende para a empresa C equipamentos de TI que poucos fabricam. A empresa B, concorrente de C e parceira comercial de A, poderá obter dados de sua concorrente por meio da empresa A. Isso é montagem mental, mas extremamente factível nos dias de hoje, em que o espaço cibernético é uma grande incógnita.

O Coronel T. X. Hammes, da reserva do Corpo de Fuzileiros Navais dos EUA, escreveu na Revista Military Review em Out 2007, que outra tendência que se apresenta em

relação à guerra cibernética é a que esse tipo de conflito estaria ligado aos conflitos de 5ª geração, ou seja, acima dos Estados e atores desconhecidos. Ainda segundo ele, as tendências políticas, econômicas e sociais apontam para a emergência de indivíduos extremamente poderosos ou pequenos grupos unidos pela devoção a uma causa mais do que a uma nação. Ao empregarem tecnologias emergentes eles serão capazes de criar um nível de poder destrutivo que costumava a exigir os recursos de uma nação-estado.

Outra medida fundamental para a garantia da defesa encontra-se na manutenção de um sistema de inteligência eficiente e eficaz, capaz de assessorar o processo decisório e garantir a preservação do Estado e da sociedade contra ameaças reais ou potenciais. Isso, obviamente, se aplica ao mundo corporativo. Verifica-se, nesse ponto, que segurança cibernética vai além das tecnologias de informação e comunicações, envolve outros sistemas da organização, como, por exemplo, pessoal e inteligência, apenas para citar em uma primeira observação. Pode envolver outros.

Com isso, a Inteligência Cibernética nada mais é do que um processo em que o espaço cibernético é o seu grande campo de trabalho, objetivando a obtenção, a análise e a capacidade de produção de conhecimentos baseados nas ameaças virtuais e com caráter prospectivo, suficientes para permitir formulações, decisões e ações de defesa e resposta imediatas visando à segurança virtual de uma empresa, organização e/ou Estado.

2.4 ATAQUES CIBERNÉTICOS NO MUNDO

Durante uma conferência em Nova York, Shawn Henry, diretor adjunto da divisão informática do *Federal Bureau of Investigation* (FBI), disse que os ataques cibernéticos estão entre as três maiores ameaças na atualidade. Segundo Shawn[1], após anos lutando contra os criminosos da internet, o FBI e os serviços de segurança de outros países sabem, agora, que os hackers são os inimigos mais difíceis de pegar. Christopher Painter, um perito do FBI especializado nas redes de cooperação internacional, destacou, nesta mesma conferência citada acima, que um dos pontos fracos da luta pela segurança em informática é a invisibilidade da ameaça.

Uma das mais assustadoras consequências da guerra cibernética é que o dano não é sempre limitado às redes e sistemas. Ele pode ser físico também. Em 1982, a *Central Intelligence Agency* (CIA) mostrou o perigo de uma "bomba lógica". Essa “bomba” causou a

[1] Disponível em:< http://www.fbi.gov/news/pressrel/press-releases/shawn-henry-named-assistant-director-of-fbi-cyber-division>. Acesso em: 20 mar. 2014.

explosão de um gasoduto soviético na Sibéria, descrito por um secretário da Força Aérea Americana como "uma monumental explosão de incêndio não nuclear jamais visto do espaço," sem o uso de um míssil ou uma bomba, mas uma sequência de código de computador. Hoje, com a proliferação de controle de computador, os alvos possíveis são praticamente infinitos.

Em 2004, um empregado da *Sandia National Laboratories*, nos EUA, descobriu uma série de invasões cibernéticas. ***Titan rain*** foi o nome dado pelo FBI a estes ataques, onde se verificou que várias redes de computadores foram infiltradas por *hackers*, como a da *Lockheed Martin*, *Sandia* (propriedade da *Lockheed*) e da *National Aeronautics and Space Administration* (NASA). O perigo, neste caso, não foi só os atacantes furtarem dados militares classificados e de inteligência, mas sim o de deixarem *backdoors*[2] e *zumbis*[3] nas máquinas, que fazem com que a espionagem cibernética seja mais fácil no futuro. Esses ataques partiram da China e acredita-se que tiveram o apoio do governo daquele país. *Titan rain* é considerado um dos maiores ataques cibernéticos da história.

Outro ataque muito semelhante ao *Titan Rain* foi o *Moonlight Maze* onde os hackers penetraram nos sistemas de computação das Forças Armadas norte-americanas cujos alvos eram os mapas, esquemas militares e configuração das tropas dos EUA. O ataque teria sido feito em 1998 e, durante dois anos, dados militares foram subtraídos do Pentágono, da NASA, do Departamento de Energia e, também, de universidades e laboratórios de pesquisa. Os EUA acusaram a Rússia pelo ataque, mas esta negou o envolvimento.

Em 2007, o que aconteceu com a Estônia foi considerado um modelo de como uma nação pode ser vulnerável a ataques cibernéticos durante um conflito. A Estônia é um país altamente informatizado, sendo um dos pioneiros na tecnologia do "governo eletrônico"[4] e por isso é muito vulnerável a ataques virtuais. Em um breve período de tempo, os sites do parlamento, da presidência, dos ministérios, de partidos políticos, dos serviços de saúde e tecnologia, dois grandes bancos e empresas da área de comunicação foram afetados. A característica dos ataques foi a de "ataque distribuído de negação de serviço" (também

---

[2] *Backdoor* é um cavalo de tróia de acesso remoto formado por dois componentes: um que ataca o servidor e outro que é instalado na máquina do usuário. Quando executado, ele permite que o hacker se conecte e administre a máquina do usuário utilizando o código instalado no PC. Disponível em: < http://www1.folha.uol.com.br/folha/informatica/ult124u11798.shtml>. Acesso em: 27 mar. 2014.

[3] O nome se refere a computadores caseiros controlados remotamente por um invasor para cometer crimes, sem que seu dono desconfie. Disponível em: < http://veja.abril.com.br/081106/p_134.html >. Acesso em 01 abr. 2014.

[4] O governo eletrônico (e-*government*) é um processo de informatização das ações de um governo, procurando facilitar e tornar operações burocráticas mais rápidas, além de tentar aproximar mais as ações do governo dos cidadãos. Disponível em:< http://www.pucminas.br/imagedb/conjuntura/CNO_ARQ_NOTIC20070704113456.pdf?PHPSSID=40d7b2656db775ea31268bf3df1c04cc>. Acesso em: 17 mar. 2014.

conhecido como **DDoS**, um acrônimo em inglês para *Distributed Denial of Service*). Ataques DDoS são caracterizados por solicitações em massa para um único site ou servidor, fazendo com que ele não suporte o tráfego e fique indisponível para outros usuários. O ataque foi um dos maiores após o *Titan Rain* e foi tão complexo, que os atacantes poderiam ter tido apoio do governo russo e de grandes empresas de telecomunicações.

Durante a campanha presidencial de 2007, Barack Obama e John McCain tiveram seus e-mail e seus dados confidenciais acessados por uma entidade estrangeira ou organização. O FBI teve que recolher todos os computadores, telefones celulares e dispositivos eletrônicos da campanha para averiguações e substituí-los. As suspeitas recaíram sobre a China ou Rússia, mas a autoria não pôde ser comprovada.

Em agosto de 2008, ocorreu um incidente envolvendo a Rússia. Durante os conflitos separatistas ocorridos na região da Geórgia e Ossétia do Sul, sites do governo da Geórgia foram bloqueados numa ação em massa coordenada por nacionalistas russos. O governo russo negou qualquer participação.

Em março de 2009, foi divulgado um extenso relatório intitulado *Tracking GhostNet: Investigating a Cyber Espionage Network*, relativo a uma pesquisa realizada pelo site *Information Warfare Monitor*, ligado ao laboratório multidisciplinar *Munk Centre for International Studies*, da Universidade de Toronto que apontou ataques cibernéticos em mais de 100 países (Mandarino, 2009, p 47).

