ESCOLA DE GUERRA NAVAL

CC LEONARDO DE OLIVEIRA SODRÉ

# A SEGURANÇA CIBERNÉTICA E O DESAFIO DA CONTENÇÃO DOS ATAQUES

Rio de Janeiro

2017

CC LEONARDO DE OLIVEIRA SODRÉ

# A SEGURANÇA CIBERNÉTICA E O DESAFIO DA CONTENÇÃO DOS ATAQUES

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

Orientador: CF EUGENIO HUGUENIN

Rio de Janeiro
Escola de Guerra Naval
2017

## AGRADECIMENTOS

Ao término deste trabalho não posso deixar de expressar meus sinceros agradecimentos à minha amada esposa Melanie, que soube compreender e apoiar em todos os momentos por ocasião das pesquisas para realização dessa etapa, bem como a meus pais Antônio e Edna, pelo apoio incondicional e compreensão nos momentos de ausência.

Ao CF Eugenio Hugenin, agradeço pelas orientações e conhecimentos transmitidos no decorrer da elaboração desse trabalho, que muito contribuíram para o meu desenvolvimento profissional.

## RESUMO

O objetivo do presente trabalho é apresentar conceitos relacionados à Segurança Cibernética, demonstrar sua crescente importância, analisar os fatores que representam um desafio para a contenção dos ataques cibernéticos, avaliando quais possuem maior influência para o sucesso das ações no ambiente virtual. No presente trabalho utilizou-se o método dedutivo e um tipo de pesquisa exploratória com características bibliográfica e documental. Foram abordados os principais conceitos relacionados ao novo campo de batalha, o da Guerra Cibernética. Apontou-se a característica e a estrutura do Espaço Cibernético, que com a ampliação da Internet tornou-se interconectado, passando a fazer parte da vida da maioria das pessoas. Apresentou-se os principais atores que fazem parte dessa nova dimensão de conflito, bem como seus recursos de ataque e defesa. Avaliou-se as vulnerabilidades presentes no ambiente virtual, algumas ameaças que estão cada vez mais presentes no cotidiano das pessoas em decorrência do avanço tecnológico, a dependência cada vez maior dessas tecnologias, bem como fatores relacionados à responsabilidade pelo sucesso das ações, sejam elas referentes à ataque ou à defesa. Por fim, conclui-se que priorizar a Segurança Cibernética é essencial nesse novo ambiente de conflito e que o sucesso das ações de defesa realizadas no espaço cibernético dependerão, não somente dessas ações serem melhores que as do atacante, mas também de não permitir que o atacante explore suas vulnerabilidades.



Palavras-chave: Guerra Cibernética. Espaço Cibernético. Segurança Cibernética. Ataque cibernético. Internet.

## LISTA DE ILUSTRAÇÕES

## LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| BGP | *Border Gateway Protocol* |
| C2 | Comando e Controle |
| CERT.BR | Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil |
| DDOS | *Distributed Denial of Service* |
| DNS | *Domain Name Servers* |
| DoD | Departamento de Defesa *(Departament of Defense)* |
| EUA | Estados Unidos da América |
| IoT | Internet das Coisas *(Internet of Things)* |
| IP | Protocolo de Internet *(Internet Protocol)* |
| ISP | Provedor de Serviço de Internet *(Internet Service Provider)* |
| ITSR | *Internet Threat Secure Report* |
| MD | Ministério da Defesa |
| NSA | Agência de Segurança Nacional dos EUA (*National Security Agency)* |
| PC | Computador Pessoal (Personal Computer) |
| RAT | Trojan de Acesso Remoto *(Remote Acess Trojan)* |
| SSR | Resposta de Segurança da Symantec *(Symantec Security Response)* |
| STIC3 | Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle |
| USCYBERCOM | Comando de Defesa Cibernética dos Estados Unidos da América *(United States Cyber Command)* |

**SUMÁRIO**

# 1 INTRODUÇÃO

Desde a disponibilização da Internet a partir de 1974 para todos os usuários ao redor do mundo, o acesso à informação e a informatização dos sistemas têm atingido níveis nunca antes imaginados. A década de 90 representou o marco dessa evolução que nunca mais parou e que continua, ano após ano, em uma exponencial crescente.

Tais avanços tecnológicos trouxeram inúmeras facilidades para toda a sociedade mundial. A Internet interligando usuários por meio de seus computadores pessoais (PC), servidores de grandes empresas e militares ligados na grande rede, telefones inteligentes que permitem as pessoas manterem-se conectadas praticamente 24 horas por dia, redes sociais que expõem de maneira voluntária a privacidade de cada um e os diversos aplicativos que disponibilizam sua localização instantaneamente, tornaram o planeta Terra uma pequena aldeia global interconectada e sem barreiras.

Ao mesmo tempo que trouxeram grandes facilidades para o nosso dia a dia, toda essa modernidade e tecnologia abriram caminho para um novo tipo de guerra, a Guerra Cibernética. Nessa nova modalidade de conflito as partes conflitantes buscam as fragilidades e vulnerabilidades nos diversos sistemas dos oponentes, no ambiente virtual interconectado, para obter acesso a documentos, planos, projetos, realizar sabotagem e praticar delitos utilizando-se do anonimato, mesmo que temporário, por meio da conectividade oferecida para Internet.

A Guerra Cibernética é, sem dúvida, um dos maiores desafios de um novo domínio no teatro de operações, o Espaço Cibernético. Dessa forma, no capítulo 2 serão abordados os principais conceitos na Guerra Cibernética de acordo com as normas emitidas pelo Ministério da Defesa. Na sequência, no capítulo 3 serão apresentadas as principais ameaças que compõem esse novo campo de batalha e no capítulo 4 serão expostos os principais recursos inerentes à Segurança Cibernética, que podem ser utilizados para a defesa

dos sistemas de interesse interligados pela Internet. No capítulo 5, por sua vez, serão analisados os efeitos de um ataque por um código malicioso que atingiu uma escala global e, por fim, o último capítulo apresentará a conclusão.

O presente trabalho procura analisar os aspectos dessa nova modalidade de guerra, quais fatores representam maior probabilidade de sucesso no desenvolvimento das ações, a importância da segurança cibernética na contenção dos ataques no espaço cibernético, e responder ao seguinte questionamento: quem é o responsável por esse sucesso das ações no espaço cibernético, o atacante bem preparado ou o defensor que deixa de adotar as medidas necessárias, para evitar o ataque realizado seja bem-sucedido?

# 2 UM NOVO CAMPO DE BATALHA

Nos dias atuais, há um consenso de que a Internet modificou a maneira como o mundo interage, realiza negócios e compartilha a informação. A Internet, ao mesmo tempo que funciona como um mecanismo de inovação, apresenta ameaças cibernéticas que se modificam mais rapidamente do que a reação das defesas.

As ameaças cibernéticas são complexas, dinâmicas e dificultam cada vez mais a elaboração de respostas eficazes, devido à interconectividade da rede.

Esse novo tipo de ameaça e sua maneira de atuação, bem como seu alcance, nos trazem a um novo campo de batalha.

## 2.1 PRINCIPAIS CONCEITOS DA GUERRA CIBERNÉTICA

Nesse novo campo de batalha é importante conhecermos os principais conceitos adotados. Tendo como referência as publicações normativas do Ministério da Defesa (MD), destacamos os seguintes conceitos definidos de acordo com a Doutrina Militar de Defesa Cibernética[1]: Guerra Cibernética, Defesa Cibernética, Espaço Cibernético, Ameaça Cibernética, Infraestrutura Crítica de Informação e Infraestruturas Críticas.

A Guerra Cibernética[2] (GCiber) empregará em uma Operação Militar ações que envolvem ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC3) do oponente e garantir a defesa do nosso STIC3. Dessa maneira, passa a ser notório o quanto a GCiber caminha em paralelo com a guerra convencional.

A Defesa Cibernética[3] (DCiber) possui como propósito a proteção dos sistemas de

1 BRASIL, Ministério da Defesa. MD31-M-07, **Doutrina Militar de Defesa Cibernética**, Brasília, DF, 2014.

2 Guerra Cibernética – corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir as capacidades de Comando e Controle (C2) do adversário, no contexto de um planejamento militar (BRASIL, 2014).

3 Defesa Cibernética – conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço

informação de interesse da Defesa Nacional, o comprometimento dos sistemas de informação do oponente e a obtenção de dados para a produção de conhecimento de inteligência.

No Espaço Cibernético[4] (ECiber) encontra-se a estrutura global de transferência de informações e comunicações digitais interconectadas, que tornou-se um grande desafio para a segurança de informações digitais de usuários, grandes empresas e governos.

Ainda, segundo o estabelecido na Doutrina Militar de Defesa (BRASIL, 2014) as ações no ECiber estão divididas conforme os seguintes níveis: o Nível Político, o Nível Estratégico, o Nível Operacional, e o Nível Tático. Além disso, de acordo com o relatório da RAND EUROPE[5], pode-se acrescentar dois níveis de atuação no novo campo de batalha: o Nível Social e o Nível Técnico.

Diante do amplo espectro do ECiber encontraremos as Ameaças Cibernéticas (ACiber) que se tornam a causa em potencial de um incidente, que pode resultar em um dano ao Espaço Cibernético de interesse (BRASIL, 2014). A preservação da integridade das informações no ECiber torna-se cada vez mais complexa, visto que não só os setores econômicos e de defesa dos Estados podem ser atacados, uma vez que usuários normais também passaram a ser vítimas das diversas ACiber existentes.

A transformação da Internet de uma rede privada de pesquisa para uma rede de comunicação em massa alterou exponencialmente a equação das ACiber globais. O sistema de TIC globalmente interconectado pode ser explorado por vários usuários mal-intencionados que podem inclusive utilizar as vulnerabilidades encontradas como uma ferramenta para atingir o nível estratégico. Sua exploração pode variar desde crimes individuais como, por exemplo, invasão de servidores para roubo de dados, até planos planejados por Estados de maneira a atingir objetivos estratégicos, como Infraestrutura Críticas da Informação e

Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa (BRASIL, 2014).

[4] Espaço Cibernético – espaço virtual composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas ou armazenadas (BRASIL,2014)

[5] BÉLGICA. RAND EUROPE. **A focus on cybersecurity**. Bruxelas, 2016. Disponível em: < https://www.rand.org/pubs/corporate_pubs/CP871.html>. Acesso em 09 jun. 2017.

Infraestruturas Críticas.

