ESCOLA DE GUERRA NAVAL

CF (VEN) GREGORIO JOSE MEJIA JUSTO

A GUERRA CIBERNÉTICA:

O quê fazer diante um ataque cibernético antes, durante e depois.

Rio de Janeiro

2016

CEMOS 2016

A GUERRA CIBERNÉTICA:

O quê fazer diante um ataque cibernético antes, durante e depois.

Monografia apresentado à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Estado-Maior para Oficiais Superiores.

Orientador: CF PAULO OZORIO.

Rio de Janeiro

Escola de Guerra Naval

2016

AGRADECIMENTOS

Agradeço a Deus pai Celestial em nome de seu filho Jesus, por permitir a oportunidade de representar a minha Pátria Venezuela no curso C-EMOS 2016.

Às minhas amadas esposa e filhos, pelo irrestrito e persistente incentivo durante o período de elaboração deste trabalho.

A meu orientador, pelos precisos ensinamentos e oportunos conselhos ao longo da jornada de dedicação à pesquisa.

À CEMOS 2016 pela colaboração na elaboração deste trabalho.

Ao Instrutor de Metodologia Científica, pela incansável dedicação aos Oficiais-Alunos, pela motivação acadêmica e pelo esmero na orientação metodológica.

Aos Docentes da Escola de Guerra Naval e da COPPEAD que, ao longo de todo o curso, sempre buscaram fazer o melhor na nobre e difícil tarefa transmitir conhecimentos.

Aos servidores militares e civis da Escola de Guerra Naval pelo grande empenho em proporcionar aos Oficiais-Alunos do C-EMOS 2016 o melhor apoio possível.

À República Bolivariana da Venezuela, Armada Bolivariana da Venezuela, Escola de Guerra Naval, bem como à Marinha do Brasil, por conceder-me esta oportunidade.

RESUMO

Em um mundo que precisa de segurança surge uma nova dimensão chamada ciberespaço. O propósito da pesquisa é analisar a perspectiva deste novo campo de batalha do século XXI, sem fronteiras, assimétrico, e com novos termos que surgem com o prefixo ciber-. Este trabalho aborda várias definições de ciberespaço e seus envolvimentos na sociedade atual. A relevância do tema reside na oportunidade de contribuir para a organização, na coleta e análise das iniciativas dos Estados Unidos, Espanhóis e Chineses em matéria de segurança relacionadas com as Tecnologias da Informação e as Comunicações, bem como o gerenciamento dessa segurança. O trabalho descreve as médias tomadas frente a este palco no âmbito estadunidense, europeu, chineses e da OTAN. São analisados na história os diferentes tipos de ataques, bem como a evolução no desenho das ciberarmas, desde o código daninho até chegar ao emprego de metodologias formais para desenvolver código. Mencionam-se especialmente as ameaças e vulnerabilidades nos elementos do ciberespaço compostos pela internet, o software e o hardware dando ênfase nas infraestruturas críticas como principal ameaça de segurança de estado. Após interrelacionar os conceitos, fatos históricos, ameaças e vulnerabilidade, surge então a necessidade das estratégias de ciberseguridad antes, durante e depois relacionadas ao risco no ciberespaço: umas se propuseram com caráter defensivo e outros com caráter ofensivo. Desta forma, sua importância é identificada face a essa nova modalidade de guerra.

Palavras chave: Ameaça. Vulnerabilidade. Ciberespaço. Ciberseguridad. Ciberataque.

LISTA DE ABREVIATURAS E SIGLAS

ABNT - Associação Brasileira de Normas Técnicas

AFD - *Análisis Forense Digital*

BGP - *Border Gateway Protocol*

CSNU - Conselho de Segurança das Nações Unidas

DNS - *Domain Name System*

DSN - *Departamento de Seguridad Nacional de España*

ENISA - *European Union Agency for Network and Information Security*

EUA - Estados Unidos da América

IEC - *Commission Electrotécnica International*

IEEE - *Instituto Español de Estudios Estratégicos*

ISO- *International Organisation of Normalisation*

MB - Marinha do Brasil

MD - Ministério da Defesa

OTAN - Organização do Tratado do Atlântico Norte

ONU - Organização das Nações Unidas

OSI - *Open System Interconnection*

PDN - Política de Defesa Nacional

PMD - Política Militar de Defesa

SCADA - *Supervisory Control And Data Acquisition*

TCP/IP - *Transmission Control Protoco /Internet Protocol*

TIC - *Tecnologías de la información y la comunicación*

LISTA DE ILUSTAÇOES

SUMÁRIO

1 INTRODUÇÃO

Após a Segunda Guerra Mundial (1939-1945), com o surgimento da Guerra Fria (1947-1989), os conflitos entre as nações sofreram mudanças profundas não existindo mais a destruição em massa, nem o massacre da população uma vez que novas formas de conduzir a guerra foram introduzidas.

Um novo cenário e uma percepção de novas ameaças e vulnerabilidades foram adicionadas comprometendo a paz e a segurança internacional. Surge então em 1969, a primeira rede de computadores da época, denominada de ARPANET[1]. Trata-se de uma iniciativa militar de comunicação, a qual evolui posteriormente para a criação de uma grande rede de redes conhecida como Internet[2]. A partir daquele momento, a Internet mudou a forma como nos comunicamos por meio de um sistema de rede horizontal, incorporando novos elementos em plataformas de Tecnologias da Informação e Comunicação (TICs[3]) integrados no mundo global. A corrida tecnológica do Século XX omite certas normas de segurança nos sistemas, nos *hardware, software*, redes e internet, o que provoca muitas vulnerabilidades a serem exploradas por meio de ataques cibernéticos.

---

[1] ARPANET. A Agencia de Projetos de Pesquisas Avançada de Defensa é a entidade do Departamento de Defensa dos Estados Unidos responsável pelo financiamento de pesquisas inovadoras para atender as necessidades das forças armas dos Estados Unidos. A pesquisa iniciada que originou a Internet foi financiada pela DARPA. Em 1969, a ARPANET se tornou a primeira rede de computação de pacotes conectando quatro universidades (CLARKE e KNAKE, 2015, p. 225).

[2] A Internet. A rede mundial das redes interligadas destinadas a acesso geral para transmissão de e-mail, compartilhamento de informações em páginas web e assim por diante. As redes podem usar o mesmo software e protocolos de transmissão e não fazerem parte da Internet, se elas forem projetadas para serem separadas do sistema da rede mundial. Tais redes separadas são chamadas de "Intranet". Muitas vezes existem conexões controladas entre a Intranet e a Internet. Outras vezes, existem conexões não intencionais (CLARKE e KNAKE, 2015, p. 226).

[3] Tecnologias de informação e comunicação (TIC): podem ser definidas como o conjunto de recursos tecnológicos, utilizados de forma integrada, com um objetivo comum. As TICs são utilizadas das mais diversas formas, na indústria (no processo de automação), no comércio (no gerenciamento, nas diversas formas de publicidade), no setor de investimentos (informação simultânea, comunicação imediata) e na educação (no processo de ensino aprendizagem, na Educação à Distância) (PINHEIRO, 2013, p. 49). (Fonte: <http://www.esg.br/images/Monografias/2013/PINHEIRO.pdf>. Acesso 07 agostos 2016).

Segundo Clarke[4] e Knake[5], a explosão da internet ocorrida nos últimos anos trouxe uma nova modalidade de ataques à rede de alguns órgãos críticos do Estado. Esses ataques vêm crescendo ao longo dos anos, principalmente pelo sucesso da capacidade em ocultar o atacante, de seu baixo custo e por ser realizado por qualquer tipo ou grupo de pessoas, sem discriminação de raça ou sexo (CLARKE e KNAKE, 2015).

Portanto, uma nova modalidade de guerra foi iniciada após o fenômeno da Internet, a guerra cibernética[6]. Em uma plataforma de Tecnologia de Comunicação e Informação (TIC), como em qualquer outro cenário onde existem elementos tecnológicos (*hardware, software,* redes e Internet) é possível que essa nova modalidade de guerra cibernética exista.

O propósito deste trabalho é identificar as medidas de segurança cibernética[7] que possam ser aplicadas na guerra cibernética, e que possam ser adaptadas antes, durante e depois do ataque cibernético.

Para atingir o proposito deste estudo, o trabalho será estruturado de maneira a responder as seguintes questões: Que devemos conhecer da guerra cibernética para classificá-la como uma ameaça de Segurança do Estado? Quais foram as ações realizadas na história da guerra cibernética? Quais são as medidas que devemos conhecer antes, durante e depois de um ataque cibernético?

O tema é de muita relevância na área da Segurança do Estado, corroborando com o desenvolvimento dos conceitos de segurança cibernética, além de proporcionar uma melhor

---

[4] *Richard A. Clarke*, serviu na Casa Blanca durante os governos Ronald Reagan, George H.W. Bush, George W. Bush e Bill Clinton, que o indicaram como Coordenador Nacional para Segurança, Proteção da Infraestrutura e contraterrorismo. LECIONA NA Harvard Kennedy School, é consultor da ABC News e presidente da consultoria *Good Harbor*. Ele é também autor do best seller *Your Government Failed You: Breaking the Cycle of National Security Disasters* (CLARKE e KNAKE, 2015).

[5] *Robert K. Knake*, trabalha com assuntos internacionais no Conselho de Relações Exteriores. Possui mestrado em segurança internacional pela Harvard Kennedy School e escreve sobre questões de segurança. Ele mora com sua esposa e filha em Washington, D.C. (CLARKE e KNAKE, 2015).

[6] A guerra cibernética ou ciberguerra. Definido em o capitulo dois fundamentos teóricos.

[7] A cibersegurança ou segurança de tecnologias da informação. Definido em o capitulo dois, fundamentos teóricos.

compreensão desta nova modalidade de guerra. Pretender-se assim contribuir no aperfeiçoamento da defesa cibernética.

Neste estudo conhecerá os conceitos de especialistas em segurança da informação com experiência na administração de plataformas de tecnologias da informação, entre eles se encontram: Richard Clarke, Robert Knake (EUA) e Henning Wegener[8] (Alemanha-Espanha). O trabalho estará delimitado a estudo dela prevenção, detecção, defesa e análise das ameaças e vulnerabilidades da guerra cibernética.

Para tornar possível a aplicação de estudo, a metodologia empregada é descritiva e analítica, fundamentada em pesquisa bibliográfica e documental baseadas em publicações doutrinarias, jornais, revistas, legislações, livros, filmes e publicações eletrônicas de especialistas e críticos no âmbito da segurança da informação e cibedefesa, por meio do uso de técnicas diretas.

O trabalho foi organizado em cinco capítulos delineados conforme a seguir. Após esta introdução, no segundo capítulo apresentar-se-á o referencial teórico do objeto do estudo, conceitos, definições, as ameaças e vulnerabilidades destacando o espaço onde a guerra cibernética se desenvolve, o capítulo três, detalhar-se-ão feitos históricos que tornam possível a guerra cibernética, o capítulo quatro fará uma análise dos que fazer frente a um ataque cibernético antes, durante e depois. Por último, no capítulo cinco, apresentará as conclusões e recomendações do trabalho, deixando aberta a possibilidade de estudos futuros.

Assim, inicia-se o estudo com a fundamentação teórica do espaço cibernético onde desenvolve-se este novo cenário da guerra.

---

[8] *Henning Wegener*. Diretor Geral da Associação Espanhola de Acionistas Minoritários das Companhias Abertas (AEMEC) e Membro do Conselho de Administração da *Euroshareholders*. Também é Presidente Honorário do *Conselho Consultivo da Cremades* e Calvo Sotelo Advogados, Membro da Federação Internacional de Cientistas e Presidente do Observatório Permanente para a Segurança da Informação da Federação. Em 1962 ingressou no serviço diplomático alemão ocupando, entre outros cargos, o de Secretário-Geral Adjunto para os Assuntos Políticos da OTAN (1986-1991) e de embaixador da Alemanha para o Reino da Espanha e do Principado de Andorra (1995-1999). Estudou Direito na Alemanha, Estados Unidos e França. (Fonte: <http://www.revista-uno.com.br/staff/henning-wegener/>. Acesso em: 07 agosto 2016).

2 FUNDAMENTOS TEÓRICOS

Este capítulo apresenta os conceitos e as definições básicas do espaço cibernético[9], onde se desenvolve a Guerra Cibernética. Sem o uso de uma linguagem técnica, serão apresentados as principais ações e definições para uma fácil compreensão e análise.

2.1 Conceitos da guerra cibernética

O home sempre há querido ter o controle do espaço onde se desenvolve, estabelece-se o espaço terrestre e procura o controle, estabelece-se o espaço naval e procura o controle, estabelece-se o espaço aéreo e procura o controle, estabelece-se o espaço espacial e procura o controle, agora estabelece-se o espaço cibernético e procura o controle, com os mesmos conceitos da guerra conforme seu emprego mas com o prefixo "*ciber*", *ciberdefensa*[10] (defensa), *ciberataque* (ofensiva), e *ciberexploração*[11] (inteligência), a Guerra Cibernética é um instrumento do poder que não substitui a força física, mas a complementa, podendo ser trabalhada isoladamente ou combinada com as demais dimensões de um conflito (mar, ar, terra e espaço).

Um conceito importante e o ciberespaço, o Instituto Espanhol de Estudos Estratégicos (IEEE), define como:

> O mundo digital gerado por computadores e redes de computadores, no qual pessoas e computadores coexistem e que inclui todos os aspectos da atividade «on-line» (tradução nossa)[12].

---

[9] Espaço Cibernético. Definido em o capitulo dois, fundamentos teóricos.

[10] Defesa Cibernética – conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com a finalidade de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de Inteligência e de causar prejuízos aos sistemas de informação do oponente (MD30-M-01, BRASIL, 2011, p. 55).

[11] Exploração Cibernética – consiste em ações de busca, nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados, de forma não autorizada, para a produção de conhecimento e/ou identificar as vulnerabilidades desses sistemas (MD30-M-01, BRASIL, 2011, p. 56).

[12] *Ciberespacio. El mundo digital generado por ordenadores y redes de ordenadores, en el cual personas y ordenadores coexisten y el cual incluye todos los aspectos de la actividad «online»* (*IEEE*, 2010). (Fonte: <https://www.cni.es/comun/recursos/descargas/Cuaderno_IEEE_149_Ciberseguridad.pdf>. Acesso 26 julho 2016.

Com esta contextualização do ciberespaço podemos disser que é um espaço existente no mundo de comunicação, dando ênfase ao ato da imaginação, necessária para a criação de uma imagem anônima, que terá comunhão com os demais. Agora uma modalidade de guerra onde a conflitualidade não ocorre com armas físicas, mas através da confrontação com meios eletrônicos e informáticos no chamado ciberespaço, e conhecida como ciberguerra ou guerra cibernética. O espaço cibernético é o médio ambiente onde se desenvolve este novo cenário da guerra, em muitos livros, revistas, e filmes vamos observar uma estreita relação entre ataques na rede e guerra cibernética, é o espaço virtual para a comunicação disposto pelo meio de tecnologia.