No feriado de Independência dos Estados Unidos, em 4 de julho de 2009, houve o bloqueio de vários sites do governo e de empresas norte americanas, incluindo a página da Casa Branca e da Bolsa de Valores de Nova York. Uma semana depois, a vítima foi à Coréia do Sul, aliada dos EUA. Ambos os ataques teriam partido da vizinha Coréia do Norte, nação comunista alinhada à China. O governo norte coreano negou qualquer participação nos incidentes.

Em 2010, mais de 286 milhões de novas pragas virtuais foram identificadas no mundo, de acordo com Relatório de Ameaças à Segurança na Internet (*Internet Security Threat Report* – ISTR), elaborado pela Symantec. Os resultados apresentados mostram que houve aumento na frequência e na sofisticação dos ataques direcionados às empresas. Isso se deve pelo surgimento das novas tecnologias e a popularização dos dispositivos móveis. Agora, o grande desafio das empresas não é mais proteger os equipamentos onde os dados estão armazenados, mas sim blindar as informações sensíveis dos negócios. Essa mudança faz com que os gestores de tecnologia da informação (TI) e as organizações repensem as estratégias de segurança da informação.

Em agosto de 2011, Dmitri Alperovitch, vice-presidente da divisão de análises de

ameaças da McAfee, empresa norte americana de software de segurança, afirmou ter descoberto o que pode ser considerada a maior série de ataques cibernéticos da história. Segundo a empresa, mais de 70 entidades foram alvo de um mesmo *cyber* ataque conduzido por um único autor nos últimos cinco anos. Os incidentes comprometeram dados de governos e organizações dos EUA, Canadá, Coréia do Sul, Vietnam, Taiwan, Japão, Suíça, Reino Unido, Indonésia, Dinamarca, Cingapura, Hong Kong, Alemanha e Índia, além da Organização das Nações Unidas (ONU). No caso da ONU, os hackers invadiram o sistema em 2008 e se "esconderam" por dois anos. Durante esse período, vasculharam e acessaram diversos dados secretos. Grande parte dos ataques teve duração de um mês. O mais longo deles, porém, que afetou o Comitê Olímpico de um país asiático, chegou a durar 28 meses. Nessa modalidade de ataque o que se busca, em princípio, é a obtenção de informações confidenciais e de propriedade intelectual, antes de visar o lucro imediato. Evidências apontam a China como autora dos ataques.

Outro ponto importante a se ressaltar são os ataques por motivação política, que têm aumentado nos últimos anos. Ataques cibernéticos como a do grupo "Anônimos"[5], que, em represália a serviços que boicotaram o WikiLeaks[6], derrubou sites de instituições como Visa, MasterCard, PayPal, além dos governos holandês e sueco, irão aumentar.

Por fim, nesta seção, é importante relembrar o caso mais recente sobre espionagem e cibernética. O caso Snowden. O ex-técnico da CIA Edward Snowden, de 30 anos, é acusado de espionagem por vazar informações sigilosas de segurança dos Estados Unidos e revelar em detalhes alguns dos programas de vigilância que o país usa para espionar a população americana -utilizando servidores de empresas como Google, Apple e Facebook- e vários países da Europa e da América Latina, entre eles o Brasil, inclusive fazendo o monitoramento de conversas da presidente Dilma Rousseff com seus principais assessores. Detalhes de todas as atividades que envolveram este caso foram publicados no G1 de 02/07/2013[7].

3 GOVERNANÇA CIBERNÉTICA – ÁREA GOVERNAMENTAL

3.1 ALGUNS EXEMPLOS ATUAIS

[5] Disponível em:< http://en.wikipedia.org/wiki/Anonymous_(group)>. Acesso em 10 mar. 2014.
[6] É uma organização transnacional sem fins lucrativos, sediada na Suécia, que publica, em seu *site*, *posts* de fontes anônimas, documentos, fotos e informações confidenciais, vazadas de governos ou empresas, sobre assuntos sensíveis. Disponível em:< http://pt.wikipedia.org/wiki/WikiLeaks>. Acesso em: 10 mar. 2014.
[7] Disponível em <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>, acesso em 01 Abr 14.

De um modo geral, governança possui vários conceitos e definições. Entretanto, para fins de homogeneizar os conceitos, neste trabalho procurou-se focar o seguinte conceito:

> Governança é o conjunto de processos, regulamentos, decisões, costumes, ideias que mostram a maneira pela qual aquela empresa ou sociedade é dirigida ou administrada (GONÇALVES, 2005).

Assim, como o foco deste trabalho é uma proposta de planejamento estratégico para essa área tão nova e sensível, não há como deixar de falar das experiências que alguns países vêm obtendo com a governança do setor cibernético.

Falar-se-á de EUA, Reino Unido, Alemanha e Brasil para que se tenha uma ideia de como essa pauta caminha nos citados países.

No caso dos EUA, eles sofreram, nos últimos anos, inúmeros ataques cibernéticos, desde suas redes domésticas até as principais instituições do país, como a NASA e a CIA. Atualmente, toda a infraestrutura americana é baseada nas redes de computadores.

Neste contexto, o governo dos EUA criou, em 2009, o *United States Cyber Command* (USCYBERCOM)[8] para centralizar o comando das operações no espaço cibernético, organizar os recursos cibernéticos existentes e sincronizar a defesa de redes militares dos EUA.

A capacidade operacional do USCYBERCOM iniciou em 21 de Maio de 2010. Para que se tenha uma exata noção da importância destinada a este novo órgão, foi nomeado para o comando o General Keith B. Alexander. A nomeação de um General para o Comando demonstrou, também, o receio que os americanos têm de ataques cibernéticos.

A rede elétrica dos EUA, bem como outros pontos críticos e infraestruturas críticas, ainda estão, nos dias atuais, vulneráveis a ataques cibernéticos treze anos depois de o então presidente Bill Clinton (1993-2001) ter declarado que proteger a infraestrutura crítica era uma prioridade nacional.

Importante destacar que o entendimento sobre a necessidade de se legislar sobre o assunto defesa cibernética tem se mostrado uma ação de Estado, pois ultrapassa os limites temporais de governos.

Entretanto, não basta existir a legislação, é preciso que os órgãos interajam entre si. O controle ao acesso, bem como a gestão da Segurança da Informação e Comunicações na administração Pública Federal, direta e indireta, e nas empresas privadas são passos necessários à coordenação das atividades, bem como a articulação e estreita colaboração dos órgãos e

[8] Disponível em: < http://www.defense.gov/home/features/2010/0410_cybersec/>. Acesso em 12 mar. 2014.

entidades públicas ou privadas.

Os esforços mostram como a administração do presidente Barack Obama está lutando para diminuir brechas no espaço cibernético norte americano. Esses esforços são, principalmente, na área militar, no entanto, a diferença global parece estar aumentando, pois os adversários e os criminosos se movem mais rápido do que o governo e as corporações, e as tecnologias, tais como aplicativos móveis para telefones inteligentes, proliferam mais rapidamente do que os políticos, funcionários e analistas podem responder.

Essa lentidão do governo se revela na falta de políticas para o setor, pois não existe consenso sobre o assunto pela falta de um debate esclarecendo-o.

O subsecretário do Departamento de Defesa dos Estados Unidos, William Lynn, revelou que os ataques cibernéticos se tornaram um problema significativo nos últimos dez anos, nos quais "invasores estrangeiros" extraíram *terabytes* de dados das redes corporativas de empresas de defesa. Segundo Lynn[9]: "em uma única invasão em março de 2011, foram roubados 24 mil arquivos de uma companhia terceirizada pelo Pentágono,[...] assinalou que a infraestrutura, rede logística e os sistemas de trabalho do Departamento de Defesa dos Estados Unidos estão muito informatizados. Com 15 mil redes e mais de 7 milhões de dispositivos informáticos, o Departamento de Defesa continua sendo um alvo de ataques no ciberespaço."