A Infraestrutura Crítica da Informação[6] (ICIn) pode ser compreendida como sendo uma ligação entre os órgãos governamentais e os órgãos do setor privado, de forma a incluir políticas para o incremento da segurança no ECiber.

Por fim, cabe esclarecer que a defesa das Infraestruturas Críticas[7] (IC) é essencial para a manutenção de toda a estrutura do Estado. A interferência de um agente externo, via Internet, aproveitando as vulnerabilidades dos diversos sistemas computacionais presentes na infraestrutura estatal, pode causar o colapso do Estado e a perda de muitas vidas em virtude de eventual interrupção ou destruição de sistemas de controle relacionados a recursos essenciais para toda a sociedade. Como exemplo, pode-se citar o sistema de controle de uma hidrelétrica que, se corrompido, poderia ocasionar o rompimento das comportas e, por conseguinte, gerar alagamento e grandes danos à área adjacente.

## 2.2 PRINCIPAIS CARACTERÍSTICAS

Os conceitos anteriormente apresentados não esgotam os termos relativos a esse novo campo de batalha. A GCiber tornou-se um dos mais sérios desafios para o espectro da segurança nos dias atuais, sendo sua atuação tão abrangente e indeterminada que não se restringe a um Estado, mas compreende também todos os usuários dos sistemas computacionais, valendo-se da interconexão entre redes de computadores estabelecidas pela Internet.

Os recursos tecnológicos empregados no ECiber, bem como seus sistemas cada vez mais complexos, propiciam que grupos de *hackers*[8] encontrem vulnerabilidades e

[6] Infraestrutura Crítica de Informação – subconjunto dos ativos de informação que afeta diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade (BRASIL, 2014).

[7] Infraestruturas Críticas – instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade (BRASIL, 2014.)

[8] *Hacker*: pessoa especializada no uso de computadores, também normalmente aquele que obtém acesso ilegal a sistemas de computadores privados (tradução nossa). Cambridge Dictionary. Disponível em < http://dictionary.cambridge.org/us/dictionary/english/hacker >. Acesso em 13 de jul. de 2017

ataquem todo o aparelhamento de um Estado, suas instituições financeiras, estruturas de energia e transporte, podendo atingir a moral pública e causar danos sem precedentes.

De acordo com o Relatório do *Chatham House*[9] sobre Guerra Cibernética, são apontadas algumas características relacionadas à GCiber dentre as quais pode-se destacar a questão de que os atacantes podem agir quase que anonimamente e com relativa sensação de impunidade, pelo menos por um curto período de tempo, operando por meio de um falso *Internet Protocol* (IP), de um servidor no exterior ou com uso de pseudônimos, e que o ECiber deve ser visto como o "quinto domínio", somado aos domínios tradicionais da terra, ar, mar e espaço. A GCiber é melhor entendida como um novo componente do campo de batalha, porém não pode ser separada do ambiente multifacetado de um conflito.

## 2.3 ATORES NO CAMPO DE BATALHA

A GCiber pode ser um conflito entre Estados, porém pode envolver atores não estatais. Neste tipo de embate é muito difícil de avaliar a precisão e a proporcionalidade da força empregada. Os alvos podem ser tanto militares, industriais ou infraestruturas civis.

Segundo Clarke/Knake[10] os ataques cibernéticos com objetivos militares, interesses políticos e econômicos têm se intensificado nos últimos anos, assim eles abordam os seguintes. Destes ataques podemos extrair os seguintes pontos (CLARKE/KNAKE, 2015): a GCiber deve ser considerada real, pois devido a sofisticação de suas ferramentas de ataque não é possível identificar a capacidade de infligir danos reais a um Estado; ocorre em velocidades muito altas, sendo difícil mensurar o tempo entre o ataque e seu efeito; pode ser considerada global, uma vez que a interconexão entre todos os computadores via Internet permite que um ataque possa atingir servidores espalhados pelo globo; não possui um limite

[9] REINO UNIDO. The Royal Institute of International Affairs. **2010-11-On Cyber Warfare – A Chatham House Report**. Disponível em < https://www.chathamhouse.org/publications/papers/view/109508 >. Acesso em 21 de maio de 2017

[10] CLARKE, Richard A., KNAKE, Robert K., **GUERRA CIBERNÉTICA – A próxima ameaça à segurança e o que fazer a respeito**, Rio de Janeiro, Brasport, 2015.

delimitado no campo de batalha, pois os sistemas são acessíveis a partir do ECiber, podendo em caso de um ataque bem-sucedido rapidamente serem comprometidos; e a GCiber já teve seu início com diversos Estados ao redor do mundo já estão se preparando, invadindo redes e infraestruturas uns dos outros, instalando *backdoors*[11] e bombas-lógicas, e acrescentando uma nova variável no campo de batalha.

Clarke/Knake, define em seu livro esse novo tipo de guerra,

> […] Esse novo tipo de guerra não é um jogo ou uma fábula de nossas imaginações. Longe de ser uma alternativa para a guerra convencional, a guerra cibernética, na verdade, pode até mesmo aumentar a chance de que um combate mais tradicional aconteça, com explosivos, balas e mísseis. Se pudéssemos pôr esse gênio de volta na garrafa, nós colocaríamos, mas não podemos. Na verdade, precisamos nos engajar em uma série de tarefas complexas: entender o que é a guerra cibernética, aprender como e por que ela funciona, analisar seus riscos e se preparar, pensando em como controlá-la. (CLARKE/KNAKE, 2015)

Conclui-se, pelo exposto, que esse novo campo de batalha é complexo, amplo e os ataques podem ser conduzidos de fora do teatro de operações. Atores tradicionais (Estados e Militares), civis e grupos não-estatais se misturam. Observa-se que exércitos e civis são colocados frente a frente, em igualdade.

A complexidade dos sistemas de informação, cada vez mais robustos, também propicia que os mesmos fiquem cada vez mais expostos. A quantidade de informação é tão grande que vulnerabilidades passam desapercebidas e podem ser exploradas ou expostas por algum código malicioso.

## 2.4 A REDE DE COMUNICAÇÕES E A ERA DA INFORMAÇÃO GLOBAL

O mundo de hoje encontra-se entrelaçado por uma rede de comunicação cujo alcance atinge as regiões mais remotas do globo terrestre. Satélites transmitem informações instantâneas de voz, dados e imagens em questão de segundos, não encontrando mais as restrições de tempo e espaço. No mundo conectado, um acontecimento pode ser transmitido

[11] Backdoor – relativo a alguma coisa que pode ser executada secretamente, ou de forma não direta e desonesta (tradução nossa). Cambridge Dictionary. Disponível em < http://dictionary.cambridge.org/us/dictionary/english/backdoor>. Acesso em 13 de jul. de 2017.

instantaneamente através de celulares, canais de televisão ou rádio via satélite, alcançando bilhões de pessoas. O globo tornou-se um lugar pequeno para todas as pessoas e principalmente para a informação, que rapidamente alcança todos os cantos do mundo, independentemente das vontades e do poder.

A dificuldade de identificação do começo de um ataque cibernético alerta para o fato de que pouco conhecemos e de que não compreendemos o poder desse novo vetor assimétrico no campo de batalha. Um *hacker* bem capacitado, sozinho, pode causar um dano muito maior a um Estado do que tropas convencionais em solo inimigo, sem sequer se aproximar desse território.

Observa-se, assim, que o tamanho da rede de comunicação mundial já atingiu um patamar no qual poucas áreas do globo estão excluídas dessa rede. Com os continuados avanços tecnológicos dos equipamentos que permitem o funcionamento dessa grande rede, em pouco tempo não haverá mais áreas esquecidas. A era da informação global já é realidade e não há como retornar, de modo que impedir o acesso à informação sensível torna-se um desafio cada vez mais sofisticado e necessário para garantia da ordem mundial.

## 2.5 ANÁLISE DO CAPÍTULO

Nesse capítulo apresentamos a maneira como o mundo atual foi modificado por meio da Internet, que alterou o modo como as pessoas interagem, realizam negócios e compartilham a informação.

Destacou-se alguns conceitos desse novo campo de batalha contidos na publicação normativa do MD, como: Guerra Cibernética, Defesa Cibernética, Espaço Cibernético, Ameaça Cibernética, Infraestrutura Crítica da Informação e Infraestrutura Crítica.

Apresentou-se os atores presentes no novo campo de batalha, os quais podem

representar um Estado ou um grupo a parte com interesses individuais, militares ou civis, interesses políticos, econômicos e estratégicos. Não há como avaliar as consequências dos ataques e a proporcionalidade da força empregada.

Por fim estabeleceu-se a relação entre a rede de comunicações nos dias atuais que permite que as informações atinjam os locais mais remotos do globo terrestre quase que instantaneamente, tornando a imensa aldeia global um mundo sem fronteiras.

A quantidade cada vez maior de informações nos sistemas permite que suas fragilidades sejam exploradas e que os diversos atores realizem suas ações no ECiber de maneira a atingir seus interesses, de forma anônima, mesmo que por um período curto de tempo.

# 3 AMEAÇAS E DESAFIOS

Como descrito pelo *Chatham House,* o conflito no ECiber possui um caráter tão diversificado quanto os atores que o exploram, como por exemplo a grande quantidade de ações que podem ser realizadas ou os inúmeros alvos que podem ser atacados simultaneamente no ECiber (REINO UNIDO, 2010). O mundo sem limites do ECiber é um campo de atuação propício para guerreiros virtuais que queiram atingir os objetivos estratégicos de um Estado ou ideologia, ou mesmo satisfazerem objetivos pessoais, aproveitando-se do anonimato para cometerem os mais diversos crimes.

À medida que as ameaças do mundo virtual aumentam exponencialmente, em escala e no seu modo de atuação, o ECiber continua desconhecido e pouco compreendido. As diferenças entre os atores e os métodos utilizados tornam essa diversidade característica desse espaço singular. Assim, o emprego de arquivos maliciosos para causar confusão por diversão, a utilização de programas para obtenção de informações individuais e a exploração das vulnerabilidades da Internet para a prática de crimes têm se tornado o grande desafio para os profissionais de segurança no ambiente virtual.

Neste capítulo, busca-se identificar as principais ameaças no mundo cibernético, qual a origem das vulnerabilidades para a segurança do ECiber; quem são os principais atores desse ambiente; e quais são suas intenções e motivações. Por fim, serão apontados os principais desafios encontrados no ambiente virtual relacionados à exploração das vulnerabilidades do ECiber.