Os autores Richard Clarke e Robert Knake (2015) conceituam a Guerra Cibernética como aquelas ações realizadas por Estados para penetrar em computadores e redes de outro Estado com a finalidade de causar danos ou neutralizá-la. Afirmam ainda que é real, rápida, global, extrapola o campo de batalha e já começou, e seu uso mais comum e livre, o termo é usado para designar ataques, represálias ou intrusão ilícita num computador ou numa rede. Outro conceito estabelecido em o glossário da marinha do Brasil (MD35-G-01), nos desse:

> Guerra cibernética: Conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil, (BRASIL, 2007).

O conceito envolve uma nova modalidade de fazer a guerra, onde se mantem os conceitos, mudam os atores, com novas ferramentas, técnicas e métodos característicos do ciberespaço, onde podem interatuam todos os espaços do poder conhecidos. Estas ações poderão ter origem diretamente em estados, ou, então, ser protagonizadas por atores não estaduais atuando de forma autónoma.

O diretor do Departamento de Segurança da Informação[13] e das Comunicações (DSIC, Brasil), Raphael Mandarino, afirma que devemos ter uma cultura sob o tema, ele disse:

> O primeiro, o grande desafio, é cultural. Vamos ter que estabelecer, de alguma forma, um projeto de cultura de segurança cibernética. Estamos fazendo isso nos cursos, mas para dentro do Estado, e temos que fazer isso para fora também. Pode ser com um hotsite que ensine como fazer, e que todos os provedores divulguem, com seminários, ou que a gente comece a ensinar na escola (MANDARINO, 2009)

Esta reflexão nos abre os olhos ante este nova ameaça, que atenta contra a segurança do estado, obrigando-nos a estabelecer a cultura do cibersegurança desde nossas primeiras aulas, além disso a segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.

2.2 Elementos do campo de batalha

Todo cenário de Guerra tem um espaço, dependendo onde se realize. Por exemplo, uma guerra terrestre se desenvolve em um espaço terrestre e assim acontece com a Guerra Naval e Aérea, por conseguinte. A Guerra Cibernética se desenvolve no Espaço Cibernético, com os elementos que a integram: *hardware, software* e redes, interconectados à internet por qualquer sistema de telecomunicação. Estes elementos se convertem em uma realidade virtual[14] a qual é operada por um homem especializado, conhecido como *hacker*[15] ou Guerreiro Cibernético[16].

---

[13] Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. (ABNT, 2005, p. 01)

[14] A realidade virtual é uma interface avançada para aplicações computacionais, que permite ao usuário a movimentação (navegação) e interação em tempo real, em um ambiente tridimensional podendo fazer uso de dispositivos multissensoriais, para atuação ou feedback (ROMERO, KIRNER e SISCOUTTO, 2006, p. 07). (Fonte:<http://www.ckirner.com/download/capitulos/Fundamentos_e_Tecnologia_de_Realidade_Virtual_e_Aumentada-v22-11-06.pdf>. Acesso em: 08 agostos 2016).

[15] Hacker é alguém com habilidades de ganhar acesso a um computador ou rede sem autorização, assim como o verbo "hackear" representa invadir um sistema (CLARKE e KNAKE, 2015, p. 226)

[16] Guerreiro Cibernético é o usuário com alto conhecimento em programação que se dedicam a descobrir novas vulnerabilidades em sistemas, e pertence a uma força de defensa cibernética (CLARKE e KNAKE, 2015, p. 32).

O espaço cibernético, ou ciberespaço está presente em todas as redes de computadores do mundo e em tudo aquilo onde se encontram conectadas ou por elas controladas. O ciberespaço inclui a Internet, além de várias outras redes de computadores que não deveriam ser acessíveis a ela. Algumas dessas redes privadas são exatamente como a Internet, mas estão, pelo menos teoricamente, isoladas. Outras partes do ciberespaço é composta por redes transacionais que atuam por meio do envio de dados sobre fluxos de dinheiro, operações de mercado de ações e transações de cartão de crédito. Algumas redes constituem sistemas de controle que permitem que somente máquinas se comuniquem com outras máquinas por exemplo, painéis de controle com bombas hidráulicas, elevadores e geradores, tornando essas redes um local onde os militares podem lutar. Em termos mais amplos, guerreiros cibernéticos podem invadir, controlar ou destruir essas redes (CLARKE e KNAKE, 2015).

Em outras palavras, quando fazemos *clik*, al enviar uma mensagem de seu computador conectado à internet, a traves de *gmail, hotmail* o qualquer outro correio, ou quando você navega em nas redes sociais *facebook*, etc, começa a interação do ciberespaço (homem, hardware, software, redes e internet)

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

2.3 Ameaças cibernéticas

Milhões de usuários acedem de maneira legítima, a dados de qualquer lugar do mundo por médio de redes internas ou através dos diversos serviços oferecem Internet, enquanto pelo outro extremo, também cresce a frequência dos acessos não autorizados por parte de

indivíduos que se servem dos canais mencionados para infligir danos aos sistemas de informação e cuja importância e significado não parece perceber a opinião pública, por mais que as espetaculares façanhas dos hackers apareçam ultimamente nos titulares de imprensa.

As ameaças que para a comunidade internacional supõe a vulnerabilidade informática das sociedades civis e suas infraestruturas de segurança têm originado muitas iniciativas internacionais empreendidas para as enfrentar. A Associação Brasileira de Normas Técnicas (ABNT), fundamentada ela normas ISO-IEC-17799, Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação, e um exemplo de essas iniciativas do segurança da informação, define ameaça como:

> Ameaça causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (ABNT, 2005, p. 03)

Em esta definição do Ameaça descreve-se qualquer acione o acontecimento não desejado e inesperado com a capacidade de ocasionar consequências adversas, o seja, as que faz os não autorizados (hackers). Ágora uma ameaça é possível quando o sistema tem uma debilidade à falha.

A perda da integridade está relacionada diretamente com a modificação indesejada dos dados dos sistemas de informação, resultando em imprecisão, fraude ou decisões equivocadas. A perda de disponibilidade é tornar indisponível para os usuários autorizados a informação necessária naquele momento. A perda da confidencialidade ocorre quando há acesso não autorizado nos sistemas de informação, podendo chegar a ameaçar até a segurança nacional, conhecida pelo comprometimento (CLARKE e KNAKE, 2015).

Um intruso informático pode aceder e empregar informação privada referida a determinado grupo ao que não pertence, deste modo destrói a confidencialidade e, ao mesmo tempo, a confiança na segurança que oferecem as novas tecnologias, requisito básico para o correto funcionamento da sociedade da informação. Para além, o intruso pode manipular arquivos introduzindo dados próprios ou alterando os existentes. Pode, também, reprogramar

sistemas de informação que controlam importantes processos mediante a introdução de comandos falsos e destruir a integridade do sistema, ou bem comprometer a disponibilidade de determinados dados os suprimindo ou modificando os serviços que proporcionam, de maneira que sistemas inteiros deixem de funcionar.

Na seguinte figura mostram-se as ameaças relacionadas à origem humana, e origem natural (os terremotos ou as inundações). As humanas podem ser sem intenção, devido a negligencia, imperícia ou mau uso. As mal-intencionadas classificam-se como internas ou externas dependendo de sua origem: desde dentro da própria organização ou desde um ponto remoto. No caso da guerra cibernética podemo-la classificar como uma ameaça de origem humana, mal-intencionada, que pode ser interna dentro da organização ou rede, e também pode ser externa desde fora da organização ou rede.

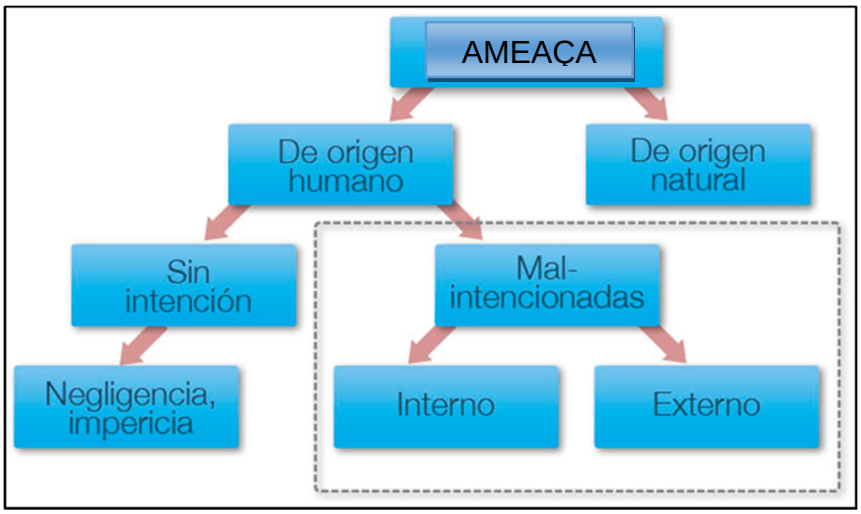

Figura 1 - Tipos de ameaças além sua natureza.
Fuente: Magazcitum. Vulnerabilidades, amenazas y riesgo en “texto claro” by Patricia Prandini (CISA y CRISC) y Marcela Pallero, 25/05/2013[17].

Todas estas ameaças de origem humana mal-intencionadas constituem as técnicas de ataque, as quais aproveitam as vulnerabilidades dos sistemas da informação e comunicação, o

[17] Disponível em: http://www.magazcitum.com.mx/?p=2193#.V5Qwe_krLIV. Acesso em 24 julho 2015.

fácil acesso a estas técnicas, junto ao enorme crescimento do número de computadores conectados às redes, tem levado a que nos países onde já se estão pesquisando e registrando estes atos, a cifra de ataques duplique-se a cada ano e tenha atingido magnitudes milionárias.

Os ataques mal-intencionados perpetrados através de meios eletrônicos contra os bancos de dados, converteu-se em uma ameaça para a Segurança de Estado e dependendo de seus fins, fala-se de delinquência ou terrorismo cibernético[18].

Pois bem, determinados os objetos de tutela, procede identificar as ameaças aos mesmos, que em todo caso são muito heterogéneas e apresentam uma natureza de alta inovação. Parece existir certo acordo em classificá-las, o Instituto Espanhol de Estudos estratégico (IEEE) no manual de estratégia N 149, 2010, em consideração a sua autoria e impacto, classifica as ameaças nas quatro seguintes categorias:

> A) Ataques perpetrados ou patrocinados por Estados. Seria a translação ao âmbito virtual dos conflitos reais entre países. Os ataques a infraestruturas críticas[19] ou classificadas ou a denominada ciberguerra, constituem bons exemplos.
> B) Ataques cometidos por grupos terroristas ou por qualquer outra manifestação de extremismos políticos, ideológicos ou religiosos. Planejamento de ações e sua execução, sabotagens, apologia, captação ou recrutamento seriam as principais condutas a considerar.
> C) Os ataques da delinquência organizada o Cibercrime[20]. O anonimato e as fronteiras nacionais oferecem uma alta rentabilidade para seu uso em fraudes econômicas a grande escala ou explorações de redes de pornografia infantil.
> D) Por último, identificam-se os ataques de perfil baixo. Sua natureza é muito heterogénea, incluindo desde intromissões na intimidem até pequenas fraudes. (Tradução nossa, Espanha, 2010)[21]

---

[18] *Ciberterrorismo* é a expressão usada para descrever os ataques terroristas executados pela Internet, com o objetivo de causar os danos a sistemas ou equipamentos. Qualquer crime informático que ataque redes de computador pode ser classificado como ciberterrorismo, em que geralmente as ferramentas utilizadas são os vírus de computador. A facilidade com que os ataques são realizados e os danos que podem causar preocupam países pelo mundo todo (tradução nossa). (Fonte: <http://www.genbeta.com/activismo-online/amenaza-cyber-documental-sobre-ciberguerra-y-ciberterrorismo>. Acesso em: 26 julho 2016).

[19] Infraestruturas Críticas: Instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade (Brasil, 2010).

[20] O *Cibercrime* é qualquer crime cometido usando um computador, rede ou dispositivo de hardware. A máquina ou dispositivo pode ser o agente, o facilitador ou o alvo do crime. O golpe pode acontecer estritamente no computador ou incluir outros locais (Fonte: <https://www.symantec.com/pt/br/theme.jsp?themeid=glossario-de-seguranca>. Acesso em, 24 julho 2016).

[21] *Instituto Espanhol de Estúdios Estratégicos (IEEE).* Espanha, 2010. (Fonte: <https://www.cni.es/comun/recursos/descargas/Cuaderno_IEEE_149_Ciberseguridad.pdf>. Acesso 26 julho 2016).

Os atores podem ser estatais ou não é as ações cibernéticas realizadas encontram no espaço cibernético uma nova dimensão de um conflito criada pelo homem e que permeia as tradicionais dimensões marítima, aérea, terrestre e espacial. Os efeitos desejados das ameaças podem abranger a perda da disponibilidade, integridade, confidencialidade e até a destruição física. Estas ações poderão ter origem diretamente em estados, ou, então, ser protagonizadas por atores não estaduais atuando de forma autónoma. A possibilidade de ciberguerra resulta da existência de redes de computadores essenciais para o funcionamento de um país. Potenciais alvos são as infraestruturas críticas, nomeadamente as redes de energia elétrica, de gás e de água, os serviços de transportes, os serviços de saúde e financeiros. Assim, inicia-se o estudo que faz possível a guerra cibernética.

2.4 Vulnerabilidades do espaço cibernético

Existem três pontos envolvidos no ciberespaço que tornam a guerra cibernética possível: (1) falha no design da Internet; (2) falha do *hardware* e *software*; e (3) a introdução cada vez maior dos *sistemas críticos on-line* (CLARKE e KNAKE, 2015).

A internet não se creio para o que é hoje, ou seja, nunca se penso que seria usada para realizar transações bancárias, fazer negócios, comunicação em massa, e muito menos administrar remotamente sistemas críticos, é por isso que tem muitas falhas de segurança em seu desenho. Os *softwares* são feitos por pessoas as quais também cometem erros em no desenho, tais falhas de desenho ou vulnerabilidades serão abordadas a seguir.

2.4.1 As vulnerabilidades da Internet

A Internet é integrada por milhares de milhões de circuitos virtuais[22] que se comunicam entre si e criam o que conhecemos como circuitos virtuais (VC), ela não foi desenvolvida para fazer negócios, transações bancárias e ainda menos controlar de longe sistemas de controle crítico *on-line*. A Internet ao www[23] não se encontra voltada para a conexão, ou seja, o sistema de direcionamento que determina para onde ir a partir de um endereço específico pode se perder no caminho ou ser desviado para outro endereço. Isto é, se a mensagem não chega é replicado por uma fonte infinitamente.

A Internet é uma rede aberta para as redes de computadores. A partir de uma rede da Internet, é possível se comunicar com qualquer computador conectado a qualquer uma das redes da Internet (CLARKE e KNAKE, 2015).

A seguir, observa-se um gráfico de um pacote de dados descrevendo sus partes, no modelo OSI[24] TCP/IP da Internet, em ele podemos olhar que tem uma cabeceira com três nível 2, 3, 4, cada nível tem uma função especifica da transportação dele mensagem, ou seja é o direcionamento da mensagem, logo vem o corpo com a informação e finaliza o nível 2 fechando o pacote. A cabeceira representa a vulnerabilidade da transportação do protocolo TCP/IP da Internet a qual é alterada por os hackers ou guerreiro cibernético, redirecionando o pacote para roubá-lo ou que se perca no caminho e não chegue a seu destino original.