Para destacar a necessidade crescente de segurança cibernética, o presidente dos EUA, Barack Obama, instituiu o mês de outubro como sendo o "mês da consciência nacional de segurança cibernética". Com isso, o presidente dos EUA está tentando criar, cultivar e ampliar a cultura de segurança cibernética naquele país.

Os EUA já executaram três exercícios (chamados de *Cyber Storm*) de grande vulto, simulando ataques cibernéticos. Os *Cyber Storm I, II* e *III* foram realizados em fevereiro de 2006, março de 2008 e novembro de 2010, respectivamente, com o objetivo de testar a capacidade do governo e das corporações na identificação, em tempo real, dos ataques cibernéticos em curso e a capacidade de sanar os problemas e as vulnerabilidades.

O planejamento do exercício ficou a cargo da National Cyber Security Division (NCSD), subordinada ao Department of Homeland Security (DHS). A NCSD trabalha em colaboração com entidades públicas, privadas e internacionais para proteger ciberespaço e infraestruturas cibernéticas dos EUA. Para isso, foram marcados dois grandes objetivos[10]:

---

[9] Disponível em:< http://blogs.estadao.com.br/link/hackers-roubaram-24-mil-documentos-do-pentago-no/>. Acesso em 18 mar. 2014.

[10] Disponível em:<http://www.dhs.gov/xabout/structure/editorial_0839.shtm> e em http://www.dhs.gov/files/training/gc_120473827585.shtm Acesso em 10 mar. 2014.

construir e manter um sistema de resposta nacional eficaz para o ciberespaço e, segundo, implementar um programa de gerenciamento de risco para a proteção da infraestrutura cibernética.

A NCSD coordena os processos e os protocolos que vão determinar quando e quais as medidas que devem ser tomadas quando surgirem incidentes cibernéticos. Para tanto, conta com os seguintes programas:

Preparação para segurança cibernética e *National Cyber Alert System* - ameaças virtuais estão mudando constantemente. Usuários de computadores (técnicos e não técnicos) recebem informações atualizadas por meio do *National Cyber Alert System*;

US-CERT Operações - US-CERT é responsável pela análise e redução das ameaças cibernéticas e vulnerabilidades, difusão de aviso de ameaça cibernética e coordena as atividades de resposta a incidentes.

NCRCG - *National Cyber Response Coordination Group* (Grupo Nacional de Coordenação de Resposta Cibernética) - Composto por 13 agências federais, é o principal mecanismo da agência federal para resposta a incidentes cibernéticos. No caso de um incidente significativo, a nível nacional, o NCRCG vai ajudar a coordenar a resposta federal, incluindo US-CERT, a aplicação da lei e a comunidade de inteligência.

Cyber Cop Portal - Coordenação com a aplicação da lei para ajudar a capturar e condenar os responsáveis por ataques cibernéticos.

Cyber Storm III foi o principal meio que o DHS teve para verificar a validação do recém criado *National Cyber Incident Response Plan* (NCIRP) ou Plano Nacional de Resposta a Incidentes Cibernéticos. O plano prevê as responsabilidades das autoridades e as atribuições dos elementos-chave da nação nas respostas a um incidente cibernético. Com o exercício *Cyber Storm III*, pôde-se realizar a análise das lições aprendidas e atualizar o NCIRP.

A administração de Barack Obama iniciou, em abril de 2011, uma estratégia para a proteção dos consumidores online e de apoio à inovação intitulada *National Strategy for Trusted Identities in Cyberspace (NSTIC)*, que visa proteger os consumidores contra fraudes e roubo de identidade, reforçar a privacidade dos indivíduos e promover o crescimento econômico, permitindo que as empresas proporcionem mais serviços online e também criem novos serviços. Com o NSTIC, as transações online serão mais confiáveis, dando às empresas e aos consumidores maior confiança na realização de negócios online. A meta de NSTIC é criar um "Ecossistema de Identidade" em que haverá interoperabilidade, segurança e credenciais confiáveis disponíveis aos consumidores.

A realidade é que a internet transformou o modo como nos comunicamos e fazemos

negócios, a abertura dos mercados e de conectar a nossa sociedade como nunca antes. Em contrapartida, levou a novos desafios, como o enfrentamento a fraudes online e roubo de identidade, que prejudicam os consumidores e custam bilhões de dólares a cada ano.

Em 16 de maio de 2011, Barack Obama anunciou aos Estados Unidos a *International Strategy for Cyberspace* (Estratégia Internacional para o Cyberespaço). Howard A. Schmidt, coordenador de segurança cibernética da Casa Branca, ressaltou que a Estratégia Internacional é um documento que explica, para o público interno americano e para o mundo, como os EUA planejam aumentar a segurança e salvaguardar os interesses da rede de internet. O documento também define uma agenda de parcerias com outras nações e povos para alcançar os objetivos propostos.

Corroborando com esta estratégia, os EUA e a Índia assinaram, em 19 de julho de 2011, um memorando de entendimento para promover uma cooperação mais estreita e o intercâmbio oportuno de informações entre as organizações responsáveis pela segurança cibernética dos dois países. O memorando estabelece o intercâmbio de informações críticas de segurança cibernética e a troca de experiências entre os dois governos por meio do *Indian Computer Emergency Response Team (CERT-In)*, do Departamento de Tecnologia da Informação, Ministério das Comunicações e Tecnologia da Informação da Índia e o *United States Computer Emergency Readiness Team28 (US-CERT)*, subordinado ao *Department of* 33 *Homeland Security* (*DHS*). Com esse acordo, tanto os Estados Unidos quanto a Índia terão a capacidade de coordenar uma ampla gama de questões técnicas e operacionais do ambiente cibernético.

Outra ação implementada pelo governo norte americano é uma campanha que se chama: *"Stop. Think. Connect."* É uma campanha nacional norte-americana de conscientização pública, destinada a aumentar a compreensão sobre as ameaças cibernéticas e capacitar as pessoas a estarem mais seguras e protegidas online. A campanha traz as seguintes mensagens (já traduzido):

Stop* (Pare)*: antes de usar a Internet, tenha tempo para compreender os riscos e aprenda a detectar potenciais problemas.

***Think* (Pense):** espere um momento e tenha a certeza que o caminho a seguir é o correto. Preste atenção nos sinais de alerta e considere como as suas ações online poderiam ter impacto na sua segurança ou da sua família.

***Connect* (Conecte):** desfrute da Internet com mais confiança, sabendo que você tomou as medidas corretas para proteger você e seu computador.

Na Europa, o Reino Unido e a Alemanha são países que já perceberam melhor as

necessidades de defesa cibernética e iniciaram ações para protegerem seus cidadãos e o Estado de ataques.

Os britânicos têm a noção que não estão significativamente protegidos e estão investindo, no ano de 2011, cerca de 650 milhões de libras esterlinas (cerca de R$ 1,6 bilhões de reais) para a área de defesa cibernética.

O Conselho de Segurança Nacional, criado por David Cameron, em maio de 2010, publicou uma nova *National Security Strategy* para o Reino Unido. Esta estratégia descreve como o Reino Unido irá utilizar a sua infraestrutura para permitir uma reação rápida e eficaz às novas ameaças segurança do país. O documento identifica 16 (dezesseis) ameaças ao Reino Unido. A mais grave - o que é chamado "*Tier 1*" – constitui-se: em atos de terrorismo internacional; ataques cibernéticos hostis a computadores do Reino Unido; um acidente grave ou de desastres naturais, tais como uma pandemia de gripe; e uma crise internacional militar entre os estados que compõem o Reino Unido e seus aliados.

Atualmente, a conclusão que britânicos possuem é que esse país precisa de uma maior capacidade para se proteger, não só contra ataques cibernéticos ao governo, mas também contra as empresas e sobre os indivíduos. O Reino Unido enfrenta um complexo conjunto de ameaças de uma miríade de fontes. A Estratégia Nacional de Segurança descreve o contexto estratégico em que estas ameaças surgem, e como eles podem se desenvolver no futuro. Nosso interesse nacional exige o nosso compromisso contínuo, pleno e ativo nos assuntos mundiais.