## 3.1 AMEAÇAS

Dentre as principais ameaças existentes no ECiber, destacam-se as diversas vulnerabilidades decorrentes do próprio desenho da Internet, da arquitetura característica da rede, da inserção de periféricos nos diversos sistemas via porta USB, e dos próprios usuários

que muitas vezes, em decorrência de suas atitudes, colaboram para que os sistemas sejam acessados por pessoas não autorizadas.

Nesse sentido, Clarke/Knake identifica seis grandes vulnerabilidades da Internet (CLARKE/KNAKE, 2015), que seriam: os Provedores de Serviço de Internet (ISP) empresas responsáveis por conduzir o tráfego pela Internet; o roteamento entre os ISP (*Border Gateway Protocol* – BGP) empregado na distribuição dos pacotes de dados entre origem e destino; a existência ou falta de governança, pois não há um administrador para a grande rede e um computador não possui a capacidade de reconhecer ambiguidades como, por exemplo, duas máquinas utilizando o mesmo IP; a ausência de criptografia devido ao fato da maior parte das comunicações transmitidas serem abertas; a propagação do tráfego malicioso presente na Internet associado a falhas de *software* e descuido de usuários; e, por fim, a arquitetura descentralizada da Internet idealizada de modo a não permitir que a Internet fosse controlada por governos, individualmente ou coletivamente.

No ECiber observa-se que as ações maliciosas são tomadas de acordo com a oportunidade que os atacantes possuem, aguardando a melhor janela para realizarem o ataque ao sistema ou rede de interesse, de maneira a alcançarem seus objetivos. No ponto de vista do *Chatham House* os alvos desses ataques podem ser encontrados não só no aparelhamento do Estado ou forças armadas, mas também em áreas civis de interesse (econômica, saúde e infraestrutura de cidades) (REINO UNIDO, 2010). De fato, a intenção do atacante pode variar desde um ataque a uma rede de infraestrutura militar até as estruturas civis, determinando o alcance da ação desencadeada.

De acordo com o relatório do *Chatham House* de março de 2009[12], pode-se observar quatro áreas de atuação das ameaças no ECiber: ataques patrocinados por Estados, extremismo político e ideológico, crime organizado profissional e crime individual (REINO

[12] REINO UNIDO. The Royal Institute of International Affairs. **Cyberspace and the National Security of the United Kingdom - Treats and Responses – A Chatham House Report.** Disponível em < https://www.chathamhouse.org/publications/papers/view/109020 > . Acesso em 26 de maio de 2017

UNIDO, 2009). Como resultado, observa-se que essas áreas de atuação contemplam um grande espectro de ações assimétricas no ECiber, permitindo que os diversos atores possam executar atividades com as mais variadas intenções.

Com o propósito de atingirem seus objetivos os atores presentes no ECiber empregam diversas técnicas, como utilização de um código malicioso *(malware)*[13], redes de "*botnet*"[14] e bombas lógicas[15], nos mais diversos sistemas de informação e C2 para obtenção de informações sensíveis, destruição de dados ou para causar danos à infraestrutura Estatal. Apesar da complexa e avançada habilidade e tecnologia empregadas na confecção, elaboração, testes e armazenamento dessas armas tecnológicas, o meio de entrega, de atuação e o efeito desejado das mesmas podem ser bem simples.

Em síntese, pode-se identificar alguns atores presentes neste novo campo de batalha por meio da análise das áreas de atuação e das técnicas empregadas no ECiber. Certamente cada atacante empregará os recursos tecnológicos disponíveis para realizar a suas ações e alcançar os objetivos de suas organizações. De acordo com a consultoria HEIMDAL SECURITY[16] e com o *Chatham House* (REINO UNIDO, 2010) alguns dos principais atores identificados são: Terroristas Cibernéticos (TerCiber), Espiões Cibernéticos (EspCiber), Ladrões Cibernéticos (LadCiber), Guerreiros Cibernéticos (GueCiber) e Ativistas Cibernéticos (AtCiber).

[13] "Código Malicioso (*malware*)" é um software malicioso utilizado para causar danos a sistemas computacionais intencionalmente ou obter informações sensíveis sem a permissão dos usuários. **Anatomy of targeted attacks with smart malware.** Disponível em <http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=4&sid=72a9dda0-d18e-406a-94ac-1b9223470e3c%40sessionmgr4007&hid=4001 >**.** Acesso em 26 de maio de 2017.

[14] Redes "*Botnet*" consistem em redes de computadores corrompidos, ligados a internet e controlados remotamente por um atacante por meio de canais de comando e controle. **Botnet spoofing - fighting botnet with itself**. Disponível em < http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=8&sid=72a9dda0-d18e-406a-94ac-1b9223470e3c%40sessionmgr4007&hid=4001 >. Acesso em 26 de maio de 2017.

[15] "Bombas Lógicas" são códigos escondidos deliberadamente inseridos em sistemas de infraestrutura crítica, capazes de causar graves danos a sua segurança e integridade. Possui como principal característica permanecer inativo até que o comando secreto para sua ativação seja executado. **Detecting Hidden Logic Bombs in Critical Infrastructure Software**. Disponível em < http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=14&sid=72a9dda0-d18e-406a-94ac-1b9223470e3c%40sessionmgr4007&hid=4001 >. Acesso em 26 de maio de 2017.

[16] CUCU, Paul. How every cyber attack works - A full list. **Heimdal Security**, fev. 2017. Disponível online em: < https://heimdalsecurity.com/blog/cyber-attack/ >**.** Acesso em 28 de maio de 2017

Como resultado da assimetria e dos espaços escondidos nos locais mais profundos do ECiber, os Terroristas Cibernéticos (TerCiber) ou *Cyberterrorists* são atores que atuam patrocinados por algum Estado ou não, encontrando no ECiber uma fonte de recursos valiosa seja para divulgação de suas ações ou captação de pessoal.

A espionagem cibernética é uma das atividades cibernéticas mais comuns no ECiber, seja como instrumento para expor informações sensíveis dos governos, roubar segredos e dados comerciais, seja como meio de obter dados de inteligência e reconhecimento de áreas de interesse. Assim, os Espiões Cibernéticos (EspCiber) ou *Cyberspies* são indivíduos que buscam obter tais informações, governamentais ou de empresas, de maneira a conquistarem vantagens estratégicas, financeiras ou políticas de modo a conseguirem superioridade de informação e grandes vitórias a um baixo custo.

Os EspCiber são peças chaves na estratégia de muitos governos ao redor do mundo na busca de informações de interesse através das vulnerabilidades dos diversos sistemas de C2 do oponente.

Em consequência do aumento do uso da Internet para o comércio eletrônico e transações financeiras, também se fazem presente no campo de batalha do ECiber os Ladrões Cibernéticos (LadCiber) ou *Cyberthieves.* Eles são indivíduos que praticam ataques ilegais aos órgãos governamentais, empresas e usuários de maneira a obterem vantagens financeiras.

Nos últimos anos tem-se observado um crescente número de ações de LadCiber, resultando em um incremento na busca por recursos para tornar as informações na internet mais seguras. Em paralelo, percebe-se que as técnicas de ataque evoluem, refinando-se constantemente. A utilização de uma vulnerabilidade no sistema Windows permitiu que LadCiber pudessem criptografar computadores do sistema de saúde do Reino Unido e de empresas ao redor do mundo. Para que os diversos usuários afetados pudessem ter suas informações decriptografadas, houve a exigência de pagamento de um “resgate”, conforme as

instruções constantes do código malicioso tipo *ramsonware*.

O crescente número de ameaças no ECiber fez com que os governos adotassem ações que permitissem se contrapor e realizar ações no ambiente virtual. Dessa forma, insere-se mais um ator no campo de batalha: os Guerreiros Cibernéticos (GueCiber) ou *Cyberwarriors*. Eles são agentes governamentais ou recrutados que desenvolvem capacidades de executar ataques cibernéticos em apoio aos objetivos estratégicos e de interesse de um Estado. Normalmente os GueCiber atuam conforme o determinado pelo governo em alvos selecionados, de acordo com a duração desejada e os meios indicados para execução do ataque.

Em geral, a autoria do ataque é sempre negada por esses GueCiber, de maneira a desqualificar as acusações dos Estados que sofreram o ataque, buscando manter o anonimato e causar confusão. Por conseguinte, é comum que quando as evidências apontam para a origem do ataque cibernético, o governo local diga que a responsabilidade é de indivíduos agindo por conta própria e não em favor do governo.

Segundo Clarke/Knake, a GCiber tornou-se tão importante para os Estados Unidos da América, que foi determinada a criação de um Comando Cibernético, reunindo GueCiber da Força Aérea, da Marinha e do Exército (CLARKE/KNAKE, 2010). De acordo com o previsto na Estratégia de Defesa Cibernética do Departamento de Defesa dos Estados Unidos da América (DoD)[17], o DoD deve ser capaz de integrar as capacidades cibernéticas de maneira a ser capaz de apoiar operações militares e estabelecer planos de contingência (EUA, 2015). Na visão do DoD,

> […] the United States military might use cyber operations to terminate an ongoing conflict on U.S. terms, or disrupt an adversary's military systems to prevent the use of force against U.S. interest. United States Cyber Command (USCYBERCOM) may also be directed to conduct cyber operations, in coordination with other U.S. government agencies as appropriate, to deter or defeat strategic threats in other domains. To ensure that the Internet remains open, secure, and prosperous, the

[17] EUA. The Departament of Defense. ***THE DoD CYBER STRATEGY***. Washington, DC 2015. Disponível online em < http://www.dtic.mil/doctrine/doctrine/other/dod_cyber_2015.pdf>. Acesso em 16 de jun. de 2017.

> United States will always conduct cyber operations under a doctrine of restraint, as required to protect human lives and to prevent the destruction of property. (EUA, 2015 p.5-6)[18]

Inegavelmente, pode-se observar que a GCiber se tornou uma das grandes preocupações do DoD dos Estados Unidos da América (EUA). Assim, a fim de reduzirem todas as possibilidades de sofrerem ataques no ECiber e adquirirem a capacidade de realizar ações no novo campo de batalha, os EUA criaram o Comando Cibernético dos Estados Unidos da América (*USCYBERCOM*), comando posicionado no mesmo nível dos comandos regionais devido a sua importância, unificando os comandos cibernéticos da Força Aérea, Marinha e Exército, responsável por coordenar e conduzir as ações no ECiber, de acordo com os interesses dos EUA.