---

[22] *Circuito virtual (VC).* Circuito lógico que se cria para garantir a comunicação confiável entre dois dispositivos de rede (tradução nossa). (Fonte: <http://uammante.uat.edu.mx/cisco/Curricula/CCNASem3/CHAPID=null/RLOID=null/RIOID=1083952940359/knet/1080604003687/entryframeset.html>. Acesso em: 27 julho 2016).

[23] *World Wide Site*. Grande rede de servidores de *Interne*t a qual fornece serviços de hipertexto e outros a terminais que executam aplicativos de clientes como, por exemplo, um navegador de Site. (Fonte: <http://uammante.uat.edu.mx/cisco/Curricula/CCNASem3/CHAPID=null/RLOID=null/RIOID=1083952940359/knet/1080604003687/entryframeset.html>. Acesso em: 27 julho 2016).

[24] O modelo de referência *OSI* não é específico de *TCP/IP*. Este modelo foi desenvolvido por ISO no final dos anos 70 como marco para descrever todas as funções necessárias em uma rede interconectada aberta. É um modelo de referência muito conhecido e aceitado no campo das comunicações de dados e utiliza-se aqui só para propósitos de comparação (tradução nossa). (Fonte: <https://msdn.microsoft.com/es-es/library/cc786900(v=ws.10).aspx>. Acesso em: 26 julho 2016).

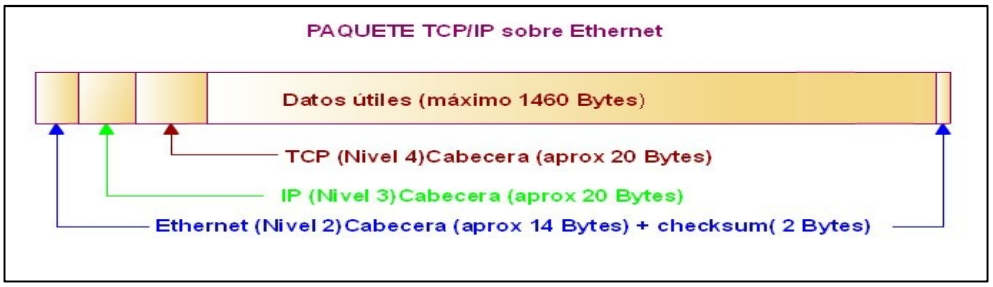

FIGURA 2 - Pacote do dado modelo *TCP/IP*.
Fonte: A Unidade Didática: "Redes de computadores". Portal ESO, Espanha, 2016[25].

Entre as vulnerabilidades de seu desenho se destaca a sua linguagem de comunicação, já que os computadores possuem seu próprio idioma para se comunicar conosco. Quando escrevemos o nome de uma página web no computador, essa palavra é traduzida em 0 e 1, o *Código Binário*[26], para que os computadores possam compreender e buscá-lo na web. Essa conversão é conhecida como Sistema de Nomes de Domínio (*DNS*) [27]. O navegador utiliza o *DNS* para direcionar os pacotes de dados[28]. Esses *DNS* são alvos para os Guerreiros Cibernéticos, que modificam essa informação direcionando os pacotes de informação para um endereço falso. Essa falha não foi pensada por aqueles que desenharam a Internet, o que implica na vulnerabilidade do endereçamento.

Na seguinte figura explica-se o processo de comunicação do Sistema de Domínio de Nome *DNS* entre os homens e os computadores, em ele vemos que são transcritos nomes

---

[25] Fonte:<http://www.portaleso.com/usuarios/Toni/web_redes/unidad_redes_informaticas_indice.html#indice>. Acesso em: 26 junho 2016.

[26] O *código binário* é um sistema de numeração que possui apenas dois algarismos: o "1" e o "0". É como o sistema de numeração arábico (usado por nós), que quando chega ao 9, retorna ao 0, mas como o código binário só possui dois algarismos, quando se aumenta 1 ao valor 1, volta-se ao 0. (Fonte: < http://www2.uol.com.br/jornalasemana/edicao65/info.htm>. Acessado em: 27 junho 2016).

[27] *Domain Name System* ou *DNS* (*Sistemas de Nomes de Domínios*), é um sistema de nomenclatura hierárquica descentralizada para dispositivos conectados em redes *IP*, como Internet ou rede privada. Esse sistema associa informação variada com nomes de domínios designados para cada um dos participantes. Sua maior função é "traduzir" nomes inteligíveis para as pessoas em identificadores binários associados com os equipamentos conectados à rede com o objetivo de poder localizar e direcionar esses equipamentos mundialmente (Clarke e Knake, 2015).

[28] Pacote de dados: referimo-nos aos dados enviados por uma conexão entre dispositivos eletrônicos. A cada pacote consta das instruções necessárias para unir com o resto uma vez atinge seu destino, tendo uma cabeceira, uma parte central com os dados, e uma fila, para permitir reconhecer onde começa e onde acaba. Essas cabeceiras e filas usam diferentes formatos segundo o protocolo usado. Os pacotes de dados podem ir encriptados por segurança (tradução nossa). (Fonte: <http://www.mastermagazine.info/termino/6223.php>. Acesso em: 27 junho 2016).

(www.cisco.com) que depois são convertidos por nossos computadores em códigos (198.133.219.25) que viajam no espaço cibernético ou ciberespaço, até chegar a seu destino em este caso "*CISCO.COM*", agora para fechar a comunicação, cisco responde ao usuário e logo os códigos são interpretados, e "traduzidos" pelos computadores em nomes (www.cisco.com). A relação "código-nome", é configurada nos dispositivos conectados em redes para poder fazer o encaminhamento e conversão *DNS*, ao ser roubada e alterada pelos atacantes, eles podem mudando o encaminhamento dos pacotes, redirecionando pacotes falsos a um servidor para sobre carregá-lo e deixa-lo inoperativo, e roubar os pacotes da informação, como por exemplo dados bancários, dados dos cartões de credito, entre outros.

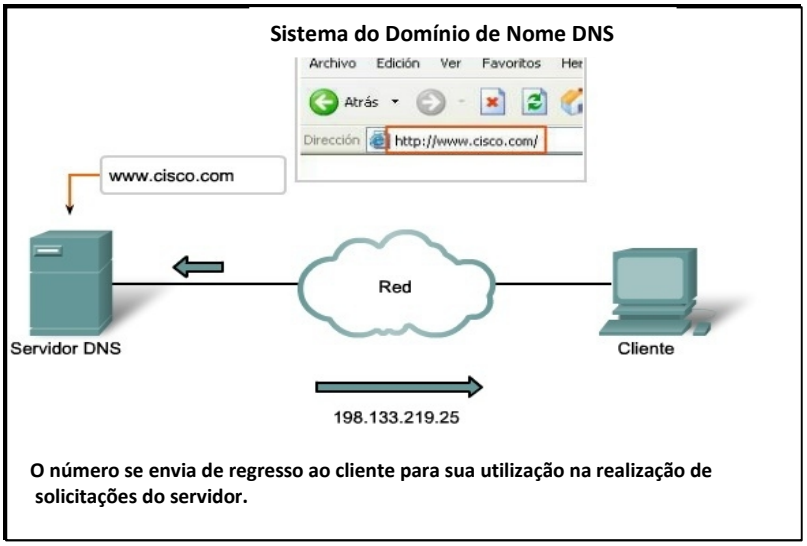

FIGURA 3: *Sistema do Domínio de Nomes DNS*.
Fonte: Camada de aplicação. Curso técnico de redes. SENAI, Brasil, 2016[29].

A segunda trata do direcionamento entre os provedores de serviço de Internet, o *Internet Service Protocol* (*ISP*)[30] e o uso de um sistema de comunicação conhecido como *Border Gateway Protocol* (*BGP*)[31] (CLARKE e KNAKE, 2015).

[29] Disponível em: <http://docplayer.com.br/752569-Curso-tecnico-de-redes-de-computadores-disciplina-de-fundamentos-de-rede.html>. Acesso em: 27 junho 2016.
[30] O *ISP* ou Provedor de Serviço de *Internet* é uma corporação ou agência do governo que fornece a conectividade por cabo ou sem fio a Internet até a casa do usuário, escritório ou computador móvel. Muitas vezes, os *ISPs* são empresas de telefonia ou provedores de televisão a cabo (Clarke e Knake, 2015, p. 227).

Resumindo, os pacotes de informação quando saem para o ciberespaço possuem um emissor e um destinatário, o BGP é o mensageiro que recebe e envia o pacote de informação, conforme a informação de destino.

Na seguinte figura explica-se o processo de comunicação ponto a ponto que fazem os *router*, entre o *ISP* do serviço de internet e o usuário com a utilização do *Border Gateway Protocol BGP*, eles são carregados nas tabelas dos *router* para realizar as conexões porta a porta, os hackers e guerreiros cibernéticos atacam a configuração do *router* para modificar as tabelas de encaminhamento do BGP, provocando que o trafego da Internet se perca ou que a mensagem não chegue no seu destino.

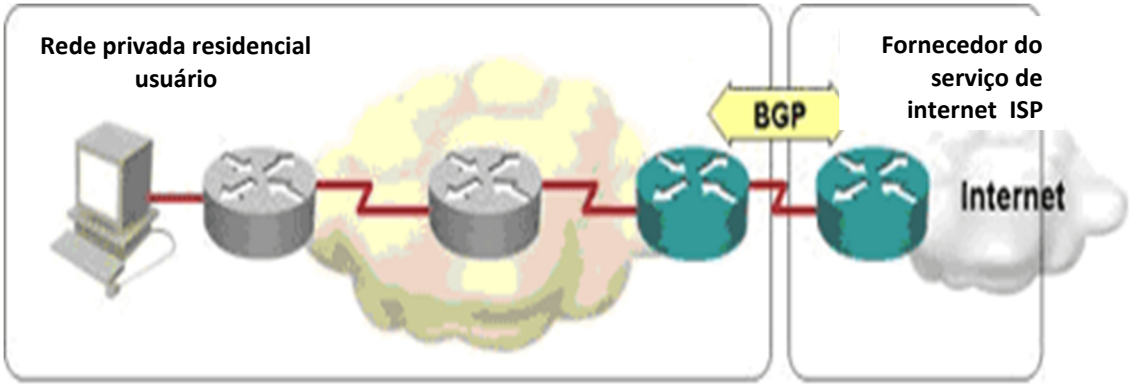

FIGURA 4 - Comunicação porta a porta, *BGP*.
Fonte: *BGP troubleshooting: Options that make the internet work*[32].

A terceira vulnerabilidade é a falta de governabilidade (CLARKE e KNAKE, 2015). Segundo Richard Clarke e Robert Knake, "ninguém está realmente no comando". No início da Internet, a ARPA (Agência de Projetos e Pesquisas Avançadas do Departamento de Defesa) assumiu a função de administradora de redes, mas agora ninguém tem este papel. Existem órgãos técnicos, mas poucas autoridades como a ICANN – corporação da internet

[31] O *BGP* ou *Border Gateway Protocol*, é um sistema de software em que os *ISPs* informam a outros *ISPs* que são seus clientes de forma que uma mensagem destinada para outro cliente possa ser roteada ou comutada para o *ISP* apropriado. Às vezes, um *ISP* pode ter outros *ISPs* como clientes. As tabelas não são altamente seguras e podem ser classificadas dependendo de um roteamento de dados incorretos (Clarke e Knake, 2015, p. 224).

[32] Disponível em: <http://searchtelecom.techtarget.com/feature/BGP-essentials-The-protocol-that-makes-the-Internet-work>. Acessado em: 27 julho 2016.

para atribuição de Nomes e Números –, pode ser considerada a organização que mais se aproxima das responsabilidades pelo gerenciamento de parte do sistema da Internet (CLARKE e KNAKE, 2015). Essa falta de governabilidade ou gerenciamento também é explorada pelos atacantes, já que não existe uma organização de fato responsável que possa corrigir as vulnerabilidades e a fortaleça com segurança, acabará sendo sempre atacada e vulnerável.

A quarta vulnerabilidade se refere à segurança dos pacotes de informação, os quais são feitos na maioria das vezes de forma aberta, ou seja, sem criptografia (CLARKE e KNAKE, 2015). Quando um pacote de informação sai para o espaço cibernético sem ser criptografado, a informação pode ser interceptada por um atacante com a finalidade de roubar o conteúdo, assim como acontece na Radiofrequência quando os sinais de rádio passam por uma intervenção (CLARKE e KNAKE, 2015). No caso da Internet, o acesso à informação é obtido por meio do provedor IPS, provedor de endereço de e-mail e uma técnica de monitoração de tráfego de rede conhecida como *Snoop*[33], a qual usa o *Sniffer de Pacotes*[34], ferramenta de trabalho que realizam a leitura de cada um dos pacotes de dados enviados por meio da rede.

A quinta vulnerabilidade é mais usada e corresponde à capacidade de propagar intensamente trafego malicioso projetado para atacar computadores (CLARKE e KNAKE, 2015). Os *malwares*[35] (código malicioso) conhecidos como vírus, *worms*[36], *phishing scams*[37],

---

33 O comando *Snoop* é apto para supervisar o estado das transferências de dados. O comando *Snoop* captura pacotes de rede e amostra seu conteúdo no formato especificado (EUA, 2016, tradução nossa). (Fonte: <https://docs.oracle.com/cd/E26921_01/html/E25871/gexkw.html>. Acesso em: 09 agostos 2016).

34 Um *sniffer* é um aplicativo especial para redes informáticas, que permite como tal capturar os pacotes que viajam por uma rede. Este é o conceito mais singelo que podemos dar ao respeito, mas aprofundando um pouco mais podemos dizer também que um *sniffer* pode capturar pacotes dependendo da topologia de rede (tradução nossa). (Fonte: <http://culturacion.com/que-es-un-sniffer/>. Acesso em: 9 agostos 2016).

35 O *Malware*, é uma descrição genérica geral para qualquer programa de computador que produza efeitos indesejados ou mal-intencionados. São considerados *malware* os vírus, *worms*, cavalos de Tróia e *back doors*. A ameaça utiliza, muitas vezes, ferramentas de comunicação populares, como e-mails e mensagens instantâneas, bem como mídias removíveis, como dispositivos USB, para se difundir. Além disso, também se espalha através de drive-by downloads e explorando vulnerabilidades de segurança em software. Atualmente, a maioria dos principais tipos de *malware* procura roubar informações pessoais que podem ser usadas para fins criminosos (Fonte:<https://www.symantec.com/pt/br/theme.jsp?themeid=glossario-de-seguranca>. Acesso em: 24 julho 2016).

são passados de usuário para usuário por meio da Internet, PC ou *notebook* com um *pendrive* infectado, aproveitando as vulnerabilidades do software e a Internet para alterar o funcionamento de um computador, estabelecer um ponto de acesso no sistema, copiar e roubar as informações pessoais.