Na Alemanha, desde janeiro de 2008, companhias de telecomunicações foram obrigadas a guardar, por motivo de segurança, dados das chamadas telefônicas e do tráfego de internet dos seus usuários durante seis meses. No dia 2 de março de 2010, o Tribunal Constitucional Federal definiu, no entanto, que esse armazenamento de dados é incompatível com a Lei Fundamental do país.

A confusão em torno do novo serviço do gigante da internet Google, o chamado *Street View*, mostrou o quanto a proteção de dados privados é algo sagrado para os alemães. Desde meados de novembro de 2010, qualquer pessoa pode explorar pela internet as primeiras 20 cidades alemãs escaneadas pelo Google. Antes do lançamento do serviço, porém, houve uma discussão acalorada em torno do tema proteção da privacidade. No final, cerca de 250 mil cidadãos obrigaram a companhia a *pixelizar* as fachadas de suas casas no *Street View*.

Durante o ano de 2009, a Alemanha registrou 900 ataques cibernéticos aos computadores do governo. Este número quase que dobrou em 2010, que passou a ser de 1,6 mil ataques. A maioria dos ataques foram provenientes da China.

Ataques cibernéticos são bastante frequentes na Alemanha. Na 47ª Conferência de

Segurança de Munique, ocorrida em 2010, a 1ª ministra lemã, Angela Merkel, afirmou que os ataques cibernéticos são tão perigosos quanto uma guerra convencional. Conforme informações do Ministério do Interior, em 2010, a cada dois segundos, houve um ataque à internet na Alemanha.

Por conta disso, em 16 de junho de 2011, foi inaugurado o centro de defesa cibernética em Bonn, com o objetivo de prevenir e investigar crimes no ciberespaço. A Alemanha mostra preocupação com *ciberataques* a setores estratégicos como o abastecimento energético. O centro, que está ligado ao Departamento para Segurança na Tecnologia de Informação (BSI36) da Alemanha, iniciou suas atividades em abril de 2011 e mantém um ritmo intenso de trabalho.

O comissário para Indústria da União Européia, Antonio Tajani, afirmou o seguinte:

Uma situação que deve chamar a atenção é o interesse chinês em tecnologias-chave do Ocidente. Devemos proteger o nosso conhecimento. As tentativas chinesas de infiltração para espionagem de dados internos acontecem por e-mail. Quando anexos são abertos, um programa espião é instalado no computador alemão e estabelece uma conexão com a China, para transmitir os dados recolhidos. O mais recente relatório de inteligência admite indiretamente o sucesso dos atacantes. Os ganhos para o lado chinês parecem predominar.

A França, por ser uma das maiores economias da Europa e do mundo, também está adotando medidas para se proteger contra ataques virtuais. Embora o país tenha sido pouco explorado por ataques cibernéticos, pelo menos até onde se sabe, o governo francês tem participado das ações que os EUA, Alemanha e Reino Unido têm adotado.

Em julho de 2009, foi criada a *L'Agence nationale de la sécurité des systèmes d'information (ANSSI)*, pois a França acredita que o risco de um ataque cibernético contra alguma infraestrutura crítica do país é uma das principais ameaças prováveis nos próximos anos.

Por isso, o Estado francês está desenvolvendo a sua capacidade para prevenir e responder aos ataques cibernéticos e a tornou prioridade de seu aparato de segurança nacional.

A *ANSSI* foi criada para implementar e desenvolver essas capacidades. Ela é a segurança nacional e dos sistemas de informação de defesa. As suas principais tarefas são as de garantir a segurança dos sistemas de informação do Estado, assegurar que os operadores nacionais coordenem as ações dos sistemas de defesa da informação, garantir as necessidades das mais altas autoridades do Estado e as necessidades interdepartamentais, e criar condições para um ambiente de confiança e segurança propícias ao desenvolvimento da sociedade da

informação na França.

Em março de 2011, o ministério francês da Economia e das Finanças foi alvo de um vasto ataque cibernético, que afetou mais de 150 computadores do ministério e visou documentos ligados à presidência francesa do G2039, poupando os dados pessoais dos contribuintes. O governo francês adotou medidas de proteção e restabeleceu a segurança. Foi o primeiro ataque desse tipo ao governo francês.

Patrick Pailloux, diretor-executivo da *ANSSI*, fez uma avaliação após os ataques de março de 2011, concluindo com as seguintes ações a serem realizadas: reforçar a capacidade operacional da intervenção do Estado através da criação de uma Unidade de Resposta Rápida; aumentar a segurança dos sistemas de informação do Estado com o estabelecimento de uma política comum de segurança [...] incentivar o cumprimento destas regras por todos os funcionários do Estado; os governos devem utilizar os produtos e serviços certificados pela *ANSSI*; [...] implantar uma intranet para cada departamento com sua própria rede - ou mesmo várias redes - com os seus próprios gateways para a Internet e vários links entre essas redes; promover a segurança cibernética do ensino superior e de pesquisa através da integração de segurança dos sistemas de informação no ensino superior, particularmente computador; melhorar a segurança das infraestruturas vitais através de parcerias com operadores de infraestrutura crítica;[...]; reforçar a *ANSSI* para chegar a 357 funcionários até 2013, contra 180 agora.

3.2 BRASIL

Para tornar efetiva a participação de todos os segmentos da sociedade nas decisões envolvendo a implantação, administração e uso da Internet, os Ministérios das Comunicações (MC) e da Ciência e Tecnologia (MCT) constituíram o Comitê Gestor da Internet no Brasil (CGI.br) em maio de 1995.

Desde então, o CGI.br é formado por representantes do Governo, 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.

Em 03 de setembro de 2003, o Decreto Presidencial nº 4.829 definiu as atribuições do CGI.br, destacando-se as seguintes:

- a proposição de normas e procedimentos relativos à regulamentação das atividades na internet;

- a recomendação de padrões e procedimentos técnicos operacionais para a internet

no Brasil;

- o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;

- a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;

- a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;

- a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas; e

- ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet.

O Núcleo de Informação e Coordenação do Ponto BR[11](NIC.br) é uma entidade civil, sem fins lucrativos, que implementa as decisões e projetos do CGI.br. São atividades permanentes do NIC.br: coordenar o registro de nomes de domínio, responder e tratar incidentes de segurança no Brasil, estudar e pesquisar tecnologias de redes e operações, produzir indicadores sobre as tecnologias da informação e da comunicação e abrigar o escritório do W3C43 no Brasil.

O Consórcio World Wide Web (W3C)[12] é um consórcio internacional no qual organizações filiadas, uma equipe em tempo integral e o público trabalham juntos para desenvolver padrões para a Web.

O Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR Gov), subordinado ao Departamento de Segurança de Informação e Comunicações (DSIC), do Gabinete de Segurança Institucional da Presidência da República, tem como finalidade precípua o atendimento aos incidentes em redes de computadores pertencentes à Administração Pública Federal.

O CTIR Gov auxilia Órgãos da Administração Pública Federal (APF) no desenvolvimento da cooperação entre os grupos de respostas de incidentes existentes no Brasil e no exterior, o fomento das iniciativas de gerenciamento de incidentes e na distribuição de informações, alertas e recomendações para os administradores de segurança em redes de computadores da APF.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) foi criado em 1997 para ser um ponto de contato nacional na notificação de

---

[11] Disponível em: http://www.nic.br/index.shtml. Acesso em 5 abr. 2014

[12] Disponível em:< http://www.w3c.br/Home/WebHome>. Acesso em: 05 abr. 2014.

incidentes de segurança na internet. Além disso, ele deve prover a coordenação e o apoio necessários no processo de resposta a incidentes, estabelecer um trabalho colaborativo com outras entidades, como os operadores da justiça, provedores de acesso e serviços e backbones45, auxiliar novos Grupos de Segurança e Resposta a Incidentes (CSIRTs) a estabelecerem suas atividades e aumentar a conscientização sobre a necessidade de segurança na internet. 40

Em 2009, o CGI.br produziu um documento importante, chamado de "decálogo" de princípios da governança e uso da Internet. Os princípios são os seguintes:

- liberdade, privacidade e direitos humanos;
- governança democrática e colaborativa;
- universalidade;
- diversidade;
- inovação;
- neutralidade da rede;
- inimputabilidade da rede;
- funcionalidade, segurança e estabilidade;
- padronização e interoperabilidade; e
- ambiente legal e regulatório.