Além disso, ainda podemos acrescentar um outro ator importante ao campo de batalha do ECiber, os Ativistas Cibernéticos (AtCiber) ou *Cyberactivists*. Tratam-se de indivíduos que efetuam ataques cibernéticos por prazer, razões filosóficas, políticas e não por questão financeira. O interesse desses AtCiber não é a informação sensível, e sim a obtenção da atenção necessária à sua causa ou às suas capacidades.

## 3.2 PRINCIPAIS RECURSOS DOS ATACANTES

Diante do amplo campo de atuação e anonimato providos pelo ECiber, os atacantes estão sempre aprimorando e atualizando seus métodos e recursos para execução de suas ações. Aproveitando-se das falhas de sistemas, das propagandas das diversas páginas da Internet, de e-mails de bancos, de outras instituições financeiras, de concessionárias prestadora de serviços, das informações de órgãos governamentais e, finalmente,

[18] "Os militares dos Estados Unidos podem usar operações cibernéticas para encerrar um conflito em andamento nos termos dos EUA, ou interromper o uso dos sistemas militares do inimigo de maneira a evitar o uso da força contra os interesses dos EUA. O Comando Cibernético dos Estados Unidos (USCYBERCOM) também pode ser direcionado a conduzir operações cibernéticas, em coordenação com outras agências governamentais dos EUA, conforme apropriado, para deter ou vencer as ameaças estratégicas em outros domínios. Para garantir que a Internet permaneça aberta, segura e próspera, os Estados Unidos sempre realizarão operações cibernéticas sob uma doutrina de restrição, conforme necessário para proteger vidas humanas e para evitar a destruição de propriedade." (Tradução nossa)

aproveitando-se do próprio usuário final, os atacantes encontram todas as ferramentas necessárias para poderem invadir um sistema e alcançarem seus objetivos.

Segundo o relatório da empresa *SYMANTEC – Internet Threat Secure Report* (ITSR)[19] de abril de 2017, os ataques cibernéticos atingiram um novo nível no ano de 2016. Tal ano foi marcado pelo crescente número de ataques virtuais ao sistema bancário, com prejuízo de milhões de dólares, por tentativas de grupos patrocinados por governos interessados prejudicarem o processo eleitoral nos EUA, assim como por grandes ataques de *Distributed Denial of Service (DDOS),* por meio de *botnets*, que utilizaram a conexão de periféricos a Internet, conhecido como Internet das Coisas *(Internet Of Things – IoT[20])* (SYMANTEC, 2017).

Sem dúvida, todos esses ataques geraram um elevado nível de interrupção nos diversos sistemas computacionais e em seus processos, embora os atacantes frequentemente tenham empregado ferramentas e táticas simples para obtenção desses grandes impactos. As vulnerabilidades de "dia-zero"[21] e os códigos maliciosos sofisticados estão sendo utilizados mais esporadicamente de maneira a manter os atacantes fora do foco dos setores de segurança do ECiber. De acordo com a Cartilha de Segurança para Internet do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR)[22] alguns dos principais recursos empregados para um ataque são: *phising*, *malware* (*vírus, worm, trojan, rootkit, spyware, adware e exploit kit*), *ramsonware*, *malvertising*, *pharming*, ataques DoS/DDoS (*Denial of Service/Distributed Denial of Service*) e *Remote Acess Trojan* (RAT).

[19] SYMANTEC. ***Internet Secure Threat Report*** **(ISTR) vol. 22. abr2017.** Disponível em < https://www.symantec.com/security-center/threat-report> . Acesso em 17 de jun. de 2017.

[20] *Internet of the Things (IoT)* – todos os diferentes aparelhos, incluindo computadores, telefones, tecnologia vestível, e todos os sistemas inteligentes, que são capazes de se interconectarem por meio da Internet (tradução nossa). Cambridge Dictionary. Disponível em < http://dictionary.cambridge.org/us/dictionary/english-portuguese/the-internet-of-things?q=internet+of+the+things >. Acesso em 13 de jul. de 2017.

[21] "Dia-Zero" – designação atribuída à situação na qual há uma ameaça capaz de explorar uma vulnerabilidade de segurança descoberta em sistemas computacionais e que não teve, ainda, sua correção disponibilizada pelo desenvolvedor ou fabricante. (BRASIL, 2014 p.18)

[22] Cartilha de Segurança para Internet. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR)**. Disponível em: < https://cartilha.cert.br/seguranca/ >**.** Acesso em 13 de jul. de 2017

Na FIGURA 1, anexo A, pode-se observar um resumo dos principais tipos de *malware* utilizados pelos atacantes, suas formas de propagação e suas ações principais.

Ressalta-se que os métodos apresentados acima não esgotam todos os recursos disponíveis para a utilização por parte de *hackers* na internet. De acordo com dados obtidos do ITSR (SYMANTEC, 2017a), o e-mail contendo códigos maliciosos foi a ferramenta escolhida para a realização dos ataques cibernéticos no ano de 2016, sendo este recurso empregado por grupos desde EspCiber financiados por governos em busca de informações por meio de espionagem cibernética, até grupos de LadCiber empregando distribuição em massa de e-mails contendo *ransomware* como forma de obtenção de recursos financeiros.

Conforme demonstra a FIGURA 2, anexo B, o ano de 2016 apresentou o maior número de ataques por código malicioso observado pela empresa SYMANTEC nos últimos anos. De acordo com os dados apresentados, um em cada 131 e-mails estava infectado por algum recurso malicioso. O emprego de e-mails contendo códigos maliciosos disfarçados em correspondência de rotina tem se tornado cada vez mais comum. Nesse sentido, pode-se destacar as faturas e as notificações de entrega contendo códigos maliciosos, apontados segundo o ITSR como um dos principais meios para a propagação do *ransomware.*

Segundo o ITSR (SYMANTEC, 2017a), o código malicioso tipo *ransomware* apresentou um significativo aumento nos casos detectados, tanto nas variantes de *ransomware* existentes, quanto nos valores pagos para a liberação dos arquivos "sequestrados", como observa-se na FIGURA 3, anexo B. O *ransomware* continua a infectar empresas e usuários com o uso indiscriminado de e-mails contendo códigos maliciosos anexados, de maneira que algumas empresas chegam a ficar sobrecarregadas com a grande quantidade de e-mails mal-intencionados que recebem. Os atacantes têm solicitado valores cada vez maiores para que os dados criptografados sejam recuperados. O pagamento do "resgate" dos dados via moedas virtuais, utilização de criptografia indecifrável e o emprego

de códigos maliciosos escondidos em e-mails inofensivos se tornou o principal modo de agir desses LadCiber.

Pelo resultado dos dados apresentados pela empresa SYMANTEC em seu ITSR de abril de 2017, verifica-se que o ECiber tem se tornado um espaço cada vez mais explorado por indivíduos mal-intencionados, e que seus métodos de atuação atingem todos os setores da sociedade. Com o avanço da tecnologia e das estratégias de defesa, que dificultam ou impedem a atuação dos atacantes, estes necessitam criar novos programas e métodos para que alcancem seus objetivos. Isso exige uma combinação cada vez maior de cuidados e procedimentos de segurança de maneira a minimizar as situações que permitam ataques e o comprometimento de sistemas e dados de interesse. Por isso, a contenção da propagação dessas ameaças é a grande e contínua luta travada no novo campo de batalha, principalmente devido ao crescente uso do ambiente virtual por governos, empresas e pessoas comuns, o que favorece o ataque por parte de usuários mal-intencionados.

## 3.3 DESAFIOS

O ambiente digital tem mudado rapidamente. Não há mais o controle sobre o crescimento da arquitetura da Internet, como no momento em que o sistema foi delineado, uma vez que todos os anos milhões de pessoas entram no mundo virtual pela primeira vez. Em face da expansão do acesso ao ECiber e do grande número de interconectores, o tráfego pela Internet aumenta significativamente ao redor do globo.

A Internet tornou-se maior do que qualquer Estado ou conjunto de Estados, e seu ritmo de crescimento está além do alcance das maiores e mais reativas empresas de tecnologia. Como resultado, observa-se no ECiber um grande espectro de usos e complexidades, que se aprofundam cada vez mais e contribuem como causa em potencial para fricções e conflitos. Outrossim, nota-se o crescimento do investimento por parte dos governos

em empresas de segurança cibernética, para a condução de ações defensivas e ofensivas no ECiber, bem como a construção de barreiras contra as mais diversas ameaças.

Indubitavelmente, uma especial atenção deve ser dada para a maneira como o conflito no ECiber moldará, conduzir ou restringir a guerra no futuro, segundo a dinâmica econômica. Sem dúvida, os danos causados a instituições financeiras e a infraestruturas críticas, seja por um ataque físico ou um ataque virtual, representará um custo elevado ao Estado envolvido. Como resultado, as consequências econômicas da entrada em uma guerra cibernética serão tão elevadas e dispendiosas a um Estado que não esteja preparado para esse novo campo de batalha, quanto são os custos para ingressar em uma guerra convencional.

Ao contrário dos conflitos no ar, mar e terra, que deixam ensinamentos para serem utilizados posteriormente, as lições apreendidas previamente no ECiber não necessariamente serão úteis ou adequadas para o emprego futuro. Não existe uma maneira adequada de descrever a complexidade do ECiber, um ambiente que permite um alto grau de anonimato com quase nenhuma barreira para entrada, e que se torna cada vez mais integrado à vida moderna.

No ponto de vista do *Chatham House*, um dos problemas existentes no desenvolvimento de um regime de controle para a GCiber é a falta de um consenso entre os líderes políticos e militares sobre o que realmente constitui a GCiber (REINO UNIDO, 2010). Como resultado, persiste a dúvida sobre quais tipos de ações podem ser efetivamente consideradas ações de guerra. Assim, conforme apontado anteriormente, um AtCiber mal interpretado pode levar à eclosão de um conflito real.

Finalmente, outro aspecto a ser observado é a interconexão entre as redes públicas, privadas e governamentais em decorrência da comercialização da Internet, tornando a rede parte da infraestrutura de informação dos Estados. O grande aumento da rede, combinado à dependência cada vez maior dos sistemas de comunicação, fez com que as

vulnerabilidades se expandissem, assim como todos os perigos decorrentes desse rápido crescimento, a exemplo da falta de atenção diante de potenciais perigos a toda infraestrutura. Uma vez que a infraestrutura crítica ligada à rede não se prende mais aos limites geográficos de um Estado, esta se encontra ligada à expansão constante da Internet independente do controle de um Estado específico, permitindo que as vulnerabilidades que existem sejam exploradas pelos mais diversos atores de acordo com seus interesses.