A última vulnerabilidade da Internet trata da sua arquitetura, são milhares de milhões de circuitos virtuais integrados que originam uma descentralização total da arquitetura da rede (CLARKE e KNAKE, 2015). Esta vulnerabilidade e uma ameaça da seguridade do estado, que ocasionaria o caos em uma Cidade solo com desligar o sistema elétrico.

Neste aspecto, desde a década de 1960, a Internet tem crescido com a concepção política da época, descentralizada e conectada a milhares de milhões de redes com seu protocolo de transmissão básico conhecido como IP e sem nenhum tipo de segurança, tornando-se em uma plataforma fundamental para o ataque dos guerreiros cibernéticos e os *hackers* (CLARKE e KNAKE, 2015). Os desenvolvedores da Internet não tinham a intenção de que ela fosse controlada pelos governos, individualmente ou coletivamente, o que implicou que fosse projetado um sistema que não priorizasse a segurança e sim a descentralização.

2.4.2 Vulnerabilidades de Software e Hardware

A maior vulnerabilidade dentre as três que propiciam a guerra cibernética no ciberespaço, é o fato de existirem falhas no *software* e *hardware* (CLARKE e KNAKE, 2015). O *hardware* (PC, laptop, Servidor, router), que opera com um *software* (programas vírus, protocolos), representam as principais armas dos guerreiros cibernéticos. Por meio

---

[36] O *worms*. Definido no item número 31.

[37] O *Phishing* é um golpe que usa spam e mensagens instantâneas para levar pessoas a divulgarem informações confidenciais, como senhas de banco e dados de cartão de crédito. Normalmente, os ataques de *phishing* demonstram ser algo que não são como comunicados de instituições financeiras (Fonte: <https://www.symantec.com/pt/br/theme.jsp?themeid=glossario-de-seguranca>. Acesso em 24 julho 2016).

destes elementos informáticos, o homem interage com a Internet e se aproveita das suas vulnerabilidades para realizar os ataques.

O *software* é usado como um meio intermediário entre homens e máquinas para traduzir a intenção humana, por exemplo, encontrar horários de filmes on-line ou ler um blog em algo que sua máquina possa entender (CLARKE e KNAKE, 2015). As máquinas têm sua própria linguagem de comunicação, assim como a Internet. Isto é, traduzem tudo o que gostaríamos de fazer nessa linguagem binária, traduzindo em pacotes de dados para serem lançados posteriormente no espaço cibernético e recebê-los de volta.

A criação de programas em muitos linguagens de programação[38] é fundamentada no processo de escrever as instruções do código fonte[39], compilar e obter o programa executável, ou seja, para criar um *software* os programadores usam instruções em sua linguagem compreensíveis por eles, o qual é traduzido por meio de um compilador[40] convertendo-o em linhas de código[41] compreensíveis pelos computadores, e desta forma poder executá-lo, as instruções que deseja o programador que seu desenho de *software* faça, constitui o código fonte que cria os direitos de autor do programador, tornando-se detentor da propriedade.

---

[38] *Programming language* – linguagem de programação, é, (1) (ISO) -Linguagem artificial estabelecida para expressar programas de computador. (2) (TC 97) -Um conjunto de caracteres e regras usadas para escrever programas de computador (SAWAYA, 1999, p. 374). (Fonte:<http://comp.ist.utl.pt/aaa/Prog/Dicion%E1rio%20De%20Inform%E1tica%20&%20Internet%20Ingl%EAs-Portugu%EAs.pdf>. Acesso em: 10 agostos 2016).

[39] *Source code* – código-fonte, (1) Instruções de programa escritas numa linguagem de alto nível ou *Assembly language*, que podem ser lidas por uma pessoa, (2) Tradutor para código de objeto (SAWAYA, 1999, p. 439). (Fonte:<http://comp.ist.utl.pt/aaa/Prog/Dicion%E1rio%20De%20Inform%E1tica%20&%20Internet%20Ingl%EAs-Portugu%EAs.pdf>. Acesso em: 10 agostos 2016).

[40] *Compiler* – compilador, é um programa de computador mais sofisticado que um Assembler. Além de traduzir funções, o que é feito normalmente usando o mesmo processo que um Assembler, o compilador é capaz de suprir certos itens na entrada e na saída por meio de uma série de instruções denominadas rotinas. Assim, enquanto o Assembler traduz item por item e produz na saída o mesmo número de instruções e constantes que foram armazenadas, o compilador traduz e expande a versão do programa original (SAWAYA, 1999, p. 91). (Fonte:<http://comp.ist.utl.pt/aaa/Prog/Dicion%E1rio%20De%20Inform%E1tica%20&%20Internet%20Ingl%EAs-Portugu%EAs.pdf>. Acesso em: 10 agostos 2016).

[41] *Code* – código. (1) um sistema de símbolos para comunicação significativa. (2) um sistema de símbolos e regras usados na representação de dados ou instruções em um computador. (3) um programa em linguagem de máquina (SAWAYA, 1999, p. 84). (Fonte:<http://comp.ist.utl.pt/aaa/Prog/Dicion%E1rio%20De%20Inform%E1tica%20&%20Internet%20Ingl%EAs-Portugu%EAs.pdf>. Acesso em: 10 agostos 2016).

Na seguinte figura, observa-se a representação do processo de criação de programas, fundamentada no processo de escrever o código fonte entendível pôr os programadores, compilar e obter o programa executável e entendível pelos computadores, o compilador se encarrega de evitar que possa ser traduzido um programa com um código fonte mal escrito e fazer outras verificações prévias, de tal forma que o código máquina tenha certas garantias de ser realizado com padrões de sintaxes obrigatórios de uma linguagem. Ainda que exista essa ferramenta, o programador também comete erros de segurança ao realizar a transcrição e deixa aberto o acesso do *software* para outras pessoas não autorizadas. Estes erros permitem que os *hackers* entrem no *software* por meio de programas maliciosos alterando o código fonte, abrindo as portas de acesso e fazendo que o *software* se comporte de forma errada.

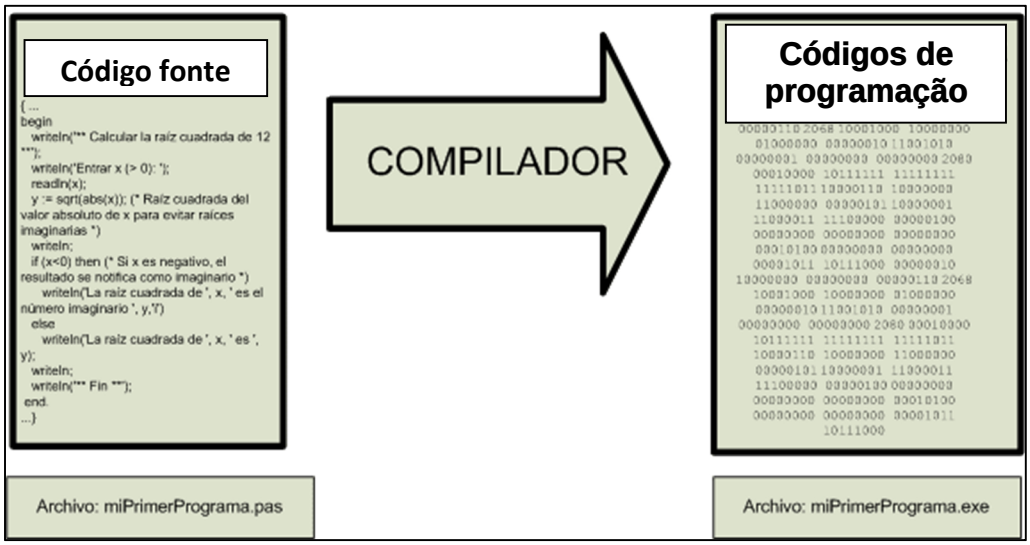

FIGURA 5 - Compilador e intérprete.
Fonte: APR. La máquina virtual Java (JVM o Java Virtual Machine). Bytecode. (CU00611B)[42].

Essas vulnerabilidades do software afetam diretamente ao hardware (laptops, PCs, router, switches, servidores), eles sem o software não podem funcionar, seriam umas caixas

[42] Disponível em: <http://aprenderaprogramar.com/index.php?option=com_content&view=article&id=392:la-maquina-virtual-java-jvm-o-java-virtual-machine-compilador-e-interprete-bytecode-cu00611b&catid=68:curso-aprender-programacion-java-desde-cero&Itemid=188>. Acesso em: 10 agostos 2016.

vazia, ou seja, sim o software é vulnerável o hardware também. Os hackers e os guerreiros cibernéticos sabem disso e usam programas maliciosos para deixar um ponto de acesso remoto para colocar bombas lógicas[43], destinadas a apoiar, queimar ou alterar o funcionamento do *hardware.* Agora no próximo item, veremos como são afetados a traves destas vulnerabilidades da internet, o software e o hardware os sistemas críticos conectados ao espaço cibernético.

2.4.3 Vulnerabilidades dos sistemas de controle conectados ao Ciberespaço

Da mesma forma que a Internet, o software e o hardware apresentam vulnerabilidades em seus desenhos, os quais são explorados pelos hackers ou guerreiros cibernéticos. As plataformas tecnológicas fazem funcionar grandes corporações de serviços, transportes, manufaturas, redes elétricas, entre outros, implicando que se tornem vulneráveis quando interagem com o espaço cibernético.

Durante a década de 1990, as empresas de tecnologia da informação mostraram como outras corporações poderiam poupar grandes quantidades de dinheiro utilizando sistemas de computador para executar suas próprias operações (CLARKE e KNAKE, 2015).

Muito além do e-mail ou do processamento de texto essas práticas de negócio envolviam controles automatizados, monitoramento de estoques, entregas em tempo real, analise de banco de dados e aplicações limitados de programas de inteligência artificial (CLARKE e KNAKE, 2015).

Portanto, pode-se assinalar o ponto relevante do tema, os sistemas SCADA[44], os quais controlam as subestações das empresas elétricas, os transformadores e os geradores de forma

[43] *Bomba logica*, é uma aplicação de software ou uma sequência de instruções que desligam um sistema ou rede e/ou apagam todos dados ou software da rede (Clarke e Knake, 2015, p. 224)

[44] Sistema de Supervisão e Aquisição de Dados (SCADA). Software para redes de dispositivos que controlam a operação de um sistema de máquina como válvulas, bombas, geradores, transformadores e braços robóticos. O

remota por meio da Internet. Se esses sistemas forem atacados por pessoas inescrupulosas, cidades inteiras ficariam sem eletricidade (CLARKE e KNAKE, 2015).

Destas afirmações de Richard Clarke e Robert Knake se pode dizer, que o empurre tecnológico da década dos 90, a automatizando os processos financeiros, o controle de processos de negócio de maneira remota, as administrações de bancos de dados por sistemas inteligentes, entre outras, fizeram possível a conexão de estações elétricas ao espaço cibernético, omitindo os riscos do segurança e vulnerabilidade da internet, o software e hardware.

Esta automatização dos processos de controle, produto da modernização dos últimos tempos e, ao mesmo tempo, querer controlá-los remotamente via Internet mesmo com as vulnerabilidades mencionadas acima, faria com que os *hackers* e guerreiros cibernéticos tivessem a oportunidade de atacar esses sistemas com a finalidade de alterar, roubar e destruir conforme o objetivo para o qual foi criado.

Em na gráfica representasse uma planta onde as principais válvulas, manômetros, chaves, e sistemas do controle, estão automatizados por SCADA, assim como os usuários podem controlar remotamente todos estes sistemas os atacantes também.

---

software SCADA coleta informações sobre as condições e atividade de um sistema e envia instruções para os dispositivos, muitas vezes para efetuar movimentos físicos. As instruções enviadas para os dispositivos em redes SCADA são, ás vezes, transmitidas por meio da Internet ou via ondas de rádio e não são criptografadas. Quando os dispositivos recebem as instruções, eles não validam quem as envio (CLARKE e KNAKE, 2015, p. 228).

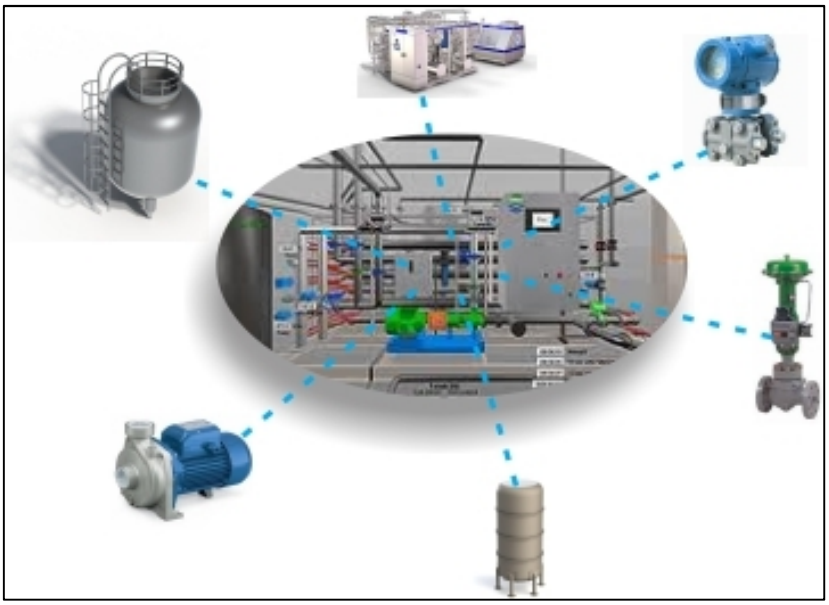

FIGURA 6 - Sistemas SCADA.
Fonte: Serviços de Informações da Tecnologia do Sistema SCADA, Rocatek[45].

Agora bem, conhecendo estes conceitos que caracterizam este novo cenário como uma ameaça contra a segurança do Estado, no seguinte capítulo estudaremos alguns feitos históricos onde as ameaças e vulnerabilidades que fazem possível o desenvolvimento da guerra cibernética foram utilizadas para dominar o espaço cibernético.

[45] Disponível em: <http://www.rocatek.com/sistema_supervision.php>. Acesso em: 10 agostos 2016.

3 ATAQUES CIBERNÉTICOS NA HISTÓRIA

Neste capitulo, adentrar-se-á na evolução da Guerra Cibernética até os dias de hoje, tem como objetivo apresentar e analisar casos e exemplos históricos de ocorrência de ataques cibernéticos, como também o entendimento das ameaças e vulnerabilidades citadas no capítulo anterior aplicadas em exemplos reais, e como sou utilizado todos aqueles elementos que integram o campo de batalha.

3.1 Ataques DDoS[46] com utilização de *botnets*[47] Estônia (2007)

Um dos casos mais notório desses ataques ao Estado aconteceu em 2007 na Estônia, em que ciberterroristas atacaram os sites do governo, o que para Estônia, um país que tem quase todos os seus serviços na Internet, sendo considerado um país digitalizado, causou vários problemas nesses serviços, afetando diretamente a população. Esse é considerado o primeiro ciberataque de grandes proporções.