Essa preocupação do governo brasileiro com o uso da internet está embasada no crescente número de usuários da rede.

Com o consequente aumento de usuários, o número de ataques de vírus aos computadores conectados à internet deu um salto, após 2011, chegando a números elevadíssimos em 2014, como mostrou o Programa Fantástico do dia 13 de abril de 2014[13].

Levantamento do CERT.br mostra que o número de notificações de problemas desse tipo passou de 61,1 mil nos seis primeiros meses de 2010 para 217,8 mil nos mesmo período desse ano, um crescimento de 256%. Segundo o CERT.br, esse crescimento se deve principalmente porque o usuário de internet tem acessado mais sites desconhecidos e que carregam algum tipo de vírus. Além disso, a vulnerabilidade também aumentou com o avanço da mobilidade da internet. No meio tradicional de acesso à internet (desktops), o usuário de internet costuma ser mais cuidadoso. Mas com o avanço dos *tablets* e *smartphones*, não há essa preocupação e acaba se tornando mais vulnerável a ataques. Outra fonte de disseminação de códigos maliciosos são as redes sociais como Facebook, Orkut e Twitter, já que grande parte

[13] Disponível em < http://globotv.globo.com/rede-globo/fantastico/t/edicoes/v/cerca-de-400-milhoes-de-computadores-no-mundo-estao-infectados-por-virus/3278883/> acesso em 14 abr. 2014

dos usuários da web participa de alguma delas. Quando se fala em corporações, em organizações privadas, fica a dúvida: como ter certeza que o monitoramento de mídias sociais e outros tipos de programas e softwares que permitem o acesso à internet não está sendo invadido por pessoas pagas pela concorrência?

O Operador Nacional do Sistema Elétrico (ONS) confirmou que, dois dias depois do apagão que atingiu dezoito (18) Estados e afetou 70 milhões de pessoas, em 11 de novembro de 2009, a rede corporativa havia sido invadida por hackers. O ONS controla o sistema interligado de produção e distribuição de energia elétrica.

Entre os dias 22 e 28 de junho de 2011, os sites da Presidência da República, do Portal Brasil, da Receita Federal e da Petrobras, dentre outros, sofreram ataques cibernéticos. Foram afetados 220 (duzentos e vinte), sendo 20 (vinte) deles ligados diretamente à esfera federal e 200 relacionados a órgãos públicos, como prefeituras, assembleias legislativas e universidades. O balanço foi divulgado pelo Serviço Federal de Processamento de Dados (SERPRO), órgão responsável por fornecer serviços em Tecnologia da Informação e Comunicações para o setor público. Segundo o órgão, nenhum dado sigiloso do governo foi acessado, mas esse tipo de ataque traz prejuízos à credibilidade do Estado. Uma das medidas tomadas pelo SERPRO para reforçar a segurança e facilitar a identificação dos cibercriminosos vai ser antecipar a migração dos sites do governo para o protocolo IPv6[14].

O governo brasileiro elaborou diretrizes relacionadas ao setor cibernético na Política de Defesa Nacional, que estabelece medidas para aperfeiçoar os dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, permitam seu pronto restabelecimento.

Em 2008, entrou em vigor a Estratégia Nacional de Defesa (END), que estabelece a independência nacional, alcançada pela capacitação tecnológica autônoma. A END fortalece três setores decisivos para a defesa nacional: cibernético, espacial e nuclear. Esse fortalecimento visa atender o conceito de flexibilidade, incluindo os requisitos estratégicos de monitoramento/controle e de mobilidade. Como diretrizes para o setor cibernético, a END determina o seguinte:

- não deve depender de tecnologia estrangeira e que as três Forças, em conjunto, possam atuar em rede, instruídas por monitoramento, inclusive pelo espaço;

---

[14] Disponível em:< http://www.serpro.gov.br/noticiasSERPRO/2011/junho/serpro-faz-balanco-de-medidas-de-seguranca-em-resposta-a-ataques-virtuais/?searchterm=ataques>. Acesso em 05 abr. 2014. O IPv6 tem como objetivo substituir o IPv4, que só suporta cerca de 4 bilhões (4x109) de endereços IP (internet protocol), contra cerca de 3,4x10 ^{38} endereços do novo protocolo.

- aumentar capacitações cibernéticas ao usos industriais, educativos e militares;

- prioridade nas tecnologias de comunicação entre todos os contingentes das Forças Armadas de modo a assegurar sua capacidade para atuar em rede;

- aperfeiçoar os dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, que permitam seu pronto restabelecimento;

- responsabilidade da Casa Civil, dos Ministérios da Defesa, das Comunicações e da Ciência e Tecnologia e do GSI-PR.

O setor cibernético brasileiro apresenta algumas vulnerabilidades, como:

- a dependência de sistemas e tecnologias externas;

- o baixo investimento em pesquisa e desenvolvimento em segurança da informação;

- uma infraestrutura de telecomunicações e energia obsoleta ou estrangeira;

- o baixo desenvolvimento e cultura em segurança da informação nas instituições e proteção do conhecimento;

- a baixa capacitação do poder judiciário na matéria de delito cibernético e prova eletrônica;

- a ausência de legislação que permita responder às solicitações internacionais de cooperação como às investigações nacionais e que permita a rastreabilidade;

- a falta de uma padronização para resposta à incidentes; e

- falta de um Plano de Segurança Cibernética Brasileira.

Isso originou a necessidade de criação do Centro de Defesa Cibernética (CDCiber), que tem como objetivo coordenar as ações de defesa cibernética e proteger as redes militares e governamentais, e também pode contribuir para proteger as infraestruturas de informação como um todo. Ele é equipado com simuladores para exercício de guerra cibernética, laboratório para análise de artefatos maliciosos na rede e centro de tratamento de incidentes.

O CDCiber busca atuar, principalmente, em quatro campos:

- prevenir o sistema contra ataques;

- criar redundância no sistema, a exemplo do que existe na rede elétrica para evitar quedas;

- estabelecer defesas para o sistema; e

- criar mecanismos para agilizar o restabelecimento operacional dos portais.

No final de 2013, o Ministro de Estado Chefe da Secretaria de Assuntos Estratégicos, por meio da Portaria nº 124, de 3 de dezembro de 2013, instituiu o Grupo de Trabalho Interministerial (GTI) do Setor Cibernético, com o objetivo de elaborar proposta de Plano Estratégico para promover e subsidiar o aperfeiçoamento das políticas públicas voltadas à segurança e defesa do espaço cibernético nacional[15]. Trata-se, portanto, da mais recente atividade governamental que visa ao estabelecimento de uma governança cibernética no país. Entretanto, ainda não existe no Brasil uma política nacional que regule essa questão da Segurança Cibernética. É ainda um campo muito novo a ser explorado.

[15] Diário Oficial da União Nr 235 de 04 Dez 2013 , páginas 2 e 3 da Seção 2

4 PLANEJAMENTO ESTRATÉGICO EM SEGURANÇA CIBERNÉTICA

4.1 CONSIDERAÇÕES TEÓRICAS SOBRE PLANEJAMENTO ESTRATÉGICO

Quanto ao Planejamento Estratégico (PE), é imperioso que se esclareçam alguns pontos sobre esse tema, para estabelecer critérios ao que se propõe nesse trabalho: linhas de ação a serem adotadas como colunas mestras em um PE, seja para empresas que fazem um único PE e utilizam Planos Táticos para detalhar ações, ou para aquelas que definem PE para algumas áreas da gestão.