## 3.4 ANÁLISE DO CAPÍTULO

Inegavelmente, o crescimento acelerado da Internet permitiu que uma grande quantidade de vulnerabilidades passasse a fazer parte do cotidiano de todos os usuários conectados na rede. Como resultado, identificou-se algumas vulnerabilidades, como a questão dos ISP responsáveis pelo carregamento dos dados pela rede, os BCG roteadores responsáveis por encaminharem corretamente os dados entre a origem e o destino, a ausência de uma governança na rede que fosse responsável por evitar que a mesma informação chegasse a dois usuários utilizando o mesmo IP, a ausência de criptografia na Internet aonde a maior parte dos dados que circulam por ela seguem abertos, a grande quantidade de tráfego malicioso presente no ambiente virtual e a Internet enquanto uma grande rede com a arquitetura descentralizada.

Também foram apontados os atores que utilizam e exploram essas vulnerabilidades no ECiber, que são: os TerCiber que utilizam a Internet como forma de divulgação de sua ideologia, recrutamento de pessoal e como recurso para coordenação de suas ações fora do mundo virtual, os EspCiber, que são responsáveis pela aquisição de informações e de dados sensíveis de interesse, assim como pela realização de ações de sabotagem no ECiber, como por exemplo a implantação de bombas lógicas em sistemas de interesse, os LadCiber que realizam ataques a diversas instituições governamentais ou privadas em busca de retorno financeiro, os GueCiber, que são agentes governamentais

responsáveis por realizar ações no ECiber de acordo com os interesses de seus governos, e os AtCiber que realizam ataques por questões ideológicas, como forma de expressarem seus protestos e divulgarem sua causa, sem a intenção de obtenção de recursos financeiros. Foi abordada a crescente preocupação dos governos com o ECiber, que buscam criar órgãos civis e comandos militares de monitoramento, ataque e defesa do ambiente virtual.

No mais, foram apresentados alguns recursos utilizados por esses atores para realizarem suas ações no ECiber, como: o *phishing*, o *malware*, o *ramsonware*, o *malvertising*, ataques a DNS por meio de *pharming*, ataques de DoS ou DDoS e o emprego de RAT. Da análise de dados de relatório de segurança da empresa SYMANTEC observou-se o crescimento acelerado do emprego das diversas formas de ataque, bem como a elevação dos custos decorrentes dessas ações.

Na sequência, apontou-se alguns desafios que estão presentes no ECiber, tais como a rapidez das mudanças no ambiente virtual em decorrência de não se possuir gestão sobre a arquitetura da Internet, a internacionalização da Internet com sua ausência de barreiras permitindo que usuários mal intencionados possam realizar suas ações dos lugares mais distantes, tornando-se um potencial foco para o início de um conflito entre Estados e a dificuldade de se mensurar o efeito que ações no ECiber poderão ocasionar no mundo real.

Também se analisou que, em face da dinâmica do mundo virtual, é difícil se beneficiar com o histórico de lições aprendidas, já que a próxima ação, por mais parecida que seja, provavelmente adotará um método diferente. Finalmente, após análise dos desafios presentes no ECiber, constatou-se que realmente é difícil se estabelecer quais ações no ECiber podem ser consideradas como ações de guerra, bem como que a dependência cada vez maior da Internet, dos meios de comunicação ligados à rede e do acesso rápido à informação buscada, ampliou as vulnerabilidades existentes para todos os usuários da grande rede.

# 4 SEGURANÇA CIBERNÉTICA

Inquestionavelmente, a infraestrutura global de Tecnologia de Informações e Comunicações (TIC) oferece uma ferramenta de interconectividade eficiente e efetiva para as pessoas e as organizações. Além disso, a capacidade de comunicação em tempo real promoveu uma revolução em termos de dinamicidade e empreendedorismo em negócios, sejam eles nacionais ou internacionais. No entanto, à medida que a Internet se torna mais acessível ao público atingindo usuários em um nível global, constata-se que o ECiber também se mostra propício ao emprego indevido por usuários capazes de explorarem as vulnerabilidades presentes em seu amplo ambiente.

Em virtude de todas essas fragilidades presentes no ECiber, vários setores da sociedade procuram proteger seus interesses e dados de uma série de danos potenciais, por meio do que podemos chamar de Segurança Cibernética (SegCiber). Diante da TIC cada vez mais presente no cotidiano das pessoas, os usuários do ECiber não podem se dar ao luxo de desprezar a SegCiber,

Neste capítulo, será apresentada a razão pela qual se faz necessário que se estabeleça uma concepção comum da SegCiber, de maneira a se compreender a amplitude e a profundidade do problema decorrente da ausência de mecanismos de proteção aos dados sensíveis. Também serão identificadas medidas que possam ser adotadas nos setores público e privado, de modo a disponibilizar para os usuários ferramentas que garantam a segurança no ambiente virtual, assim como serão apresentadas algumas políticas para colocar em prática os princípios da SegCiber.

## 4.1 SEGURANÇA CIBERNÉTICA E A ATUALIDADE

A SegCiber tem sido conceituada de formas diferentes de modo que tais conceitos provocam inúmeras políticas de respostas a ataques no ECiber. Essas respostas geralmente

seguem o nível de ameaça percebido pela SegCiber e essa percepção está relacionada a um usuário comum, uma empresa ou a um órgão governamental. Para todos esses usuários a combinação de segurança de computadores e segurança de rede é o que melhor representa o conceito de SegCiber.

A segurança de computadores está concentrada na proteção tanto do sistema como um todo (*hardware*[23] e *software*[24]), quanto da informação contida nessas máquinas, de maneira que eles estejam protegidos de roubo, corrompimento ou negação do acesso eventualmente causado por um código malicioso implantado na estação de trabalho.

De acordo com o *Chatham House* a segurança de computadores assume um papel protetivo e reativo, de forma que as medidas de segurança adotadas tanto no campo físico quanto no virtual limitam o acesso a diversos sistemas e reagem a uma vulnerabilidade de *software* quando identificada (REINO UNIDO, 2009). Assim, cabe à SegCiber manter essas medidas atualizadas e prontas para enfrentar os atacantes.

A segurança das redes também será possível por meio de medidas físicas, como maneira de limitar o acesso não autorizado aos recursos e equipamentos que compõe a estrutura daquela rede, bem como por meio de medidas eletrônicas, que visam proteger a infraestrutura das redes de computadores.

Sem dúvida, a segurança de computadores será complementada pela segurança de rede e ambas devem ser vistas de forma prioritária pela SegCiber. Os recursos mais sofisticados de planejamento e preparação devem ser empregados, a fim de garantir a segurança e inviolabilidade dos sistemas de informação de interesse para os diversos usuários do ECiber.

De acordo com o Prof. Dr. Antonio Brasiliano em sua publicação Coletânea de

[23] *Hardware* – maquinas ou equipamentos que compõem um sistema de computador, sem os programas (tradução nossa). Disponível em < http://dictionary.cambridge.org/us/dictionary/english-portuguese/hardware >. Acesso em 13 de jul. de 2017.

[24] *Software* – programas usados nos computadores para executar diferentes tarefas (tradução nossa). Disponível em < http://dictionary.cambridge.org/us/dictionary/english-portuguese/software >. Acesso em 13 de jul. de 2017.

Riscos Cibernéticos[25], a mutabilidade e dinamicidade fazem parte do atual cenário da segurança da informação. Em sua publicação ele comenta que, com frequência, é possível observar notícias divulgadas pela mídia de casos de vazamento de dados, invasões por arquivos maliciosos em grandes empresas e órgãos governamentais, sequestro de informações e ataques de cibercriminosos (BRASILIANO, 2016). Tal colocação reforça a importância que deve ser dada para a SegCiber, devendo essa questão tornar-se prioridade na utilização do ECiber.

Brasiliano chama a atenção para a questão das ameaças e dos principais métodos utilizados pelos atacantes, ressaltando o valor da segurança cibernética para as empresas (BRASILIANO, 2016 p.6):

> O campo de batalha mudou!! Hoje, a transformação digital pela qual as empresas do mundo todo estão passando tornou a luta contra ações cibercriminosas ainda mais complexa. Cada brecha de Segurança é aproveitada pelas quadrilhas de bandidos virtuais, seja uma porta semiaberta, um link despretensioso em um e-mail ou um simples *pen drive*, tudo pode servir como meio de um ataque virtual. Com esse novo campo de batalha, as empresas devem se armar com tecnologia e novas estratégias.

De certo, a análise acima não se limita ao campo empresarial, mas é válida para todos os usuários do ECiber. Percebe-se que a batalha não é justa, já que, ainda que os usuários sejam cuidadosos, em algum momento o atacante vai conseguir encontrar uma vulnerabilidade e realizar o ataque, seja empregando seus recursos próprios ou utilizando um usuário interno. Enquanto o defensor precisa manter suas defesas, em todas as frentes, sempre atualizadas e protegidas, basta que o atacante realize um ataque bem-sucedido para que ele ganhe a batalha.

## 4.2 SEGURANÇA CIBERNÉTICA ALGUNS PRINCÍPIOS

Uma política comum para a SegCiber pode reunir os interesses, as preocupações e as abordagens utilizadas por diversos atores, como usuários, empresas e governos. Como

[25] BRASILIANO, Antonio C. R., PhD. **Coletânea de Riscos Cibernéticos.** São Paulo, Interisk, 2017. Disponível em <https://www.brasiliano.com.br/coletanea-riscos-ciberneticos>. Acesso em 30 de jun. de 2017.

exemplo, destaca-se que a SegCiber deve ser tratada como um assunto de segurança nacional, a ser priorizada e adotada concomitantemente por todos os setores interessados. Na opinião de Brasiliano uma infraestrutura crítica confiável é essencial para a segurança nacional e econômica de um país (BRASILIANO, 2016), e para se alcançar essa confiabilidade é necessário que todos os sistemas que compõem essas infraestruturas estejam protegidos.

No ponto de vista do *Chatham House* uma abordagem comum da SegCiber está baseada em três princípios: a governança, o gerenciamento de risco e a inclusão (REINO UNIDO, 2009).

A governança na SegCiber equivale a um esforço conjunto, por parte de todos os usuários do ECiber, de forma a garantir que o estabelecimento de uma cultura de SegCiber seja eficaz e duradoura.