Os ataques cibernéticos à Estônia iniciaram-se o 27 de abril de 2007 e deixou sites do governo fora do ar. O governo estoniano acusou a Rússia, que teria se motivado a realizar os ataques por conta da remoção de uma estátua que marcava a vitória russa contra o nazismo, a estátua do Soldado de bronze de Tallinn, porém confirmou-se que o governo russo não estava

[46] Ataque Distribuído de Negação de Serviço (DDoS). Técnica básica de guerra cibernética frequentemente utilizada por criminosos e outros personagens não estatais em que um site da Internet, um servidor ou um roteador é inundado com mais solicitações de pacotes que o site pode responder ou processar. O resultado disso é que o trafego legitimo não consiga acessar o site e este fica em um estado desligado. *Botnet* são utilizadas para conduzir tais ataques, “distribuídos” o ataque ao longo de milhares de computadores que agem com um único fim: derrubar o recurso (CLARKE e KNAKE, 2015, p. 223).

[47] *Botnet*. Uma rede de computadores forçada a operar sob comandos de um usuário remoto não autorizado, geralmente sem o conhecimento de seu dono ou operador. Essa rede de computadores “*robot*” é então utilizada para realizar ataques a outros sistemas. Uma *botnet* geralmente tem um ou mais computadores de controle, que estão diretamente associados ao operador por de trás da *botnet*, para o envio de ordens a dispositivos controlados secretamente. Os computadores da *botnet* são frequentemente referenciados como “*zombis*”. *Botnet* são utilizadas, entre propósitos, para conduzir inundações de mensagem (veja DDoS) (CLARKE e KNAKE, 2015, p. 224).

envolvido diretamente nos ataques, sendo sua origem desconhecida até hoje (CARREIRO[48], 2012).

Se recordando as seis vulnerabilidades da internet DNS, BGP, Propagação e Infecção, Falta de Criptografia, Falta de Governança, e Descentralização, analisadas no capítulo anterior, Estônia por ser um pais altamente ligado a internet converte-se também em um pais altamente vulnerável aos ataques cibernéticos, quase todos os serviços são integrados à Internet, o que torna o país vulnerável a esses ataques. Quase todas as tarefas cotidianas estão ligadas à rede, por isso a população do país foi atingida diretamente com o ataque.

No caso da Estônia, uma série de sites governamentais e de empresas locais foi tirada do ar ou alterada para exibir conteúdo diferentes dos originais (um tipo de vandalismo digital conhecido como *defacement*[49]). O método de ataque que indisponibilizava os sites eram simples – a geração de gigantescas quantidades artificiais de pedidos de acesso, até os sistemas não conseguirem mais processá-las e saírem do ar. Essa técnica de ataque, conhecida como *Distributed Denial of Service* (DDoS) exige participação em massa de computadores dedicados ao processo – com ou sem o conhecimento de seus proprietários (CARREIRO, 2012).

Em outras palavras, infectando as redes com *botnet* a nível mundial, e aproveitando as vulnerabilidades da internet, com a utilização da família de protocolos TCP/IP, os atacantes conseguiram fazer um ataque de denegação de serviço (DDoS e *defacement*), fazendo que

[48] Tecnólogo em Processamento de Dados (PUC-Rio), administrador de redes especializado em segurança; bacharel em História (UFRJ), mestre em Relações Internacionais, Segurança e Defesa Nacional (Pró-Defesa/PPGHC/UFRJ), doutorando em História Comparada (PPGHC/UFRJ) e membro do grupo de pesquisa UFFDefesa. (Fonte:< http://www.historia.uff.br/cantareira/v3/wp-content/uploads/2013/05/e17a9.pdf>. Acesso em: 26 de junho 2016).

[49] *Defacement* ou, como é conhecido de maneira popular, deface, é uma técnica que consiste na realização de modificações de conteúdo e estética de uma página da web. A palavra de origem inglesa é utilizada na segurança da informação para categorizar ataques realizados por defacers, que são usuários de computador que na maioria das vezes possuem pouco conhecimento técnico e, por isso, precisam de várias horas para explorar vulnerabilidades de um site a fim de alterar sua página principal através de um servidor. (Fonte: < http://canaltech.com.br/o-que-e/o-que-e/O-que-e-defacement-ou-deface/>. Acesso em: 11 de agosto 2016).

milhares de milhões de computadores a nível mundial fizeram solicitações de conexões a os servidores do Estônia, impedindo o uso legítimo dos usuários ao usar um serviço de rede.

Apesar disso, o governo da Estônia prontamente acusou a Rússia de coordenar o ataque – algo que confronta o modus operandi do ataque pulverizado em questão. Embora o governo Russo tenha negado diplomaticamente o ataque, a Estônia tratou o caso como uma violação real a seu território, invocando o suporte militar da OTAN, que despachou um time de especialistas em TI para observar o cenário e auxiliar a retomada dos serviços. Pela primeira vez, a OTAN admitiu em público a relação entre ataques virtuais e uma guerra real: “Se o centro de comunicação de um estado-membro é atacado com um míssil, você chama isso de um ato de guerra. Então, do que você chama se a mesma instalação é desabilitada por um cyberataque? (CARREIRO, 2012).

Com este ataque *DDoS* a Estônia 2007, vemos que começa a opinião pública mundial a dar-lhe importância ao tema da guerra cibernética, e a pensar na segurança de seu ciberespaço. Começa também uma disputa internacional entre Rússia e Estônia, até nossos dias, e a pesar de as acusações de Estônia sob Rússia, não há responsáveis.

3.2 Ataques DDoS com utilização de *botnets* Geórgia (2008)

A Republica de Geórgia Situada mais ao Sul da Rússia, junto ao Mar Negro, a Geórgia era vista como a área de influência de Moscou. Em agosto de 2008, a Geórgia e Ossétia do Sul iniciaram um sério conflito. Os georgianos intensificaram os ataques militares e, no dia seguinte a este ataque, a Rússia interveio no conflito a favor da Ossétia do Sul, declarando guerra contra a Geórgia, deslocando rapidamente seu exército e expulsando os georgianos da Ossétia do Sul. Precisamente no mesmo dia do ataque terrestre russo, houve uma grande movimentação de ataques cibernéticos contra a Geórgia (CLARKE e KNAKE 2015).

Na Geórgia, os ataques foram diferentes a Estônia, ocorrendo no contexto do conflito militar russo georgiano na Ossétia do Sul. Contudo, apesar de se situar no meio de um conflito militar real, os ataques foram similares aos da Estônia em 2007 – *defacement* de sites, como do Parlamento da Geórgia, acompanhados de DDoS que tiraram do ar sites oficiais como o da página oficial do presidente e do Ministério do Exterior. Sites russos também foram atingidos, assim como páginas da Ossétia do Sul. (CARREIRO, 2012)

Os efeitos destes ataques foram devastadores. Os roteadores que demandavam às redes da Geórgia, com dados oriundos dos tráfegos da Rússia e Turquia, praticamente pararam devido à inundação de pacotes nas redes criada pelos ataques DDoS com utilização de *botnets*. Além disso, os atacantes assumiram os controles de roteadores da *internet* situados na Geórgia, fazendo com que a população ficasse sem comunicação com o mundo externo, sem receber notícias, *e-mails* e sem acesso à rede de dados. As tentativas de defesa eram ineficazes. Novos ataques eram realizados a partir de qualquer tentativa de bloqueio. (CLARKE e KNAKE, 2015).

Uma das ações de proteção cibernética foi a de bloquear o tráfego oriundo da Rússia, mas os ataques foram redirecionados e chegaram a passar pela China. A Geórgia transferiu os servidores de seu governo para as redes do *Google* na Califórnia (EUA) para que pudessem voltar a operar, mesmo assim, os servidores foram alvos de ataques contínuos. A rede bancária foi praticamente neutralizada, além das redes de cartões de crédito e sistemas de telefonia móvel (CLARKE e KNAKE 2015).

O Governo russo negou a participação e citou que acreditava ser uma resposta popular. Para este caso, há fortes indícios de que alguns sítios que foram utilizados como origens dos ataques estavam hospedados em *links* do aparato de inteligência Russo. Cabe deduzir que as ações orquestradas nos ataques não seriam possíveis de serem realizadas por uma cruzada patriótica cibernética somente baseada no clamor popular (CLARKE e KNAKE 2015).

Neste caso de ataque cibernético a Geórgia vemos novamente, a pulverização dos DDoS e outros métodos primitivos de ataque, os quais permitem criar um cenário consideravelmente hostil com a participação de Guerreiros cibernéticos treinados e com armas cibernéticas [50] capazes de danificar a infraestruturas, e atentar contra a Segurança Nacional de um Estado. Com respeito ao desenvolvimento dos ataques verificamos ações de defensa cibernética, como bloquear o tráfego oriundo de uma região, e transferir os servidores para outras redes mais seguras para que pudessem voltar a operar, e ao igual que Estônia .as acusações persistem sem nenhum responsável sancionado.

3.3 O ataque por meio da inserção do código malicioso *Stuxnet*[51], Irã (2010)

Agora, no caso do Irã temos não um ataque do tipo DDoS e *defacements* – mas o aparente uso de uma ferramenta específica, o *worm* Stuxnet, que teria sido capaz de atingir e danificar centrífugas nucleares iranianas de Bushehr.

Em 2010, o Irã sofreu um poderoso ataque cibernético que afetou os computadores da central nuclear. O *Stuxnet* é um vírus informático que afeta os equipamentos que trabalham com Windows, descoberto em junho de 2010 pelo Vírus *BlokAda*, uma empresa de segurança localizada em Bielorrússia, *Stuxnet* é um programa malicioso sofisticado com alto valor tecnológico agregado, produzido em laboratório (SYMANTEC, 2011).

Este vírus foi produzido, especialmente, para atacar o sistema SCADA que controlava as usinas nucleares de Irã, a fim de frear o programa de enriquecimento de urânio. Além de

[50] Armas cibernéticas ou Ciberarmas: são instrumentos, meios ou dispositivos úteis para operar no ciberespaço, destinados a atacar ou defender (tradução nossa). (Fonte:< http://molinamateos.com/content/conceptos-y-definiciones-0.>. Acesso em: 29 junho 2016).

[51] *Stuxnet* é um verme informático que aponta aos sistemas industriais de controle que se utilizam para controlar instalações industriais como plantas de energia elétrica, represas, sistemas de processamento de desfeitos entre outras operações industriais. (Fonte: < https://www.symantec.com/es/mx/page.jsp?id=stuxnet>. Acesso em: 29 junho 2016).

ser acionado à distância, é um vírus instável e migra com rapidez. A medida que se começa a contra-atacá-lo, o vírus muda de versão. (SYMANTEC, 2011).

O *Stuxnet* é um programa desenhado para afetar um hardware específico – o controlador-programador lógico (PLC) Siemens S7-300, com drives de frequência variável fabricados por apenas dois vendedores: a empresa Vacon, finlandesa, e a Fararo, iraniana. Mais ainda, ele ataca apenas os motores que funcionam entre a frequência de 807 e 1210Hz – incluindo aí as centrífugas a gás de enriquecimento de urânio. Ao encontrar tão específicos parâmetros de funcionamento, o *Stuxnet* altera o funcionamento dos motores, ocultando essa diferença em sua operação e inviabilizando seu funcionamento. O Stuxnet não foi disseminado através da Internet, mas de *pendrives* contaminados. Essa diferença é crucial e identifica o Stuxnet como uma sofisticada ferramenta de sabotagem, empregada localmente, tornando sua ação compatível com um ato de espionagem tradicional – ou seja, para sua inoculação ele dependeu da mão humana em uma ação direta e local. (CARREIRO, 2012)

Conclui-se que o constante monitoramento e adoção de políticas de segurança não são suficientes para garantir a proteção das redes e dos dados, já que em este caso as centrífugas iranianas não tinham justificativa operacional alguma para estarem conectadas à Internet. O contágio pelo *Stuxnet* exigiu o contato direto com o equipamento – o que traz a questão de que, como esse contato direto já foi conseguido, qualquer outro tipo de sabotagem era possível. A falha de segurança foi no controle de acesso humano – não na insegurança da Internet.

Conhecidos os conceitos e feitos históricos, passemos a observar as medidas frente a um ataque cibernético.

4 O QUÊ FAZER DIANTE UM ATAQUE CIBERNÉTICO

Considerando as vulnerabilidades apresentadas no capítulo dois, e os feitos históricos no capítulo três, abordar-se-ão os conceitos relacionados com as medidas de segurança adotadas pelos países e especialistas em segurança da informação, os quais permitirão compreender o que deve ser feito antes, durante e após o ataque cibernético.

4.1 O quê fazer antes do ataque cibernético

O tema da segurança da informação é um tema complexo que deve ser atualizado diariamente; os últimos métodos e ferramentas conhecidas pode nós fazer acreditar que estamos protegidos mas é provável que estejamos sendo atacados. Agora, o primeiro que deve ser considerado com esta nova modalidade de guerra é a prevenção por meio da aplicação dos conceitos de segurança da informação, particularmente, no aspecto da cibersegurança (proteção do espaço cibernético) e sua relação com a prevenção e detecção das ameaças.

Percebeu-se que alguns países como os Estados Unidos, a China e a Espanha, entre outras nações, já se organizaram para controlar o ciberespaço por meio da criação de instituições com recursos humanos capacitados com a finalidade de proteger o ciberespaço. A Espanha tem o DSN[52] (Conselho Nacional de Segurança), o qual estabelece que:

> O grau de dependência de nossa sociedade em relação às TICs e o ciberespaço cresce diariamente. Conhecer suas ameaças, gerenciar os riscos e articular uma adequada capacidade de prevenção, defesa, detecção, análise, investigação, recuperação e resposta constituem os elementos essenciais da Política da Cibersegurança Nacional (Tradução nossa).

[52] O DSN Conselho de Segurança Nacional que em sua condição de Comissão Delegada do Governo para a Segurança Nacional é o órgão que deve atender o Presidente do Governo em relação à política de Segurança Nacional e ao Sistema de Segurança Nacional, assim como exercer as funções determinadas pela Lei de Segurança Nacional e regulamentadas pelo seu regimento (tradução nossa). (Fonte: <http://www.dsn.gob.es/es/sistema-seguridad-nacional/consejo-seguridad-nacional>. Acesso em: 27 junho 2016).

Os europeus criaram a Agência Europeia de Segurança das redes e da informação (ENISA[53]) para lutar contra as violações da segurança das redes e dos sistemas de informação, com a finalidade de reforçar as capacidades da União Europeia, seus Estados Membros e as empresas para a prevenção, reação e gestão dos problemas relacionados com a segurança das redes e informação. Mas, este não é o único objetivo porque acaba prestando assistência e assessoramento à Comissão e aos Estados da União Europeia toda vez que a requerem. Esta agencia também ajuda, a Comissão nos trabalhos preparatórios de caráter técnico de atualização e desenvolvimento da normativa comunitária.

Os autores Clarke e Knake no seu livro "Guerra Cibernética", p. 31, afirmam que os Estados Unidos foi o primeiro país a criar uma organização com o objetivo de combater neste novo domínio por meio do Comando Cibernético das Força Aérea dos Estados Unidos.