Para tanto, serão recordados alguns conceitos de como se elabora e concebe um PE e, em uma segunda parte, serão apresentadas ideias que devam ser tratadas em planejamentos estratégicos para segurança cibernética no mundo corporativo.

4.2 A ELABORAÇÃO DE UM PLANEJAMENTO ESTRATÉGICO

4.2.1 **O processo do planejamento estratégico**

O conceito de planejamento estratégico tem-se tornado excepcionalmente importante nos círculos empresariais hoje, em grande parte devido à crescente complexidade dos ambientes tanto interno como externo, assim como à sofisticação cada vez maior da administração. O termo estratégia vem do grego *strategos*, que significa "general". Antigamente, significava a arte e a ciência de levar as forças militares à vitória. Hoje, empresas pequenas e grandes, e também organizações não lucrativas, usam estratégia para escolher as melhores opções para atingir seus objetivos.

4.2.2 **O que é planejamento estratégico**

O Planejamento estratégico inclui atividades que envolvem a definição da missão da organização, o estabelecimento de seus objetivos e o desenvolvimento de estratégias que possibilitem o sucesso das operações no seu ambiente. Planejamento estratégico se diferencia de outros tipos de planejamento organizacional segundo estes critérios:

- Envolve decisões tomadas pela alta administração;
- Envolve apropriação de muitos recursos, como dinheiro, mão de obra ou capacidade física;

- Tem impacto significativo a longo prazo;
- Focaliza a interação da organização com o ambiente externo.

4.2.3 **Quem faz o planejamento estratégico**

As decisões sobre o planejamento estratégico, por seu significado para a empresa, são de responsabilidade dos administradores de linha e não dos assessores especiais de planejamento. Os assessores de planejamento, se os houver, estejam centralizados ou descentralizados, desempenham um papel importante ajudando os administradores de linha, sobretudo ao fornecer análise ambiental.

Em grandes empresas diversificadas, o planejamento estratégico pode abranger vários níveis da estrutura, incluindo:

- O presidente e outros membros da alta administração;
- Os gerentes gerais das subsidiárias, como os gerentes de divisão e presidentes regionais;
- Gerentes funcionais das subsidiarias, que chefiam áreas funcionais como *marketing*, fabricação e finanças e devem apoiar sua estratégia;
- Gerentes dos principais departamentos operacionais, que têm responsabilidade de desempenhar seu papel no plano estratégico geral.

4.2.4 **Componentes do planejamento estratégico**

Para que uma empresa conceda um eficaz planejamento estratégico, desde o início deve-se ter uma compreensão clara da missão organizacional. Em segundo lugar, deve-se estabelecer os objetivos, para todos saberem o que a administração quer realizar. Em terceiro lugar, a administração identifica as alternativas estratégicas disponíveis para atingir esses objetivos. Esta etapa exige o exame dos pontos fracos e fortes da organização, prevendo o ambiente futuro. Finalmente, para completar o processo de planejamento, fazem-se as escolhas estratégicas. No caso da Segurança Cibernética, é imperioso que sejam estabelecidos objetivos estratégicos e divulgados, executados e fiscalizados constantemente, de modo a mudar a cultura organizacional da corporação.

Embora a ênfase seja no planejamento estratégico, os administradores devem se preocupar também com os processos de implementação e controle, quando os planos

estratégicos forem estabelecidos. Há necessidade de se estabelecer eficazes meios de controle para se checar, periodicamente, se as regras são ou não cumpridas por todos os colaboradores.

Nesse momento, nessa fase, os gestores devem atuar em coordenação com, principalmente, os especialistas em contrainteligência, pois são esses que deverão pontuar todas as vulnerabilidades dos meios de TI e dos recursos humanos que trabalham em TI na organização. Isso é vital. Se houver erros nessa fase do PE, haverá muitas dúvidas durante a implementação do mesmo.

Normalmente, dos pontos ou temas que devem ser abordados em um PE, de modo geral, os mais empregados são:

1 - Missão organizacional ou "o que queremos?"

2 - Papel dos clientes ao determinar sua missão

3 - Valores, crenças e missão

4 - Objetivos Organizacionais

5 - Como a Missão afeta os objetivos

6 - Áreas que precisam de objetivos

Nesse aspecto, cabem algumas considerações. Peter Drucker[16] identificou oito áreas em que uma empresa deveria estabelecer objetivos, e essas áreas são: ***Posição de Mercado, Produtividade, Recursos Físicos e Financeiro, Lucratividade, Inovação, Desempenho e desenvolvimento de executivos, Desempenho e atitudes dos trabalhadores e Responsabilidade pública e social.*** Observa-se que não há como se considerar Segurança Cibernética se fosse apenas pulverizar nas outras áreas. Disso, vem a proposta deste trabalho, que é justamente mostrar que o caminho para um atual planejamento estratégico de organizações é que não existe mais como excluir cibernética. Essa área da segurança orgânica da empresa deve, sem sombras de dúvida, ter seus objetivos organizacionais.

7 - Identificação de alternativas estratégicas

8 - Quatro áreas relevantes de análise

9 - Fatores que afetam o processo de planejamento

10 -Análise SWOT (**Forças – Fraquezas – Oportunidades e ameaças)**

11 - Planejamento tático

12 - Planejamento operacional

13 - Responsabilidade pela Elaboração do Plano

14 - Vantagens e Desvantagens do Planejamento

[16] Disponível em < http://www.excelencia.com.br/oportunidades/planejamento.html>, acesso em 15 abr. 2014

4.3 UM EXEMPLO SUCINTO DE PLANEJAMENTO ESTRATÉGICO EM SEGURANÇA CIBERNÉTICA

4.3.1 Um “case”: uma companhia global de TI

Neste trabalho, para fins de entendimento de um Planejamento Estratégico em Segurança Cibernética será usada como modelo a companhia **Huawei**[17] (nome oficial: **Huawei Technologies Co. Ltd.**). Salienta-se que todos os dados relacionados a essa companhia foram retirados da “internet”. A Huawei é uma empresa multinacional de equipamentos para redes e telecomunicações sediada na cidade de Shenzhen, localizada na província de Guangdong, na China. Ela é a maior fornecedora de equipamentos para redes e telecomunicações da China e a segunda maior do mundo. A Huawei foi fundada em 1988 por Ren Zhengfei e é uma empresa proprietária. Suas atividades principais são pesquisa e desenvolvimento, a produção e o marketing de equipamentos de telecomunicações, e o fornecimento de serviços personalizados de rede a operadoras de telecomunicações.

4.3.2 Principais tópicos do Planejamento Estratégico em Segurança Cibernética da Huawei (core[18])

O Planejamento Estratégico da empresa em questão é denominado de “*Perspectivas para a Segurança Cibernética – fazendo com que a Segurança Cibernética seja parte do DNA da Companhia*”. Isso revela o alto grau de importância que é atribuído a essa área da organização. Eles dividiram o Planejamento em 12 (doze) partes, as quais denominam os doze “core” ou corações da empresa. São as seguintes cada uma dessas partes:

1 - Estratégia , Governança e Controle.

2 - Construir os conceitos básicos de processos e padrões.

3 - Leis e Regulamentos.

4 – Pessoas.

5 - Pesquisa e Desenvolvimento.

6 - Verificação: não aceite nada, não acredite em ninguém , verifique tudo.

7 - Gestão de fornecedores de terceiros.

8 – Produção.

---

[17] Disponível em < http://pt.wikipedia.org/wiki/Huawei> acesso em 15 abr. 2014

[18] Coração em Latim

9 - Prestação de serviços de forma segura.

10 - Quando as coisas dão errado, o assunto é: defeito e vulnerabilidade.

11 – Rastreabilidade.

12 – Auditoria.

A seguir, então, serão apresentadas as principais ideias de cada um desses doze "cores".