Por conseguinte, o gerenciamento de risco busca a identificação das principais vulnerabilidades e ameaças em potencial para a TIC, assim como a avaliação de contramedidas e de recursos que possam ser aplicados na diminuição dos danos causados por um ataque cibernético. Para Brasiliano, a gestão de risco é um processo de avaliação, identificação e resposta aos riscos aonde cada organização deverá conhecer a probabilidade do acontecimento de um evento e seu impacto resultante (BRASILIANO, 2016).

Por fim, no tocante à inclusão, é importante se saber que a terminologia do ECiber e SegCiber deve ser compreendida nas esferas política e social, e não apenas no campo técnico, já que como visto para que se garanta segurança é necessária a participação dos Governos e dos usuários, que não poderão colaborar de modo eficiente se o conhecimento sobre SegCiber estiver restrito a especialistas da área. Já que o ECiber é um local global para a troca de informações e comunicações, os usuários precisam estar familiarizados com os recursos e termos necessários para a compreensão do ambiente virtual.

Assim sendo, o acesso aos conceitos presentes no ECiber, pelo maior número

possível de usuários, passa a ser de suma importância para que se alcance a amplitude necessária para assegurar a participação, a compreensão e a resposta aos desafios impostos pela SegCiber.

## 4.3 SEGURANÇA CIBERNÉTICA: ALGUMAS QUESTÕES OPERACIONAIS.

Considerando os princípios apresentados no item anterior, a orientação para uma concepção comum da SegCiber passa a ser prioridade. O nível estratégico passa a ser responsável pela implementação de políticas coerentes para SegCiber, porém a inconsistência dessas políticas prejudica o alcance de uma concepção comum. Assim, verifica-se que cabe ao nível operacional a responsabilidade por empregar essas políticas dando atenção a algumas questões importantes como a agilidade e iniciativa, a neutralidade de atores e gerenciamentos de riscos, conforme apontado pelo *Chatham House* (REINO UNIDO, 2009). Tais questões, que estão intrínsecas ao vasto campo do ECiber, e devem ser consideradas na confecção das políticas estabelecidas pelo nível estratégico.

Primeiramente, esclarece-se que a agilidade e a iniciativa das ações são decorrentes da característica de que as ameaças cibernéticas possuem um alcance muito amplo e têm a capacidade de mutação grande, podendo assumir uma posição estática, defensiva ou ofensiva.

Nesse contexto acima, as respostas às ameaças no ECiber são reativas em vez de antecipadas. Assim, quando os usuários, as empresas e os governos estão começando a se preocupar com a SegCiber, as ameaças no ECiber já estão sendo ocorrendo e ataques sendo realizados.

O emprego das políticas de SegCiber, como visto, também deverá levar em consideração a questão da neutralidade de atores. Isso porque, um “ator neutro”, seja numa ameaça ou numa resposta a um ataque, pode garantir que os recursos disponíveis sejam

aplicados prontamente e eficientemente, assegurando que as ações de SegCiber tenham sucesso.

Por fim, a gestão de risco igualmente tem papel cada vez mais relevante, já que a eliminação de todas as ameaças presentes no ECiber é impossível, especialmente por estarem em constante evolução, assim como na maioria das vezes e o filtro de toda atividade criminosa ou maliciosa (atual ou potencial), na infraestrutura global de TIC, é de difícil alcance.

Certamente a ampliação do de cobertura da TIC, a facilidade de acesso ao ECiber por todos e a crescente dependência por parte dos usuários, dificultam as ações de SegCiber. No ponto de vista do gerenciamento de risco em SegCiber o *Chatham House* aponta alguns aspectos a serem observados (REINO UNIDO, 2009): o uso das TIC por usuários autorizados não livra o ECiber de ameaças e ataques, implementação da SegCiber em todos os níveis, a constante revisão das prioridades da SegCiber e a concepção de políticas de acordo com os riscos apontados.

Por fim, cabe destacar que Brasiliano, ao analisar a importância da SegCiber, enfatiza que cada organização deve estabelecer bases sólidas de segurança, cujas especificações e necessidades dependerão de questões como o setor de atividade e a sua localização geográfica (BRASILIANO, 2016).

## 4.4 ANÁLISE DO CAPÍTULO

Sem dúvida a SegCiber se tornou a grande preocupação de todos os usuários do ECiber, principalmente devido ao avanço das ameaças nesse novo campo de batalha.

Dessa forma, a infraestrutura de TIC representa a grande vulnerabilidade do ECiber, pois por ela diariamente são trafegados uma grande quantidade de dados que permitem o funcionamento de praticamente todos os sistemas presentes em nosso cotidiano.

Diante dessa fragilidade torna-se fundamental que todos, desde o usuário comum, as grandes empresas, as instituições financeiras, até os setores governamentais e militares, adotem a questão da SegCiber como prioritária. Em síntese, a adoção de uma política comum para SegCiber poderá reunir interesses dos diversos atores e fortalecer as defesas contra as ameaças no mundo virtual. Além disso, tais políticas poderão consolidar a proteção às infraestruturas críticas essenciais para segurança nacional e economia dos Estados.

A fim de se tornar efetiva a SegCiber deve se basear em três princípios, a governança, para a efetivação de políticas no ECiber, o gerenciamento de risco, de maneira a identificar as vulnerabilidades e estabelecer as contramedidas para defesa, e, por fim, a inclusão, como forma de permitir que todos os usuários tenham acesso e compreendam a linguagem no âmbito da SegCiber, para que possam ter o conhecimento necessário para implementarem medidas que possibilitem o fortalecimento da SegCiber. Todos os usuários devem estar preocupados com a manutenção e atualização de seus sistemas computacionais (*hardware e software*), bem como com a segurança das redes que se interconectam ao ECiber, para garantir a confiabilidade e a estabilidade necessária para SegCiber.

Outrossim, ressalta-se alguns aspectos operacionais necessários para a implementação eficaz de medidas de SegCiber, como por exemplo a agilidade e iniciativa que o defensor deve praticar para contrapor aos atacantes e resolver os problemas decorrentes de ataques bem-sucedidos, a identificação das possíveis ameaças e suas capacidades de forma a reduzir a influência dos atores “neutros” e ainda a implementação da gestão de risco como maneira de minimizar os efeitos decorrentes da impossibilidade de se isolar completamente as redes do ECiber.

Portanto, conclui-se que a SegCiber deve ser priorizada em todos os setores da sociedade como forma de preservação dos dados individuais e garantia do bom funcionamento de todos os sistemas presentes no ECiber.

# 5 *WANNACRY* O *RANSOMWARE* QUE ALERTOU O MUNDO

A expansão da conectividade dos sistemas de informação, das infraestruturas críticas e do número de usuários no ECiber permitiu a disseminação indiscriminada de um *malware* mais inteligente.

O emprego desse novo tipo de *malware* inteligente, que utiliza as vulnerabilidades de segurança dos sistemas para atingir seus objetivos, sem a necessidade de interação com o usuário, torna os ataques que empregam esse novo recurso muito mais perigosos do que os que utilizam o *malware* convencional, que dependem da interação com o usuário para serem ativados.

Nesse sentido, cabe ressaltar que os ataques realizados com esse novo recurso podem resultar em perdas econômicas significativas, além de provocarem um grande efeito na sociedade em geral. Como resultado, o emprego de um *malware* inteligente do tipo *ransomware* em conjunto com um tipo *worm*, como visto no capítulo 3, o *WannaCry*, expôs em escala global os perigos decorrentes das diversas vulnerabilidades dos sistemas que integram o ECiber e sua utilização por criminosos cibernéticos.

## 5.1 O *WANNACRY* E SUA FORMA DE OPERAÇÃO

No dia 12 de maio de 2017, um ataque sem precedentes chamou a atenção do mundo. Por causa da combinação do código malicioso tipo *ransomware* com um tipo *worm*, que possui como característica se replicar rapidamente e se espalhar, automaticamente, por computadores em rede, o *WannaCry* se expandiu e atingiu um grande número de usuários simultaneamente.

A grande diferença desse código malicioso é que uma vez instalado em um computador de uma organização o *WannaCry* passa a buscar outras máquinas vulneráveis dentro da mesma rede, e como uma reação em cadeia infecta uma a uma, sem a necessidade

do usuário abrir qualquer link malicioso.

De acordo com o relatório de Resposta de Segurança da Symantec (*Symantec Security Response – SSR*)[26] o modo de operação do *WannaCry* é descrito como: "*Ransom.Wannacry is a worm that spreads by exploiting vulnerabilities in the Windows operating system. Once installed, it encrypts files and demands a payment to decrypt them.*"[27].

Desse modo, como relatado no SSR da Symantec (SYMANTEC, 2017b), o *WannaCry* utilizou o método supramencionado para se disseminar, explorando as vulnerabilidades do sistema operacional *Windows* de maneira nunca antes vista. Empregou um modo de operação que consistiu no uso de criptografia para "sequestrar" os dados dos usuários (empresas, instituições financeiras, indivíduos, etc.) e solicitar o pagamento de "resgate", normalmente em moedas virtuais, como condição para realizar a descriptografar os arquivos e, assim, disponibilizar novamente os dados aos usuários.

Ainda, segundo o relatório SSR da Symantec (SYMANTEC, 2017b) observou-se que alertas sobre possíveis ataques já vinham sendo divulgados na Internet desde fevereiro de 2017, por empresas de SegCiber, especialmente em virtude da divulgação, pelo *WikiLeaks*[28], de uma ferramenta usada pela Agência de Segurança Nacional dos EUA (*NSA – National Security Agency*[29]) para espionar alvos de interesse Estatal, por meio de uma vulnerabilidade do sistema Windows.

Sem dúvida, a grande vantagem e o poder deste ataque estão concentrados na capacidade do código malicioso se espalhar de forma ampla e independente. O atacante se

[26] SYMANTEC, **Ransom.Wannacry** – Symantec Security Response. Maio 2017. Disponível em < https://www.symantec.com/security_response/writeup.jsp?docid=2017-051310-3522-99 >. Acesso em 7 de julho de 2017.

[27] "Ramson.Wannacry é um *worm* que se espalha por meio da exploração de vulnerabilidades do Sistema operacional Windows. Uma vez instalado, ele criptografa os arquivos e solicita o pagamento para decriptografar eles." (tradução nossa)

[28] Wikileaks é um site especializado em analisar e publicar grandes conjuntos de dados e materiais oficiais censurados ou restritos sobre guerra, espionagem e corrupção (tradução nossa). Disponível em <https://wikileaks.org/What-is-Wikileaks.html>. Acesso em 7 de jul. de 2017.