Em outubro de 2009, quando as portas da multiforça Militar se abriam, a articulação do comando cibernético dos Estados Unidos, a Marinha já havia seguido a Força Área na criação de sua própria unidade de Guerra Cibernética (CLARKE e KNAKE, 2015, p. 33).

Os Estados Unidos têm a *TRÍADE* defensiva, que seria uma continuação do que foi feito por Clinton em seu Plano Nacional como Bush em sua Estratégia Nacional quando procuraram fazer com que todas as infraestruturas críticas essenciais se defendessem de ataques cibernético (CLARE e KNAKE 2015, p. 131).

Portanto, é possível perceber a progressão do conceito de guerra cibernética ao evoluir dentro das Forças Armadas dos Estados Unidos, tornando o controle do espaço cibernético uma necessidade de extrema importância estratégica do novo milênio. Do outro lado do mundo, a China não fica atrás porque também se prepara para controlar o espaço cibernético.

[53] A Agência Europeia de Redes e Segurança da Informação (ENISA) é um centro de excelência para segurança cibernética na Europa. A Agência se encontra localizada na Grécia, com sede à Heraclião, em Creta e um escritório operacional em Atenas (Tradução nossa). (Fonte: <https://www.enisa.europa.eu/about-enisa>. Acesso em: 28 junho 2016).

Em 2003, a China anunciou a criação de unidades de Guerra Cibernética, situadas na Base Naval da Ilha de Haimam, onde se encontram o terceiro departamento técnico do PLA[54] e as Instalações de Inteligência de Sinais de Lingshui (CLARKE e KNAKE, 2015).

Os chineses com essas unidades começaram a planejar a prevenção diante dos ataques cibernéticos desenvolvendo armas de ataque cibernético jamais vistos antes.

Clarke e Knake, 2015, apresentam dez exemplos das armas e técnicas aplicadas pelos chineses:

- Instalação de minas de informação;
- Realização de reconhecimento de informações;
- Alteração de dados de rede;
- Lançamento de bombas de informação;
- Lançamento de informações lixos;
- Aplicação de dissimulação de informações;
- Divulgação de informações clonadas;
- Organização de defensa da informação; e
- Estabelecimento de estações de redes espiãs.

Observa-se nestes exemplos que no âmbito mundial, as grandes potências e outros países têm se organizado para controlar o ciberespaço.

Diante dos exemplos no âmbito mundial, as grandes potências e outros países tem se organizado de tal forma a administrar a segurança para enfrentar as vulnerabilidades que tornam possível o ataque cibernético. Essas nações desenvolveram ferramentas, metodologias e técnicas, além de capacitar o pessoal técnico especializado com a finalidade de controlar o espaço cibernético, proteger seus sistemas de informação, detectar ataques e se for necessário, atacar também.

[54] O PLA é o Exército Popular de Libertação, braço armado da República Popular da China, fundado em 1 de agosto de 1927 (comemorado anualmente como “Dia do Exército Popular da Libertação”), como extensão militar do Partido Comunista da China (PCC). Sua insígnia é composta por dispositivo arredondado com uma estrela vermelha que contém os ideogramas chineses para primeiro do oitavo (1 de agosto) alusivo à Revolução de Nanchang (tradução nossa). (Fonte: <http://www.eurasia1945.com/protagonistas/ejercitos/ejercito-de-liberacion-popular/>. Acessado em: 28 junho 2016).

4.2 O quê fazer durante um ataque cibernético

A ideia de uma grande unidade estratégica que siga políticas de segurança de Estado, com alta capacidade de controle do ciberespaço por meio da aplicação de métodos, procedimentos, armas cibernéticas e a preparação de um ciberespaço pronto para a batalha, acaba ajudando no bloqueio e detecção do agente atacante, para levantar todos os sistemas afetados e estabilizá-los com normalidade de forma transparente para organização e, portanto, evitando o nível de instabilidade de crise[55]. Nesta área, muitas empresas de segurança da informação (antivírus e auditoria) recomendam aplicar ações rápidas de corte do ataque, em seguida identificação da ameaça e finalmente, correção dos danos causados.

Quando do ataque, o primeiro a ser compreendido é que a segurança é falha e que devem ser tomadas ações para resolver essa situação. A empresa Norton, líder em segurança da informação, recomenda que os usuários devem aplicar as seguintes medidas:

> *1.Desconectar-se imediatamente.* Tire da tomada o cabo de rede, de telefone ou de dados do equipamento. Deste modo, é possível evitar que os dados cheguem até o atacante. Os *bots* também podem utilizar seu equipamento como zumbi em um ataque coordenado de maior escala. Desconectar a conexão da rede é um método infalível para evitar danos imediatos.
> *2.Analise seu equipamento com um programa antivírus atualizado* como o Norton Antivírus ou Norton Internet Security (um pacote completo de *software* de segurança). Um programa com funções de antivírus e *antispyware* pode detectar e, com frequência, eliminar as ameaças de *softwares* de atividades ilegais que, de outra forma, permaneceriam escondidas no equipamento.
> *3.Realice cópias de respaldo de sua informação importante.* Os softwares de atividades ilegais podem transmitir dados confidenciais e até destruí-los ou durante a tarefa de limpeza podem ser perdidos involuntariamente.
> *4.Pense na possibilidade de voltar a começar do zero e reinstalar o sistema operacional do equipamento* (por exemplo: Microsoft Windows) ou usar o software de cópia de respaldo. Os exemplos de software das piores atividades ilegais são bastantes complexos para adentrar no sistema com a intenção de ficarem escondidos do software de segurança por meio de técnicas "rootkit" (tradução nossa)[56].

[55] Instabilidade de Crise: Em um período de elevadas tensões e hostilidades entre nações, podem existir precondições ou ações tomadas por um lado que fazem com que a outra nação acredite que a sua melhor alternativa e agir de forma mais agressiva. Essa condição pode levar a decisões para escalar ações militares (Clarke e Knake 2015, p 226).
[56] Disponível em: <http://mx.norton.com/cybercrime-victim>. Acessado em: 29 junho 2016.

Estas recomendações, de forma muito genérica, representam quatro passos para a desconexão, busca da vulnerabilidade, restauração dos danos e levantamento dos sistemas afetados. No âmbito do usuário, esse cenário é aplicado da mesma forma mas em maior escala, porque não se trata apenas de computador pessoal mas da rede mundial da Internet, a rede estadual ou os sistemas críticos com a mesma finalidade de roubar, destruir ou alterar o bom funcionamento dos sistemas.

No caso da política norte-americana, a *TRÍADE* é fundamentada na proteção de sua principal plataforma de comunicação, o *Backbone* da Internet, por meio da exigência da segurança e monitoração do tráfego dos *IP*s primários e secundários. Também a exigência de segurança em vários níveis das empresas de rede elétrica com seu rigoroso regulamento obrigatório pelo Estado para a conexão de monitoração remota e, finalmente, o estabelecimento da ciberdefesa em sua própria rede de segurança nacional, proporcionando um ótimo resultado para o governo dos EUA., permitindo-lhes detectar, prevenir e cortar a atividade inimiga, reparar os danos e restaurar os sistemas rapidamente, nas três principais redes públicas: Internet, sistemas críticos e redes de segurança de Estado.

4.3 O quê fazer depois do ataque cibernético

No momento da investigação, na sequência dos eventos diante do ataque cibernético deve ser considerado o pior, ao contar com uma grande unidade especializada na Guerra Cibernética com um pessoal altamente capacitado na área de segurança da informação e a ciberdefesa falha e provocando danos gravíssimos para corrigir. Isto é, o objetivo de prevenção, descoberta e bloquear a ameaça falha.

Neste cenário formulado, deve-se realizar um procedimento conhecido em segurança da informação como Forense Computacional[57], também conhecido por informática forense, computação forense, análise forense digital (AFD) ou exame forense digital. Não importa o nome usado e sim o diagnóstico geral da plataforma de informação atacada, onde pode ser determinado o que aconteceu, quais vulnerabilidades foram exploradas pelo atacante, se o ataque foi externo ou interno e, finalmente, avaliar os danos ocasionados para reforçar a cibersegurança, corrigir as vulnerabilidades e restaurar o funcionamento dos sistemas de forma rápida para não afetar a operação da organização.

Miguel López, espanhol, especialista em segurança da informação afirma que dentro da Análise Forense Digital podem ser destacadas as seguintes fases:

1. Identificação do incidente;
2. Coleta das evidências;
3. Preservação das evidências;
4. Análise da evidência;
5. Documentação e apresentação dos resultados.

Em caso de realizar a primeira análise e ainda persistirem suspeitas de que o incidente foi provocado internamente da rede, será necessário formular a possibilidade de realizar uma investigação interna da organização para apurar as responsabilidades. Somente será necessário coletar informação suficiente, quantitativa e qualitativamente, para poder acionar disciplinas posteriores, sem chegar até os tribunais. Nesta situação, além do equipamento técnico para dar respostas aos incidentes, deve-se contar com outros departamentos como Recursos Humanos e até o Sindicato (LOPEZ, 2007).

[57] Forense, trata-se do *Computer Forensics* ou *Análise Forense Digital*. Essa disciplina é praticamente nova e se aplica tanto para a pesquisa de delitos tradicionais (homicídios, fraudes financeiras, narcotráfico, terrorismo, etc.), como para aqueles voltados com Tecnologias da Informação e Comunicação. Destaca-se a pirataria de software e comunicações, distribuição de pornografia infantil, intromissões e *hacking* em organizações, *spam*, *phishing*, etc (tradução nossa). (Fonte: <http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf>. Acesso em: 30 junho 2016).

Quando o resultado da investigação indicar um crime cibernético[58], o processo deve ser ainda mais formal, estabelecendo responsabilidades conforme o caso, sancionadas pelos órgãos judiciais, pelas leis nacionais e internacionais. Este tema é complexo e polêmico no âmbito mundial, porque pode iniciar um conflito armado entre Nações.

Em 1997, o Conselho da Europa, por meio do Conselho de Ministros, designou um Comitê de Especialistas do Ciberespaço integrado por policiais, juristas e informáticos, convidados de peso para a sociedade da informação global de países não europeus (EUA., Canadá, Japão e Austrália) para debater os problemas gerados por uma incipiente delinquência na Internet. Após quatro anos e 25 rascunhos revisados, a comunidade internacional aceitou o Convênio sobre Ciberdelinquência, aprovado e firmado pelo Plenário do Conselho de Ministros em Budapeste no dia 23 de novembro de 2001.

O Convênio tem a finalidade de harmonizar a legislação dos diversos países que o assinaram, não apenas o direito penal substantivo, mas o direito processual para enfrentar esse tipo de delinquência. O Convênio define os delitos informáticos os agrupando em quatro categorias:

> a. Delitos contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos.
> b. Delitos pelos seus conteúdos, que compreende condutas que englobam os delitos relacionados com a posse e distribuição de conteúdo de pornografia infantil na Rede.
> c. Delitos relacionados com a Informática, entre eles, dois tipos penais: a falsificação, informática e fraude informática.
> d. Delitos relacionados com infrações da propriedade intelectual e dos direitos afins (Espanha 2011, tradução nossa).

Neste grupo, o Convênio faz um levantamento normativo dos tratados e convênios internacionais sobre a propriedade intelectual, que engloba as condutas de acesso ilícito, interceptação ilícita, interferência de dados, interferência dos sistemas e o abuso de dispositivos.

[58] O Crime Cibernético é um conceito usado socialmente para determinar um conjunto de condutas que atingem os direitos à terceiros e produzem um cenário ou meio tecnológico, provocando uma rejeição social e sob aquelas mediadas pelo direito penal (tradução nossa). (Fonte: <http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf>. Acesso em: 30 junho 2016).

Especialistas em segurança da informação, como Clarke e Knake 2015, afirmam que nenhuma segurança é perfeita, apenas minimizam os dados e capacidade de resposta ao ataque. Clarke e Knake declaram que é necessário dificultar ao máximo para que nenhum ataque desative a capacidade de resposta do poder militar ou que mine severamente a economia (CLARKE e KNAKE, 2015).

Se os usuários não são capazes de detectar suas vulnerabilidades, os delinquentes podem fazê-lo de forma muito eficiente. Proteger os usuários é quase impossível, mas fortalecer as redes que os atacantes usam como alvo em um Estado ou nação é muito provável com a concessão das vulnerabilidades por meio da cibersegurança. Trata-se de tornar difícil a possibilidade de ataque com a finalidade que o atacante desista e abandone a atividade do ataque cibernético.

Todo crime implica na investigação, principalmente, no âmbito policial, no âmbito cibernético, os especialistas em segurança da informação utilizam a Ciência Computacional Forense, o qual oferece respostas às indagações durante a detecção do ciberataque[59], por meio de um conjunto de técnicas destinado a extrair dados valiosos da fonte original, o computador, o dispositivo móvel, o disco, etc., sem alterar o estado dos mesmos. Isto é uma prova chave em inúmeras ocasiões, entre eles: os problemas de privacidade, roubo de informação confidencial, revelação de segredos, espionagem industrial e fraude.

A ESET NOD32[60] Latino-Americana, empresa de segurança da informação enumera as ações que deve desenvolver uma empresa para superar um ataque onde os recursos da organização podem ser afetados:

---

[59] O *Ciberataque* é qualquer tipo de manobra ofensiva feita por indivíduos ou organizações que atacam os sistemas de informação como as infraestruturas, redes de computadores, bases de dados localizadas em serviços remotos, por meio de atos maliciosos usualmente originados por fontes anônimas que também roubam, alteram ou destroem um alvo específico por meio da invasão de um sistema vulnerável (tradução nossa). (Fonte: <http://www.nsciva.org/CyberReferenceLib/201011Joint%20Terminology%20for%20Cyberspace%20Operations.pdf>. Acesso em: 01 julhos 2016).

[60] A *ESET NOD32*, é uma empresa pioneira em proteção antivírus, nasceu da criação de um multipremiado software para a detecção de ameaças (tradução nossa). (Fonte: <http://www.eset-la.com/compania>. Acesso em: 01 julhos 2016).

> Passo 1: *Determinar o alcance da infecção.* Neste passo, a reação rápida é extremamente importante.
> Passo 2: *Assegurar a continuidade do serviço.* Se a fuga da informação compromete os empregados e usuários finais, deve alertar e aconselhar os mesmos para que estejam atentos a qualquer movimento estranho que possa apreciar sobre seus dados.
> Passo 3: *Deter a infecção*. Isto deve acontecer com o isolamento dos equipamentos comprometidos. A suspensão dos segmentos da rede, evita que a infecção continue se espalhando por meio da rede corporativa e interrompa qualquer conexão que possa ter estabelecido com o atacante para o roubo da informação.
> Passo 4: *Diminuir a infecção e eliminar o vetor do ataque.* A remoção da peça maliciosa implica na análise minuciosa do código para compreender seu funcionamento. As soluções do antivírus proporcionam um suporte para essas atividades, permitindo a automação da desinfecção e economia do tempo no processo de resposta.
> Passo 5: *Aprender dos erros.* Realizar uma profunda investigação do acontecido, ajuda a melhorar os processos dentro da organização. A eliminação das vulnerabilidades, identificação de outros potenciais pontos de acesso do sistema que não tinham sido antes considerados dentro do leque de vetores do ataque (tradução nossa)[61].