4.3.2.1 Estratégia, Governança e Controle

Se a Segurança Cibernética não for importante para a diretoria e altos funcionários, não será importante para o funcionários. Garantir que a segurança cibernética esteja embutida no projeto organizacional, na governança estratégia de gerenciamento de risco e na estrutura de controle interno é o ponto de partida para a concepção, desenvolvimento e realização de um boa segurança cibernética.

4.3.2.2 Construir os conceitos básicos de processos e padrões

Para obter um produto de qualidade em todas as situações, são vitais processos de qualidade, normas e aproximação continuada de empregados e fornecedores. Na Segurança cibernética é a mesma situação: se os seus processos forem aleatórios ou o estabelecimento de padrões for aleatório, sua qualidade final será aleatória. As vezes se tem segurança, às vezes não tem segurança.

4.3.2.3 Leis e Regulamentos

O conjunto de leis de um país é algo complexo, variável e em constante mudança. As formas de aplicação de leis podem ser muito diferente ou pode haver diferentes interpretações da mesma lei ou código. Leis, códigos, normas e controles internacionais adicionam complexidade e risco a um fornecedor e um negócio. Os processos da organização devem atender e lidar com essa variabilidade e confusão e trabalhar para o mais alto nível de lei não o nível mais baixo

4.3.2.4 Pessoas

Muitas empresas dizem que suas pessoas são seu ativo mais importante, o que é verdade. No entanto, a partir de uma perspectiva de segurança também podem ser a sua maior fraqueza. A forma como as pessoas estão empregadas, como são treinadas e motivadas e como são gerenciadas, muitas vezes, determina a diferença entre o sucesso e o fracasso - não apenas para a segurança cibernética , mas também para a estratégia global da empresa.

4.3.2.5 Pesquisa e Desenvolvimento.

De um modo geral, as boas empresas não querem comprar produtos de alta tecnologia de empresas fracas. Entretanto, comprar alta tecnologia de marcas competitivas pode deixar sempre uma dependência entre organizações, devido ao "gap" tecnológico. É necessário, então, investir em pesquisa e desenvolvimento e tornar-se independente em cada aspecto de sua tecnologia própria.

4.3.2.6 Verificação: não aceite nada, não acredite em ninguém, verifique tudo.

Enquanto um processo de pesquisa e desenvolvimento robusto é fundamental para a qualidade e para que os produtos sejam seguros e protegidos, ao mesmo tempo pode estar sob pressão para lançar produtos sem a devida verificação e certificação da qualidade. Proteja seus produtos e serviços, por meio de verificações, checagens, certificações e use seus colaboradores e parceiros, antes de lançar ou vender seus produtos. Sua marca não pode correr riscos.

4.3.2.7 Gestão de fornecedores terceirizados.

Muitas grandes empresas de alta tecnologia usam empresas de terceiros para os componentes de hardware, componentes de software, entrega e instalação . Se essas empresas tiverem falhas em tecnologia, em segurança ou em processos, isso aumentará, significativamente, as fraquezas dos produtos e serviços da empresa que dependa desse fornecedor. Essa gestão deve ser muito bem conduzida, seja por reparações de contrato ou mesmo treinamento desses terceiros para que não venham a surgir falhas, pelas quais a empresa não é responsável.

4.3.2.8 Produção.

Se a empresa fabrica ou monta produtos, em especial da área de TI, ela deve ficar ligada nos insumos que recebe para a sua produção. É importante que tudo seja controlado pela empresa, para se ter a segurança que nada abaixo do padrão foi introduzido na produção ou montagem do seu produto final.

4.3.2.9 Prestação de serviços de forma segura.

Não há muito sentido em se concentrar no “design” de produtos, abrindo mão da segurnança. Implantar produtos com segurança é abrir mão da preocupação com o “design”. O que clientes buscam são equipmanentos que auxiliam seus negócios, com mautenção fácil, seguros, e que permitem atualizações e correções de falhas.

4.3.2.10 Quando as coisas dão errado, o assunto é: defeito e vulnerabilidade.

Nenhuma empresa será escusada se disser que garante 100% de segurança. Portanto, a capacidade da empresa para responder eficazmente aos problemas e aprender as lições com o que deu errado é fundamental para seu cliente e seu fornecedor. Saber o que fazer em uma "crise", garantindo que os altos executivos sejam informados para tomar decisões rápidas é o mais importante.

4.3.2.11 Rastreabilidade.

Não basta detectar o que deu errado. É importante que seja rastreado todo o caminho do processo que deu errado e com efetividade, para, assim, corrigir o ponto onde o erro aconteceu ou iniciou.

4.3.2.12 Auditoria.

Auditorias rigorosas desempenham um papel fundamental para garantir a diretoria e altos funcionários da empresa que tudo vai bem e assegurar a seus clientes que as políticas adequadas, os procedimentos e os padrões desejados estão sendo executados para entregar os melhores resultados ou produtos.

5 CONCLUSÃO

Chegando ao fim deste trabalho, com o qual espero contribuir, em muito, para expandir a mentalidade da Segurança Cibernética (Cyber Security) no mundo corporativo, em especial para empresas que trabalham na área da segurança, serão apontadas várias ideias conclusivas e que propõem medidas ou soluções para diversos problemas existentes no meio corporativo, bem como na administração pública.

Atualmente, a tecnologia da informação se transformou na base de todos os ramos do conhecimento, criando uma dependência cada vez maior. Tudo depende de computadores e da internet: a comunicação (celulares, email), entretenimento (TV a cabo digital, MP3), transporte (sistemas de carro motor, navegação de aeronaves, metrôs), shopping (lojas online, cartões de crédito), medicina (equipamentos, registros médicos) dentre outros. A vida diária das pessoas depende de computadores. Muitas informações pessoais são armazenadas em computadores. Defesa e segurança cibernética envolvem proteger essa informação por prevenção, detecção e resposta a ataques. Uma empresa que tem como objetivo ampliar seu mercado, ampliar sua produção, conquistar mais e mais clientes, enfim, que almeja o crescimento, não tem a opção de excluir Planejamento Estratégico de Segurança Cibernética de sua organização.

Os ataques cibernéticos se apresentam em uma escalada mundial crescente, silenciosa e se caracterizam como um dos grandes desafios do século XXI. Todas as pessoas, empresas, governos e entidades que utilizam o espaço cibernético estão expostos a riscos. Na realidade, nos dias atuais, é praticamente inexistente empresas de grande porte que não possuem os meios de TI permeando seus processos.

Uma medida fundamental para a garantia da Segurança Cibernética encontra-se na manutenção de um sistema de inteligência eficiente e eficaz, capaz de assessorar o processo decisório e garantir o sucesso da corporação. Verifica-se, nesse ponto, que segurança cibernética vai além das tecnologias de informação e comunicações, envolve outros sistemas da organização, como, por exemplo, pessoal e inteligência, logística, finanças. Mais uma vez reforço, não existe a opção de não se interessar pela “guerra cibernética”.

Com isso, a Inteligência Cibernética nada mais é do que um processo em que o espaço cibernético é o seu grande campo de trabalho, objetivando a obtenção, a análise e a capacidade de produção de conhecimentos baseados nas ameaças virtuais e com caráter prospectivo, suficientes para permitir formulações, decisões e ações de segurança e resposta imediatas, visando à preservação dos dados corporativos e pessoais e segurança virtual de uma

empresa, organização e/ou Estado.

Como dito por Shawn Henry, da divisão de informática do FBI, os ataques cibernéticos estão entre as três maiores ameaças na atualidade.

Agora, o grande desafio das empresas não é mais proteger os equipamentos onde os dados estão armazenados, mas sim blindar as informações sensíveis dos negócios. Essa mudança faz com que os gestores de tecnologia da informação (TI) e as organizações repensem as estratégias de segurança da informação. Ou se constrói uma mentalidade de Segurança Cibernética e a implante na organização ou a organização vai conhecer o insucesso.