[29] NSA – organização governamental dos EUA responsável por verificar as comunicações estrangeiras, especialmente aquelas que possam conter alguma ameaça a segurança do país, bem como proteger suas comunicações eletrônicas (tradução nossa). Disponível em < http://dictionary.cambridge.org/us/dictionary/english/nsa?q=NSA >. Acesso em 14 de jul. 2017.

valeu do poder dessa estratégia, aproveitando-se de uma organização vulnerável e de grande porte para, na sequência, pulverizar seu código pela rede. No caso, o *WannaCry* atacou os servidores do sistema de saúde do Reino Unido, deixando inúmeras instituições de saúde, como hospitais e clínicas médicas, sem qualquer acesso aos dados e documentação médica de milhares de pacientes, cujas informações se tornaram inacessíveis por meio de criptografia.

Logo após a infecção bem-sucedida dos servidores, uma mensagem nos computadores "sequestrados" solicitava o pagamento de cerca de US$ 600,00 que deveria se dar através do uso de um tipo de moeda virtual, para que os acessos aos dados criptografados fossem liberados. Acredita-se que a escolha dos servidores do sistema de saúde do Reino Unido foi devido à dependência desse sistema da TIC, aliado aos fatos de se tratar de uma instituição pública, com infraestrutura tecnológica antiga, cujas estações de trabalho não possuíam as atualizações necessárias que garantissem a manutenção da segurança de nos seus sistemas operacionais em rede.

Uma vez infectadas diversas estações de trabalho que estavam conectadas na rede do sistema de saúde acima citado, o vírus começou a se espalhar rapidamente por meio da Internet, atingindo milhares de servidores pelo mundo. Assim, aproveitando-se dessa característica de fácil disseminação, o mesmo seguiu explorando as vulnerabilidades existentes em outras redes atingindo, inclusive, computadores de grandes empresas e de órgãos públicos, como a *Telefônica* da Espanha, e a FEDEX dos EUA e outros serviços em diversos países.

Provavelmente, o atacante deve ter acreditado que as instituições afetadas disponibilizariam recursos financeiros para custearem o "resgate" do "pequeno" valor cobrado por estação de trabalho, de modo a evitarem um colapso e prejuízos maiores. Contudo, não foi exatamente assim que ocorreu. Existiram alguns pagamentos, porém grande parte dos usuários afetados seguiram as recomendações dos especialistas em SegCiber, não

cedendo à chantagem.

Nesse sentido, e com base nas análises do ataque ocorrido, imagina-se que os alvos principais desse tipo de ação sejam organizações que possuem serviços críticos e para quem a segurança e manutenção de dados sejam essenciais para a continuidade das atividades. Assim, empresas de telecomunicações, de saúde, de logística e de transporte, cujos bancos de dados são fundamentais para o funcionamento de suas operações, parecem ser alvos em potencial.

De acordo com a análise da empresa *McAfee*[30], o *WannaCry* usou a vulnerabilidade do sistema operacional para se propagar por outras máquinas através do *NetBIOS*[31]. Assim o *malware* gerou endereços de IP aleatórios, não limitados à rede local, se espalhando pela Internet por meio de diversos sites que permitem o recebimento de pacotes de *NetBIOS* a partir de outras redes externas. Essa característica do *ransomware* possibilitou sua dispersão pela rede sem que os usuários pudessem ter certeza sobre o vetor inicial do *malware (MACAFEE, 2017)*.

O *WannaCry* também possui uma outra característica, qual seja, uma vez encontrada uma máquina com o *NetBIOS* liberado, o *malware* envia três pacotes de configuração de *NetBIOS*, um contendo o próprio IP da máquina invadida e outros dois com IP diferentes, configurados para a exploração pelo *malware*. Como resultado, esse recurso torna muito difícil a detecção da infecção da máquina antes da ativação do *ransomware* e criptografia dos arquivos.

Assim sendo, apesar de toda a dificuldade para detectar a infecção, a interrupção da propagação do *WannaCry* se deu por acaso. Segundo o site da BBC Brasil[32], enquanto um

30 MACAFEE. McAfee Labs – **Futher Analysis of WannaCry Ransomware** – May 14,2017. Disponível online em < https://securingtomorrow.mcafee.com/mcafee-labs/analysis-wannacry-ransomware/ >. Acesso em 09 de jul. de 2017.

31 NetBIOS – "Network Basic Input/Output System" protocolo que permite a interface de conexão entre o sistema operacional, hardware e a comunicação com outros computadores ligados a rede (tradução nossa) Disponível em < https://techterms.com/definition/netbios >. Acesso em 09 de jul. de 2017.

32 BARANIUCK, Chris – BBC Tecnologia – **Como uma descoberta acidental interrompeu o "sequestro" de computadores em grandes empresas ao redor do mundo**. Disponível em <

pesquisador analisava o código responsável pelo funcionamento do *ransomware*, percebeu que esse código buscava acessar um endereço de Internet incomum, de modo que ele decidiu "comprar" o endereço para poder analisar melhor o funcionamento do código. Ao realizar tal operação, percebeu que a compra do registro interrompera a propagação do *ransomware*.

Em consequência, essa cessação na disseminação do *WannaCry* evitou que outras milhares de estações de trabalho ao redor do globo tivessem seus dados bloqueados. Porém, de acordo com a *MacAfee* (MACAFEE, 2017), outras variáveis do *ransomware* podem, ainda, ser encontradas no ECiber, com capacidade de infectar e se espalhar pela rede, embora de maneira menos agressiva. A redução dessa agressividade se deve ao fato de que as equipes de SegCiber apresentaram uma resposta ágil, que logo disponibilizando atualizações, inclusive para sistemas já obsoletos, que eliminando com a vulnerabilidade explorada pelo *WannaCry*.

## 5.2 WANNACRY: MANEIRAS DE PREVENÇÃO

Em decorrência do modo de operação inédito do *WannaCry* se faz necessário que todos os usuários do ECiber deem grande importância à SegCiber, buscando a adoção de medidas de defesa profundas, por meio da utilização de *firewalls*[33], de antivírus, de atualizações constantes nos sistemas operacionais e, também, através da realização de *backups*[34]. Adicionalmente, e especificamente no caso de um *ransomware,* é importante dar atenção a detalhes como falhas de atualização importantes dos sistemas operacionais e ações humanas indevidas.

Em síntese, todas essas recomendações e políticas auxiliam na busca pela garantia da integridade dos sistemas e dos dados de todos os usuários na rede, em face das ameaças

http://www.bbc.com/portuguese/geral-39903918 >. Acesso em 09 de jul. de 2017.

[33] *Firewall* – um dispositivo ou programa que impede que pessoas acessem ou usem informações em um computador sem autorização enquanto ele esteja conectado na Internet (tradução nossa). Disponível em < http://dictionary.cambridge.org/us/dictionary/english/firewall >. Acesso em 14 de jul. de 2017.

[34] *Backup* – é a cópia extra da informação de um computador que fica armazenada separadamente (tradução nossa). Disponível em < http://dictionary.cambridge.org/us/dictionary/english/backup >. Acesso em 14 de jul. de 2017.

existentes no ECiber. Porém, como afirma Brasiliano, existe uma constante multiplicação das ameaças cibernéticas, principalmente em um mundo digital e interconectado que abrem constantemente caminhos para uma nova gama de vulnerabilidades (BRASILIANO, 2016).

Sendo assim, torna-se fundamental que todos os usuários ponham em prática as recomendações de segurança estabelecidas pelos administradores de rede em suas estações de trabalho, seja no âmbito das instituições, seja no âmbito pessoal.

## 5.3 ANÁLISE DO CAPÍTULO

Nesse capítulo foi estudado o caso do *ransomware WannaCry*, que se aproveitou de uma falha do sistema Windows para infectar milhares de computadores ao redor do mundo. Os estudos do caso demonstraram a importância de que os responsáveis pela SegCiber estejam aptos a tomarem ações com mais agilidade de forma a conter e reduzir os efeitos desses ataques, ou mesmo evitarem-nos.

Em decorrência do caso *WannaCry,* observou-se que novos ataques de proporção mundial podem vir a ocorrer, porém, também se constatou que as respostas das equipes de SegCiber ao redor do globo demonstraram a crescente preocupação com a manutenção da segurança no ECiber. Por ocasião do ataque, atualizações de segurança para sistemas operacionais descontinuados foram rapidamente disponibilizadas aos usuários.

Outrossim, foi visto que diversos estudos e relatórios reforçaram a necessidade de implementação de diversas políticas de SegCiber, e constante aperfeiçoamento dessas práticas, visando evitar ou reduzir os efeitos de ataques generalizados.

Por fim, ressaltou-se que todos os usuários que utilizam o ECiber devem tratar a SegCiber como prioridade,, de modo a impedirem que ameaças como o *WannaCry* desestabilizem os diversos setores da sociedade.

# 6 CONCLUSÃO

Inicialmente, no presente trabalho apresentou-se a maneira como o mundo atual foi modificado por meio da Internet, que alterou o modo como as pessoas interagem, realizam negócios e compartilham a informação. Foi observado que essas mudanças propiciaram o surgimento de um novo campo de batalha, o campo da Guerra Cibernética.

Destacou-se alguns conceitos, próprios desse novo campo de batalha, contidos na publicação normativa do MD, como GCiber, DCiber, ECiber, ACiber, ICIn e IC. Ainda, foram tecidos comentários sobre os atores que podem se apresentar nesse novo campo, esclarecendo-se que os mesmos podem estar tanto representando um Estado, quanto um grupo a parte, o qual poderá ter interesses de diversas naturezas, sejam elas individuais, militares, civis, políticos, econômicos ou estratégicos. Conclui-se, após análises, que nesse novo campo de batalha não há como avaliar as consequências dos ataques e a proporcionalidade da força empregada.

Na sequência, estabeleceu-se a relação entre a evolução das redes de comunicações nos dias atuais e a velocidade de propagação das informações, bem como seu alcance. Foi visto que tal evolução tecnológica permitiu que as informações passassem a atingir os locais mais remotos do globo terrestre, com rapidez quase que instantânea, tornando a imensa aldeia global um mundo sem fronteiras. Nesse contexto, ficou evidenciado que as ações no ECiber também se tornaram mais ágeis.