Analisar os custos, o ataque é muito econômico e, na maioria das vezes, as ferramentas são gratuitas e de fácil acesso na Internet. Entretanto, a defesa requer um gasto maior e com ferramentas externas de *hardware, software* e redes elaboradas por empresas especialistas em segurança da informação que oferecem esse serviço e ferramentas internas desenhadas e implementadas pela organização por meio do pessoal técnico especializado (guerreiros cibernéticos), o qual requer um investimento alto em relação ao adestramento e capacitação. No caso de não contar com esse pessoal, é necessário oferecer benefícios e salários adaptados no mercado profissional na área, os quais também são altíssimos.

O tema foi abordado de forma simples e sem muita terminologia técnica. No próximo capítulo, apresentar-se-ão as conclusões.

[61] Disponível em: <http://www.elsalvador.com/articulo/tendencias/que-hacer-despues-ataque-cibernetico-76135>. Acesso em: 01 julhos 2016.

5 CONCLUSÃO

Neste trabalho foi possível verificar as particularidades do espaço cibernético como um novo cenário onde acontece a Guerra Cibernética, a qual representa um instrumento de poder que não substitui a força física, mas a complementa, conseguindo ser trabalhada de forma isolada ou combinada com outras dimensões do conflito (terra, mar, ar e espaço). Entende-se que a Guerra Cibernética é possível por causa das vulnerabilidades existentes na Internet, o *hardware, software* e a introdução de sistemas críticos *on-line* presentes cada vez mais no ciberespaço. Estas vulnerabilidades encontradas nestes três elementos são aproveitadas pelos *hackers* e guerreiros cibernéticos para realizar os ataques. Outro ponto relevante, é que da mesma forma que uma guerra convencional, a guerra cibernética requer o conhecimento da sua composição, força, recursos, ambiente e forma de ação ofensiva (ciberataque), defensiva (ciberdefesa) e exploração (ciberexploração).

Conclui-se que na Estônia 2007, onde foi realizado um ataque DDoS em todos os sistemas de informação e comunicação conectados ao ciberespaço, os sistemas financeiros (os Bancos), o comércio eletrônico e as telecomunicações foram atacadas pelos guerreiros cibernéticos, tudo em razão da vingança, a retirada de uma estátua (soldado gigante de bronze) de grande valor nacional para os Russos. Na Geórgia, ao igual que na Estônia foi lançado um ataque DDoS aos sistemas de comunicações derrubando os seus serviços e deixando sem comunicações os Georgianos, a diferença da Estônia que se tratava de uma vingança subversiva da Rússia. Finalmente em 2010, o Irã sofreu um poderoso ataque cibernético que afetou os computadores da central nuclear de Bushehr, supõe-se que a técnica utilizada para inserção do código malicioso produzido em laboratório do nome *Stuxnet* nos computadores com Windows, sistemas SCADA, por meio de um dispositivo de mídia removível (*pen-drive*) trazido por um dos funcionários internos.

Observou-se que a Guerra Cibernética tem sido classificada como nova modalidade de guerra dos novos tempos, tornando-se em uma ameaça que prejudica a segurança de uma Nação. Neste aspecto, preventivamente, surge a necessidade de criar organizações alinhadas às políticas de Segurança da Nação, com a missão de estabelecer o controle de seu espaço cibernético, direcionado para a função estratégica, a segurança das infraestruturas críticas de um país no âmbito da Energia, Defesa, Transporte, Telecomunicações, Finanças e até a própria informação. Verifica-se que o recurso humano da área de pesquisa, desenvolvimento e inovação, é fundamental nesta área, conseguindo desta forma a atualização e a inovação das novas tecnologias. O fator econômico desempenha um papel importante, porque ser ofensivo é de fácil acesso e de baixo custo, muitas técnicas e ferramentas estão disponíveis na *web*, a diferença da defesa que requer uma preparação técnica especializada do recurso humano (guerreiro cibernético) aliado ao alto custo de investimento em aquisição de sistemas de segurança (*hardware, software* e redes), os quais são muito caros.

Outra recomendação preventiva, seria a aplicação de ferramentas da autoavaliação e da análise de nossa segurança cibernética com a finalidade de descobrir as ameaças e as vulnerabilidades para serem corrigidas antes de um terceiro ataque. Essas ferramentas são muito utilizadas pelas empresas voltadas para a área de segurança da informação, as quais são ofensivas na sua maioria e medem os níveis de resistência diante um ataque. Entre as ferramentas conhecidas se encontram: os diagnósticos de segurança, o ataque DdoS, os testes de invasão em redes e os testes de invasão de infraestruturas críticas.

Abordando o tema da investigação no tempo presente, quando somos atacados, as experiências dos especialistas em Segurança da Informação como Richard Clarke e das empresas de antivírus como a Northon sugerem que não se deve entrar em pânico porque a segurança falhou e se acontecer o ataque deve ser realizado um corte da atividade inimiga, isolando-o da Internet, negando-lhe a saída para o espaço cibernético e neutralizando desta

forma o ataque. Posteriormente, deve ser procurado o inimigo dentro da plataforma TICs, em todas as áreas do *hardware*, *software* e redes, e logo reparar o dano causado, restabelecer os sistemas e o banco de dados que foram atingidos pelo ataque. Recomenda-se reinstalar novamente tudo por meio de uma cópia de segurança atualizada, porque esses ataques são usados ferramentas (programas maliciosos) que podem ficar na plataforma de forma passiva sem ser descobertos pelo sistema de detecção de ameaças como os *botnets*, os quais serão ativados uma vez feita a conexão com ciberespaço e provoque a repetição do ataque.

Compreende-se que, após o ocorrido, a melhor prática é a realização de uma investigação pericial informática para determinar o motivo pelo qual ocorreu, assim como, quais foram as vulnerabilidades exploradas pelo atacante, a falha da segurança. Da mesma forma que acontece quando um crime é cometido e os investigadores analisam as evidências para elucidá-lo. Em um ataque cibernético também existem evidências que determinam como aconteceu o ataque, quais as vulnerabilidades foram aproveitadas, quais danos foram ocasionados e até onde pode ter chegado o ataque por meio de um vestígio ou pista deixada por ele, essa é a parte mais difícil de todas mas não impossível porque teve motivação por meio das vulnerabilidades do espaço cibernético mencionadas no capítulo dois, principalmente, a Internet, o que a torna complexa demais e demanda um tempo maior para conseguir chegar até o atacante. Concluído o trabalho de investigação pericial e esclarecido o fato, determinam-se as responsabilidades perante as instituições judiciais nacional ou internacional, conforme o caso.

Finalmente este estudo, deixa uma interrogação para ser respondida em futuras investigações derivadas da Guerra Cibernética, tais como: a criação de sistemas redundantes para reforçar a segurança frente a um ataque cibernético, a criação de um laboratório de Guerra Cibernética na EGN, para conhecimento dos alunos do curso C-EMOS, e a Segurança Ofensiva como melhor pratica contra a guerra cibernética (veja anexo).

REFERÊNCIAS

ANDRADE J. *Camada de aplicação.* SENAI. Curso técnico de redes dos computadores. Brasil. Disponível em: <http://docplayer.com.br/752569-Curso-tecnico-de-redes-de-computadores-disciplina-de-fundamentos-de-rede.html>. Acesso em: 27 junho 2016.

APR. *La máquina virtual Java (JVM o Java Virtual Machine). Compilador e intérprete. Bytecode. (CU00611B).* Disponível em: <http://aprenderaprogramar.com/index.php?option=com_content&view=article&id=392:la-maquina-virtual-java-jvm-o-java-virtual-machine-compilador-e-interprete-bytecode-cu00611b&catid=68:curso-aprender-programacion-java-desde-cero&Itemid=188>. Acesso em: 10 agostos 2016.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT), Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação. Brasil, 2005. Disponível em: <http://www.ciencianasnuvens.com.br/site/wp-content/uploads/2014/09/215545813-ABNT-NBR-177991.pdf>. Acesso em: 23 julho 2016.

BRASIL. Livro Verde: Segurança Cibernética no Brasil/Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia e Rafael Mandarino Junior – Brasília: GSIPR/SE/DSIC, 2010b. Disponível em:<http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf>. Acesso em 02 jun. 2016.

BRASIL. Ministério da Defesa. *MD30-M-01*, Doutrina de Operações Conjuntas. 1 vol. Brasília, 2011.

BRASIL. Ministério da Defesa. *MD35-G-01:* Glossário das Forças Armadas. 5. ed. Brasília. 2015. 292 p.

BUENO Antonio. *Redes de Computadoras. Transmisión de datos.* Unidad didáctica. Disponível em: <http://www.portaleso.com/usuarios/Toni/web_redes/unidad_redes_informaticas_indice.html>. Acesso em: 26 junho 20016.

CANALTECH. *O que é defacement ou deface?* SP. BRASIL, 2016. Disponível em: <http://canaltech.com.br/o-que-e/o-que-e/O-que-e-defacement-ou-deface/>. Acesso em: 11 de agostos 2016.

CARREIRO Marcelo. *A Guerra Cibernética: Cyberwarfare e a Securitização da Internet*. Dossiê Guerras, Conflitos e tenções, 2013. 137 p. Disponível em: http://www.historia.uff.br/cantareira/v3/wp-content/uploads/2013/05/e17a9.pdf Acesso em: 26 junho 2016.

CHINA. *Ejército de Liberación Popular* (PLA). China. Disponível em: <http://www.eurasia1945.com/protagonistas/ejercitos/ejercito-de-liberacion-popular/>. Acesso em: 26 julho 2016.

CLARKE, Richard A.; KNAKE, Robert K. *Guerra Cibernética: A próxima ameaça a segurança o que fazer a respeito*. Rio de Janeiro: Brasport, 2015. 241 p

CLARKE Richard. *Entrevista sobre Guerra Cibernética: en la creciente amenaza ciberguerra.* NPR. abril 2010. Disponível em: http://www.npr.org/templates/story/story.php?storyId=126097038. Acesso em: 26 junho 2016.

DA CRUZ Samuel. *Tecnologias e riscos: Armas Cibernéticas*. Instituto de pesquisa econômica aplicada (IPEA). Brasília julho 2013. 13 p. Disponível em: <http://repositorio.ipea.gov.br/bitstream/11058/5813/1/NT_n11_Tecnologias-riscos_Diset_2013-jul.pdf>. Acesso em: 10 julho 2016.

DANG S. T. *The Prevention of Cyberterrorism and Cyberwar*. Issue one for the GA First Committee: Disarmament and International Security (DISEC). Vietnam: Old Dominion University, 2011. Disponível em: https://www.odu.edu/content/dam/odu/offices/mun/2011/disec/issue-brief-2011-the-prevention-of-cyberterrorism-and-cyberwar.pdf. Acesso em: 27 junho 2016.

ESET. Revista Digital elsalvador. *Que hacer después de un ataque cibernético*. Abr. 2015. Disponível em: <http://www.elsalvador.com/articulo/tendencias/que-hacer-despues-ataque-cibernetico-76135>. Acesso em: 01 julho 2016.

ESET. *Empresa de Antivirus*. NOD32 Eslováquia. Disponível em: <http://www.eset-la.com/compania.> Acesso em: 10 junho 2016.

ESPANHA. Departamento de Seguridad Nacional. *Estratégia de Ciberseguridad Nacional*. España. 2013. Disponível em: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ES_NCSS.pdf>. Acesso em: 28 junho 2016.

ESPANHA. *Departamento de Seguridad Nacional.* DSN. Disponível em: http://www.dsn.gob.es/es/sistema-seguridad-nacional/consejo-seguridad-nacional. Acesso em: 26 julho 2016.

EUA, *Joint terminology for cyberspace operations*, Joint Chiefs of Staff, Department of Defense, USA, 2010. Disponível em: <http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf>. Acesso em: 20 de maio de 2016.

EUA. US Army Training and Doctrine Command Deputy Chief of Staff for Intelligence. Handbook No. 1.02, *Critical Infrastructure Threats and Terrorism*. EUA, 2006. Disponível em: <http://fas.org/irp/threat/terrorism/sup2.pdf>. Acesso em: 11 junho de 2016.

INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS (IEEE). General Gutiérrez Mellado. *Ciberseguridad, retos y amenazas a la seguridad Nacional en el Ciberespacio.* España febrero 2011. Disponível em: < http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf>. Acesso em: 07 junho 2016

LAKATOS, E. M.; MARCONI, M. A. *Fundamentos da Metodologia Científica*. 3 ed. São Paulo: Atlas, 1991. 214 p.

LOPEZ Miguel. *Análisis Forense Digital.* Hackers & Seguridad. 2da Edición junho 2007. 40 P. Disponível em: <http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf>. Acesso em: 07 junho 2016

MANDARINO Raphael. *Um estudo sobre a Segurança e a defesa do espaço cibernético*. Monografia de especialização. Universidade de Brasília – UNB. Instituto de Ciências Exatas. Brasília. Junho, 2009. Disponível em: <http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/raphael_mandarino.pdf >. Acesso em: 15 junho 2016.

MASTERMAGAZINE. *Paquete de datos*. Disponível em: <http://www.mastermagazine.info/termino/6223.php>. Acesso em: 27 junho 2016.

MICROSOFT. *O modelo, TCP/IP*. EUA. 2016. Disponível em: <https://msdn.microsoft.com/es-es/library/cc786900(v=ws.10).aspx>. Acesso em: 26 julho 2016.

ORACLE. *Control de transferencias de paquetes con el comando snoop.* Administración de Oracle Solaris: sevicio IP. EUA, 2016. Disponível em: <https://docs.oracle.com/cd/E26921_01/html/E25871/gexkw.html>. Acesso em: 09 agostos 2016.

PEPELNJAK Ivan. *BGP troubleshooting: Options that make the internet work*. Telecom Routing and Switching. EUA. 2016. Disponível em: <http://searchtelecom.techtarget.com/feature/BGP-essentials-The-protocol-that-makes-the-Internet-work>. Acesso em: 27 de julho 2016.

PINHEIRO Fábio. *A cibernética como arma de combate*. ESG. RJ, Brasil 2013. 50 p. Disponível em: <http://www.esg.br/images/Monografias/2013/PINHEIRO.pdf>. Acesso em: 07 agosto 2016.

PRANDINI Patricia, PALLERO Marcela. *Vulnerabilidades, amenazas y riesgo en "texto claro"*. Magazcitum. 25 de mayo 2013. Disponível em: <http://www.magazcitum.com.mx/?p=2193#.V5Qwe_krLIV>. Acesso em: 24 julho 2016.

ROCATEK. Serviços de Informações da Tecnologia do Sistema SCADA. Disponível em: <http://www.rocatek.com/sistema_supervision.php>. Acesso em: 10 agosto 2016.

ROMERO Tori, KIRNER Claudio e SISCOUTTO Robson. *Fundamentos e Tecnologia de Realidade Virtual e Aumentada*. Belém. PA. 2006. Brasil. 399 p. Disponível em: <http://www.ckirner.com/download/capitulos/Fundamentos_e_Tecnologia_de_Realidade_Virtual_e_Aumentada-v22-11-06.pdf>. Acesso em: 08 agostos 2016.