Toda empresa, entidade, corporações industriais ou comerciais, enfim, em todos os ramos da atividade econômica há uma sensível independência a pontos críticos e infraestruturas críticas. Um sistema elétrico de uma indústria, por exemplo, que já tenha uma central digital, pode ser invadido. Algo que pode parece uma "brincadeira de criança" com uma simples teclada pode levar uma indústria ao caos, pois, mesmo que existam geradores, mesmo que existam opções físicas, se o comando ou central forem desativados, tudo para. Chegou a hora dos grandes empresários pensarem nisso e investir em Segurança Cibernética.

Toda organização deve ampliar a cultura de segurança cibernética no seu meio. Segurança Cibernética não é TI. É uma cultura organizacional que mexe com toda a estrutura administrativa da organização. Não adianta ter bons equipamentos, se as pessoas não viveram todo o tempo uma mentalidade de segurança.

As empresas e entidades em geral precisam estabelecer medidas que façam o monitoramento de mídias sociais e outros tipos de programas e softwares que permitem o acesso à internet, para assegurar-se que seus sistemas não estão sendo invadidos.

Hoje, ou a empresa faz um Planejamento Estratégico de Segurança Cibernética ou insira o tema como um dos pontos do plano. Segurança Cibernética tem que ser uma coluna mestra no Planejamento Estratégico Organizacional. Esse Plano tem como objetivo maior é mudar a cultura organizacional da corporação.

Como resultado do estudo do caso da Huawei, pode-se, também, delinear algumas recomendações para o mundo corporativo, que serão exemplificadas a seguir.

"Cibersegurança" é uma questão de grande interesse para clientes e governos, bem como para os parceiros, sejam compradores ou vendedores. A garantia de segurança cibernética é uma das principais estratégias da empresa .

Somente por meio de um trabalho conjunto a nível internacional, com fornecedores, clientes, políticos e legisladores é que se atinge uma diferença substancial na abordagem do desafio global de segurança cibernética .

Partilhar conhecimento e compreensão do que funciona e do que não funciona auxilia em muito na redução de riscos para pessoas que utilizam tecnologia para todos os fins. Isso é de suma importância no seio da organização, partindo dos gestores de TI da corporação.

Se houvesse uma resposta simples ou uma solução para o desafio de segurança cibernética já teria sido encontrada e adotada. No entanto, o simples fato de o mundo continuar a debater normas, leis e códigos no mostra que estamos no início.

Pessoas precisam compreender as políticas e procedimentos em relação ao espaço cibernético e como isso lhes afeta pessoal e socialmente.

Organizações precisam entender que seu maior valor (pessoas) também são suas maiores ameaças, pois se estiverem mal formadas, mal treinadas, mal orientadas, enfim, se estiverem atuando fora do escopo da organização, poderão ser as causas da queda dessa organização.

Deste modo, ou estabelecendo um Planejamento Estratégico específico para Segurança Cibernética (minha recomendação é essa linha de ação em virtude da magnitude desse assunto e pelo fato de estar presente em todas as áreas da organização), ou estabelecendo normas em seu Plano Estratégico e regulando tais normas em Planos Táticos ou Operacionais, uma coisa é certa: a organização que não se voltar para o tema Segurança Cibernética o mais rápido e com bons investimentos, assistirá sua derrocada ainda nos próximos anos. Isso se explica pelo fato de, quanto mais vulneráveis todos os meios de TI e com pessoas despreparadas para operá-los e sem mentalidade de segurança, ser muito fácil parar toda uma empresa com uma simples invasão.

Qualquer que seja o modo a ser executado, um bom início é a utilização dos 12 (doze) “cores” do estudo do caso apresentado neste trabalho. Como dizem os norte-americanos e ingleses: “Think about”!

REFERÊNCIAS

BRASIL. Ministério da Defesa. **Política de Defesa Nacional**. Brasília, DF, 2013.

_____. Presidência da República. Secretaria de Assuntos Estratégicos e Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília, DF, 2008.

_____. _____. Gabinete de Segurança Institucional. **Livro verde de segurança cibernética**. Brasília, DF, 2010.

CEBRÍAN, Juan Luis. La Red*:* como cambiarán nuestras vidas los nuevos medios de **comunicación**. Buenos Aires: Taurus, 1998. 197p.

CLARKE, Richard. **Ataques cibernéticos se tornaram armas de guerra**. **Ideias do Milênio.** [S.l.], 2011. Disponível em:< http://www.conjur.com.br/2011-mar-11/ideias-milenio-ataques-ciberneticos-tornaram-armas-guerra>. Acesso em 02 abr. 2014.

HAMMES, Thomas X.. **A guerra de quarta geração evolui, a quinta emerge**. Military Review, USA, p. 16 – 27, set./out. 2007. Disponível em:< http://www.ecsbdefesa.com.br/defesa/fts/MRSetOut07.pdf>. Acesso em: 20 mar. 2014.

HECK, Gustavo Alberto Trompowsky. **Conferência para o curso de altos estudos de política e estratégia**, 2011, Rio de Janeiro, RJ. Apresentação. Rio de Janeiro; ESG, 2011.

MANDARINO JUNIOR, Raphael. **Organizando o Caos**. Gestor da Internet no Brasil, 2001. Brasília, DF. **Resumos.** Brasília, DF, 2001. Disponível em: <http://www.cgi.br/publicacoes/indice/page:9>. Acesso em: 10 mar. 2014.

_____. **Segurança e defesa do espaço cibernético brasileiro**. Recife: Cubzac, 2010. 182p.

_____. **Um estudo sobre a segurança e a defesa do espaço cibernético.** 2009. 139 f. Trabalho de Conclusão de Curso (Especialidade em Ciência da Computação) – Universidade de Brasília, Brasília, DF, 2009. 49

MARQUES, Luiz Antônio. **Segurança Cibernética de Defesa.** Trabalho de Conclusão do Curso de Altos Estudos de Política e Estratégia da Escola Superior de Guerra. Rio de Janeiro,RJ, 2011.

MONTES, Antônio. **Monitoração de Atividades Maliciosas na Internet Brasileira**. Seminário de Defesa Cibernética. 2010. Brasília, DF. Resumos**...**, Brasília, DF: Brasília, 2010. 1 CD-ROM.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Declaração sobre segurança nas Américas: aprovada na terceira sessão plenária realizada em 28 de outubro de 2003**. Conferência Interamericana sobre os problemas da guerra e da paz, 2003, México. 2003.

RAYMOND, Eric Steven. **The New Hacker's Dictionary**. [S.I. : s.n.] Disponível em: <http://www.manybooks.net/titles/anonetext02jarg422.html>. Acesso em: 10 de jun. de 2011.

SHAWN, Henry. Federal Bureau Of Investigation. **Cyber Attacks Press Release**. USA, 2008. Disponível em:< http://www.fbi.gov/news/pressrel/press-releases/shawn-henry-named-assistant-director-of-fbi-cyber-division>. Acesso em: 20 mar. 2014.

SUFFOLK , John. **Cyber Security Perspectives - Making cyber security a part of a company's DNA -A set of integrated processes, policies and standards.** Huawei Technologies. China: out. 2013.

THE ECONOMIST. **A New Map of the World**. EUA, 2000. Disponível em:< http://www.highbeam.com/doc/1G1-62904332.html>. Acesso em: 20 jul. 2011.

TOFFLER, Alvin; TOFFLER, Heidi. **Guerra e Anti-Guerra**. Lisboa: Livros do Brasil, 1994.

VILELA, Geraldo Majela. **O uso do termo hacker nas notícias veiculadas pela internet brasileira.** 2006. 61 f. Monografia de Ciência da Computação – Curso de Pós Graduação em Administração de Redes Linux, Lavras, MG, 2006.

WENDT, Emerson. **Ciberguerra, inteligência cibernética e segurança virtual: alguns aspectos**. Revista Brasileira de Inteligência, Brasília, DF, n. 6, p. 15 – 25, abr. 2011.