SAWAYA Márcia. *Dicionário de Informática & Internet, Inglês/Português*. Centro Estadual de Educação Tecnológica Paula Souza (CEETEPS). Nobel. SP, Brasil, 1999. 545 p. Disponível em: <http://comp.ist.utl.pt/aaa/Prog/Dicion%E1rio%20De%20Inform%E1tica%20&%20Internet%20Ingl%EAs-Portugu%EAs.pdf>. Acesso em: 10 agostos 2016.

SYMANTEC. *Dossiê W32 Stuxnet.* EUA, 2011. Disponível em: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf Acesso em: 29 julho 2016.

.SYMANTEC. *Glossário*. EUA. 2016. Disponível em: <https://www.symantec.com/pt/br/theme.jsp?themeid=glossario-de-seguranca>. Acesso em 24 julho 2016.

SYMANTEC. *Qué debe hacer si resulta víctima de los ataques*. EUA. 2016. Disponível em: <http://mx.norton.com/cybercrime-victim>. Acesso em: 28 junho 2016.

UE. *La Agencia Europea de Redes y Seguridad de la Información*. ENISA.UE. Disponível em:<https://www.enisa.europa.eu/about-enisa> Acesso em: 26 julho 2016.

UNIVERSIDAD AUTÓNOMA DE TAMAULIPAS (UAT). *Glosario. Unidad Académica Multidisciplinaria Mante*. México 2015. Disponível em: <http://uammante.uat.edu.mx/cisco/Curricula/CCNASem3/CHAPID=null/RLOID=null/RIOID=1083952940359/knet/1080604003687/entryframeset.html>. Acesso em: 27 julho 2016.

UNO. *Wegene Henning*. Revista UNO. Llorente & Cuenta, SP. Brasil 2016. Disponível em: <http://www.revista-uno.com.br/staff/henning-wegener/>. Acesso em: 07 agostos 2016.

WEGENER Henning. *La guerra cibernética.* Política exterior. 2001. 17 p. Disponível em: <https://www.unibw.de/infosecur/publications/individual_publications/wegener_la_guerra_cibernetica_article_2001>. Acesso em 24 julho 2016.

WIENER, R., ROSENBLUETH, A. & BIGELOW, J. *Behavior, Purpose and teleology*. U.S. Philosophy of Science, Volume 10, Issue, 1943. 18-24p. Disponível em: <http://courses.media.mit.edu/2004spring/mas966/rosenblueth_1943.pdf>. Acesso em: 13 junho 2016.

WIRED. *An Unprecedented look at Stuxnet, the World's First Digital Weapon*. by Kim Zetter. Published by Crown Publishers, an imprint of Random House LLC. 2014. Disponível em: <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>. Acesso em: 27 junho 2016.

ANEXO

POSFÁCIO DA EDIÇÃO BRASILEIRA

Segurança Ofensiva: Um Aliado no Caminho para a Defesa Cibernética

Resumo

Métodos tradicionais para a elaboração de diagnósticos de segurança são fortemente orientados aos aspectos de gestão da segurança de informação. No presente artigo, apresentamos uma moderna abordagem para a avaliação do status de segurança de organizações, à qual nos referimos como “segurança ofensiva”. Durante a execução de um diagnóstico baseado em segurança ofensiva, o analista de segurança assume o ponto de vista de potenciais atacantes, buscando identificar vulnerabilidades que possam, de fato, ser exploradas, comprometendo a segurança e impactando os negócios da organização sob avaliação. Trata-se de uma abordagem orientada aos aspectos tecnológicos da infraestrutura **e aos ativos** de segurança da organização sob avaliação, permitindo obter um diagnóstico muito mais concreto a respeito dos riscos aos quais a organização está submetida, complementando, dessa forma, os diagnósticos oferecidos por ferramentas mais tradicionais, como as auditorias de segurança.

Introdução

Enquanto a solução clássica de segurança da informação tem foco em aspectos de alto nível, como a estrutura de gestão e processos corporativos, organizações com elevada dependência em relação à Internet buscam diagnósticos que forneçam respostas concretas sobre suas condições de segurança.

Nos dias de hoje não é necessário iniciar um texto sobre segurança da Informação argumentando sobre a sua importância. Todos nós sabemos que um grande volume de dados é manipulado, a cada segundo, por complexos sistemas de informação, e que esses dados carregam valor – seja este valor expresso em grandezas concretas, como unidades monetárias, ou abstratas, como “confiança” e “reputação”. Todos temos a percepção de que a indisponibilidade de um sistema e o comprometimento da integridade ou da confidencialidade de informações sensíveis podem representar uma elevada perda financeira, consequência da interrupção de processos corporativos, e que o vazamento de informações pode levar a danos irreversíveis a imagem de uma empresa e até mesmo a complicadas ações judiciais.

A questão hoje não é decidir entre investir e não investir em segurança, mas quanto investir e, principalmente, como investir.

Diagnósticos de Segurança

Diagnósticos de Segurança tem por objetivo identificar o nível de maturidade de segurança de uma organização. Uma empresa que busque a evolução em Segurança da Informação deve, no mínimo, compreender o ponto em que se encontra e dispor de mecanismos que permitam quantificar a sua segurança. Bons diagnostico de segurança vem acompanhados por recomendações e orientações sobre como sanar as falhas identificadas, **e por sugestões de melhorias em políticas, normas, processos e procedimentos.**

A opção tradicional de empresas interessadas em Diagnósticos de Segurança são as chamadas Auditorias de Segurança. São mecanismos de avaliação fundamentados na análise documental e na execução de atividades “passivas” e “pouco intrusivas”, tais como entrevistas a funcionários; o foco é fortemente orientado a aspectos de gestão e processos. A execução periódica de auditorias de segurança, indubitavelmente, traz benefícios à organização, na

medida em que permite a implantação de uma infraestrutura de apoio à segurança e a eliminação de práticas inseguras dos processos corporativos – as consequências são claramente positivas para a manutenção de um status de segurança no longo prazo.

Auditorias "clássicas" como as descritas anteriormente, no entanto, no entanto, não costumam estender seu escopo de atuação até o nível técnico – ou, pelo menos, não o fazem de maneira sistemática. Dificilmente o contratante de uma Auditoria de Segurança nos moldes da ISO27001 ficará sabendo, ao final de uma auditoria, que seu webserver possui uma vulnerabilidade que permite a execução de um ataque de negação de serviço que poderia deixar o site da empresa fora do ar, ou que sua aplicação de e-commerce é vulnerável a um ataque do tipo SQL Injection, que poderia levar ao vazamento de informações sensíveis sobre clientes. Para infraestruturas altamente dependentes de sistema de informação, como é o caso de grande parte das atuais infraestruturas críticas, esse tipo de conhecimento "concreto" a respeito de segurança é essencial.

Testes de Invasão

Nos últimos tempos, vem se consolidando uma nova forma de executar Diagnósticos de Segurança. Tal conjunto de técnicas e metodologias consagrou-se sob o nome Testes de Invasão, denominação decorrente de seu forte "orientação a ataques", ou seja, a reprodução de cenários de ataques aos quais os sistemas e ativos sob avalição podem vir a ser submetidos.

Em um Diagnóstico de Segurança do tipo Teste de Invasão, o avaliador é denominado *pentester* (do inglês *penetration tester*). O trabalho do *pentester* é usar de todas as ferramentas e **técnicas** que estejam disponíveis a usuários maliciosos com o objetivo de simular ataques aos sistemas sob avaliação. No entanto, a atuação do *pentester* começa muitos antes do *gran finale* representado pela execução dos ataques.

As fases de um teste de invasão

Um Teste de Invasão "profissional" começara com atividades muito menos emocionantes do que aquelas associada á imagem de um *pentester*, atrás de um computador, embrenhando-se coração dos sistemas de uma organização. Uma série de atividades "burocráticas" são necessárias antes antes do início do Teste de Invasao propriamente dito-e essas atividades são fundamentais para garantir o perfeito entendimento entre o cliente e o provedor do Teste de Invasão. Entre os aspectos que serão definidos nesta etapa, destacamos os seguintes:

- **Objetivos e escopo.** Quais sistemas serão testados e contra que classes de ataques?
- **Janelas de execução e efeitos colaterais aceitáveis.** Há restrições de horário para a execução dos testes? Há sistemas para os quais a possibilidades de determinados tipo de dano – por exemplo, indisponibilidade – é inaceitável?
- **Prazo.** Que o tempo de execução desejado pelo cliente e qual o prazo exequível pelo fornecedor do Teste de Invasão?

Um fornecedor de Testes de Invasão profissional usará as informações mencionadas para estimar o tamanho do projeto e a equipe necessária, que, por sua vez, definirão os custos do projeto e o valor do investimento para o contratante.

O trabalho técnico envolve as atividades de reconhecimento, mapeamento e ataque. A atividade de reconhecimento tem por objetivo levantar informações preliminares a respeito da organização sob avaliação. Tais informações são obtidas em repositórios públicos de informações, disponíveis a partir da Internet – e é impressionante a quantidade de informações sensíveis a respeito de sua empresa que podem ser facilmente obtidas no Internet com o uso das ferramentas certas! As atividades de mapeamento já envolvem uma interação direta com o sistema da organização e buscam caracterizar a topologia das redes, a organização dos sistemas e as vulnerabilidades ali presentes. Uma vez dispondo de

informações suficientes sobre as redes e sistemas sob avaliação, o *pentester* parte para a execução de simulações de ataque, sempre levando em conta o impacto potencial e regras de danos aceitáveis acordadas com o cliente.

Uma vez concluídas as atividades “técnicas”, é hora de elaborar o relatório onde se apresentarão os resultados do Teste de Invasão. Um bom relatório deve mostrar as “conclusões do teste” em diversos níveis de abstração. De fato, é prática dividir o relatório em várias partes, algumas delas orientada á alta administração e apresentando resultados em alto nível – por exemplo, explicando os impactos de um ataque aos processos críticos do negócio – e outras orientadas aos profissionais técnicos, detalhando as vulnerabilidades encontradas, **como foram identificadas e exploradas**, e como saná-las.

Ataques DDoS: A Questão da Indisponibilidade

A disponibilidade é um fator para os atuais sistemas de informação. Vivemos em um mundo onde a dependência de usuários em relação aos sistemas computacionais é enorme, e a indisponibilidade desses sistemas, ainda que temporária, causa prejuízos enormes a clientes e responsáveis pelo serviço. Os chamados “ataques de negação de serviço” são exatamente aqueles que visam indisponibilizar um sistema de informação, que deixa de oferecer o serviço para o qual foi concebido – ou, ainda, passa a oferece – lo de maneira precária. A partir do final da década de 1990 percebeu – se que a indisponibilidades de sistemas poderia ser forcada a partir da sobrecarga de requisições causada pela atuação coordenada de um grande número de maquinas executando solicitações rotineiras a um sistema de informação. Devido á ação de diversas unidades computacionais atuando como um sistema disbruído, tais ataques passaram a ser denominados Ataques Distribuídos de Negação de Serviço, ou ataques DDoS (do inglês Distributed Denial of Service). Por serem baseadas não apenas em falhas de software, mas no uso massivo dos recursos de um sistema – alvo, esses ataques estão entre

aqueles de mais difícil prevenção, detecção e reposta. Ataques DDoS vem se consolidando com uma das armas mais letais contra sistemas computacionais.

O cenário mudou com o aumento da dependência de organizações e infraestruturas críticas em relação a sistema de informação e á Internet. A indisponibilidade de sistemas Internet pode representar, na prática, a interrupção de serviços essenciais, comprometendo o equilíbrio da sociedade e, inclusive, colocando vidas em risco.

Mais uma vez, a resposta para uma empresa que quer compreender a seu grau de vulnerabilidade é a segurança ofensiva. Felizmente, empresas líderes no ramo de Teste de Invasão dispõem de ferramentas, técnicas e metologias que permitem simular os mais diversos tipos de ataques DDsS, caracterizando a resiliência de sistemas face a esses ataques. Em geral, um estudo de vulnerabilidade a ataques DDoS poder ser contratado como parte de um Teste de Invasão, ou como um serviço avulso. E, como sempre, bons fornecedores desse serviço orientarão quanto á solução dos problemas identificados.

Testes Invasão e Infraestruturas Criticas

Atualmente, vemos uma crescente dependência das chamadas “infraestruturas críticas” em relação aos sistemas de informação. Trata – se de um mundo praticamente invisível ao cidadão, mas que sustenta a produção da indústria, a distribuição da energia, o funcionamento de sistemas de transportes e de comunicações ... e que enfatizar o impacto que acesso indevido a um desses “computadores” pode gerar: eles controlam o núcleo de infraestruturas fundamentais para o funcionamento da sociedade, e seu mau funcionamento pode, em último caso, gerar um colapso com impactos de grandes proporções, incluindo danos físicos a equipamentos, construções e até mesmo pessoas.

Ocorre que a cultura da segurança da informação ainda não é amplamente difundida na maioria das industrias responsáveis por essas infraestruturas críticas. O leitor deve imaginar:

se vemos, com frequência, notícias sobre empresas de tecnologia de outras áreas da engenharia desenvolvam seus produtos sem ter em mente a possibilidade de ataques maliciosos. Mesmo quando se tem alguma preocupação com segurança, o que se observa é um foco muito grande na manutenção dos Sistemas de Gestão de Segurança da Informação. No em tanto, questões concretas como "o que acontece se um hacker tiver acesso aos sistemas de controle de temperatura de meu ambiente de produção – e será que isso é possível? Dificilmente são consideradas.

A confiança nas organizações que mantêm infraestruturas críticas passa, sim, pela manutenção de técnicas de segurança ofensiva parece ser a única maneira de prevenir ataques concretos contra tais infraestruturas.

Segurança Ofensiva

O cenário é complicado: sistemas cada vez mais complexos e dos quais dependemos cada vez mais, ao mesmo tempo em que proliferam ferramentas que possibilitam ataques cada vez mais sofisticados, mesmo quando conduzidos por usuários que não possuem elevado conhecimento técnico. Como consequência, um bom Diagnóstico de Segurança, nos dias de hoje, precisa apresentar dados concretos a respeito dos sistemas avaliados, ou seja, quais são as vulnerabilidades presentes, quais são os ataques factíveis, quais são os impactos possíveis. Os chamados Testes de Invasão a ferramenta que mais se adequa a essa nova visão de "segurança ofensiva", na qual o analista de segurança se coloca na posição do atacante e, somente aí, é capaz de visualizar com precisão quais os danos que é capaz de imprimir a um sistema e a uma organização.

Para saber mais sobre Teste de Invasão e o conceito de "segurança ofensiva", sugerimos uma visita ao site da Clavis (http://www.clavis.com.br) e ao Portal Seginfo

(http:/www.seginfo.com.br), **que trata somente de assuntos ligados á área de segurança da informação.**

Fonte: CLARKE, Richard A.; KNAKE, Robert K. Guerra Cibernética: *A próxima ameaça a segurança o que fazer a respeito*. Rio de Janeiro: Brasport, 2015. 241 p.