Como se demonstrou, é inegável que o crescimento acelerado da Internet permitiu o surgimento de vulnerabilidades que se tornaram parte do cotidiano de todos os usuários conectados à rede. Consequentemente, algumas dessas vulnerabilidades foram mapeadas, como os ISP, os roteadores BCG, a ausência de uma governança na rede, a ausência de criptografia na Internet, a grande quantidade de tráfego malicioso presente no ambiente virtual e a Internet enquanto uma grande rede com a arquitetura descentralizada.

Da mesma forma que foram apontadas as vulnerabilidades, também indicou-se os atores que procuram explorar essas vulnerabilidades presentes no ECiber, como: os TerCiber, os EspCiber, os LadCiber, os GueCiber e os AtCiber.

Como resultado da diversidade de atores atuando nesse novo campo de batalha, observou-se ser crescente a preocupação dos governos com o ECiber. Nesse contexto, muitos governos, que buscam criar órgãos civis e comandos militares de monitoramento, ataque e defesa do ambiente virtual.

A seguir, identificou-se alguns recursos utilizados por esses atores para realizarem suas ações no ECiber, como: o *phishing*, o *malware*, o *ramsonware*, o *malvertising*, o *pharming*, os ataques de DoS ou DDoS e o emprego de RAT.

Ressaltou-se alguns desafios que estão presentes no ECiber, como: a rapidez das mudanças no ambiente virtual, a globalização da Internet sem a imposição de barreiras, a dificuldade de se mensurar o efeito que ações no ECiber poderão ocasionar no mundo real; a ineficiência do histórico das lições aprendidas, a dúvida em se estabelecer quais ações no ECiber podem ser consideradas como ações de guerra; e a dependência cada vez maior da Internet por parte de todos os usuários.

Indubitavelmente, conforme analisado no decorrer do trabalho, a SegCiber vem se tornando, dia após dia, a grande preocupação de todos os usuários do ECiber, principalmente em razão do avanço das ameaças nesse novo campo de batalha.

Em decorrência do modo de atuação dos atacantes, uma das principais vulnerabilidades do ECiber foi representada como sendo a própria infraestrutura de TIC. Diante dessa fragilidade torna-se fundamental que, desde o usuário comum, as grandes empresas, as instituições financeiras, até os setores governamentais e os militares, todos assumam a questão da SegCiber como prioritária.

Assim, como visto, tal prioridade deve vir a consolidar-se com a adoção de uma

política comum para SegCiber, que procure reunir os interesses dos diversos atores e fortalecer as defesas contra as ameaças no mundo virtual. Com o propósito de consolidação da SegCiber, apontou-se três princípios a serem observados na busca de tal objetivo: a governança, o gerenciamento de risco e a inclusão.

Outro ponto importante que foi tratado consiste no fato de que a manutenção dos sistemas computacionais *(hardware e software)*, bem como a segurança das redes que interconectam todos os sistemas no ECiber tornem-se motivo de preocupação por parte de todos os usuários. Por conseguinte, a implementação eficaz de medidas de SegCiber se dará por meio de alguns aspectos operacionais necessários, como por exemplo: a agilidade e a iniciativa para se contrapor aos atacantes rapidamente , a reduzição da neutralidade de alguns atores; e a implementação da gestão de risco.

Analisou-se o caso do *ransomware WannaCry,* que utilizando uma falha do sistema Windows combinado com um método de propagação de um *worm*, infectou milhares de computadores ao redor do mundo. Constatou-se que são diversas as possibilidades de ataques no ECiber e que a falta de prioridade que os usuários dão à SegCiber facilita para o sucesso das ações por atacantes.

Os estudos referentes ao caso *WannaCry* evidenciaram que a resposta das equipes de SegCiber ao redor do mundo demonstrou ser crescente a preocupação com a manutenção da segurança no Eciber. Atualizações de segurança para sistemas operacionais descontinuados foram rapidamente disponibilizadas a todos usuários que se encontravam expostos à infecção e políticas de segurança começaram a ser divulgadas com maior intensidade entre usuários.

Os Estados precisavam estar permanentemente preocupados com salvaguardar as ferramentas que utilizam para atingirem seus propósitos políticos e militares, de modo a evitarem vazamentos como o que permitiu o emprego do *WannaCry*, assim como os demais usuários da rede devem se esforçar para garantirem maior SegCiber.

Sem dúvida, o estabelecimento da SegCiber como prioridade por parte dos usuários garantirá que tais ferramentas tenham sucesso, de forma a impedir que ameaças como o *WannaCry* desestabilizem diversos setores da sociedade, prejudicando pessoas e serviços, possibilitando, inclusive, em virtude dos sistemas afetados, o surgimento de um eventual conflito real.

Em suma, com base em todos os aspectos relacionados ao novo campo de batalha da Guerra Cibernética, levando-se em consideração os recursos disponíveis para que os atacantes possam realizar suas ações e as medidas de Segurança Cibernética que podem ser adotadas por todos os usuários que utilizam o Espaço Cibernético, pode-se chegar à seguinte conclusão: certamente o atacante tem muitos méritos por conta do seu elevado conhecimento e em face do modo como emprega todos os recursos que se encontram a sua disposição para realização de um ataque, mas é notório que a influência do usuário, seja expondo as vulnerabilidades dos sistemas, seja deixando de observar as recomendações de SegCiber, permite que o atacante tenha sucesso em suas ações.

Ante o exposto, conclui-se que a resposta ao questionamento apresentado no princípio da presente dissertação, o qual motivou este estudo, no sentido de buscar elucidar quem seria o responsável pelo sucesso das ações no espaço cibernético, isto é, se seria o atacante bem preparado ou o defensor que deixa de adotar as medidas necessárias para evitar que o ataque realizado seja bem-sucedido, consiste na combinação do atacante bem preparado com o defensor que deixa alguma vulnerabilidade exposta. Sem dúvida, caso o defensor adote todas as medidas necessárias, por mais bem preparado que o atacante esteja, ele encontrará uma grande dificuldade para transpor as barreiras impostas pelo defensor, sendo a exposição da vulnerabilidade fator determinante para o sucesso das ações do atacante preparado e a SegCiber um fator determinante na contenção do atacante.

## REFERÊNCIAS


**Anatomy of targeted attacks with smart malware.** Disponível em <http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=4&sid=72a9dda0-d18e-406a-94ac-1b9223470e3c%40sessionmgr4007&hid=4001 >**.** Acesso em 26 de maio de 2017.

ASSANGE, Julien. **Wikileaks**. Disponível em < https://wikileaks.org/What-is-Wikileaks.html >. Acesso em 7 de jul. de 2017.

**Botnet spoofing - fighting botnet with itself**. Disponível em < http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=8&sid=72a9dda0-d18e-406a-94ac-1b9223470e3c%40sessionmgr4007&hid=4001 >. Acesso em 26 de maio de 2017.

BARANIUCK, Chris – BBC Tecnologia – **Como uma descoberta acidental interrompeu o "sequestro" de computadores em grandes empresas ao redor do mundo**. Disponível em < http://www.bbc.com/portuguese/geral-39903918 >. Acesso em 09 de jul. de 2017.

BÉLGICA. RAND EUROPE. **A focus on cybersecurity**. Bruxelas, 2016. Disponível em: < https://www.rand.org/pubs/corporate_pubs/CP871.html>. Acesso em 09 jun. 2017.

BRASILIANO, Antonio C. R., PhD. **Coletânea de Riscos Cibernéticos.** São Paulo, Interisk, 2017. Disponível em <https://www.brasiliano.com.br/coletanea-riscos-ciberneticos>. Acesso em 30 de junho de 2017

**Cambridge Dictionary.** Disponível online em < http://dictionary.cambridge.org/pt/dicionario/ingles-portugues/ >. Acesso em 13 de jul. de 2017.

**Cartilha de Segurança para Internet** – CERT.BR. Disponível em < https://cartilha.cert.br/malware/ >. Acesso em 13 de jul. de 2017

CLARKE, Richard A., KNAKE, Robert K., **GUERRA CIBERNÉTICA: a próxima ameaça à segurança e o que fazer a respeito.** Rio de Janeiro, Brasport, 2015.

CUCU, Paul. **How every cyber attack works - A full list. Heimdal Security**, fev. 2017. Disponível online em: < https://heimdalsecurity.com/blog/cyber-attack/ >**.** Acesso em 28 de maio de 2017.

Defending the digital frontier. **The Economist – Special Report Cyber Security**, jul. 2014. Disponível em < https://www.economist.com/news/special-report/21606416-companies-markets-and-countries-are-increasingly-under-attack-cyber-criminals >. Acesso em 28 de maio de 2017.

**Detecting Hidden Logic Bombs in Critical Infrastructure Software**. Disponível em < http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=14&sid=72a9dda0-d18e-406a-94ac-1b9223470e3c%40sessionmgr4007&hid=4001 >. Acesso em 26 de maio de 2017.

EUA. The Departament of Defense. **THE DoD CYBER STRATEGY**. Washington, DC 2015. Disponível em < http://www.dtic.mil/doctrine/doctrine/other/dod_cyber_2015.pdf>. Acesso em 16 de jun. de 2017.

MACAFEE. McAfee Labs – **Futher Analysis of WannaCry Ransomware** – May 14,2017. Disponível online em < https://securingtomorrow.mcafee.com/mcafee-labs/analysis-wannacry-ransomware/ >. Acesso em 09 de jul. de 2017..

REINO UNIDO. The Royal Institute of International Affairs. **2010-11-On Cyber Warfare - A Chatham House Report**. Disponível em < https://www.chathamhouse.org/publications/papers/view/109508>. Acesso em 21 de maio de 2017.

REINO UNIDO. The Royal Institute of International Affairs. **Cyberspace and the National Security of the United Kingdom - Treats and Responses - A Chatham House Report**. Disponível em <https://www.chathamhouse.org/publications/papers/view/109020>. Acesso em 26 de maio de 2017.

SYMANTEC a. **Internet Secure Threat Report (ISTR) vol. 22. abr2017.** Disponível em < https://www.symantec.com/security-center/threat-report> . Acesso em 17 de jun. de 2017

SYMANTEC b. **Ransom.Wannacry** – Symantec Security Response. Maio 2017. Disponível em < https://www.symantec.com/security_response/writeup.jsp?docid=2017-051310-3522-99 >. Acesso em 7 de jul. de 2017.

# ANEXO A

TIPOS DE CÓDIGOS MALICIOSOS

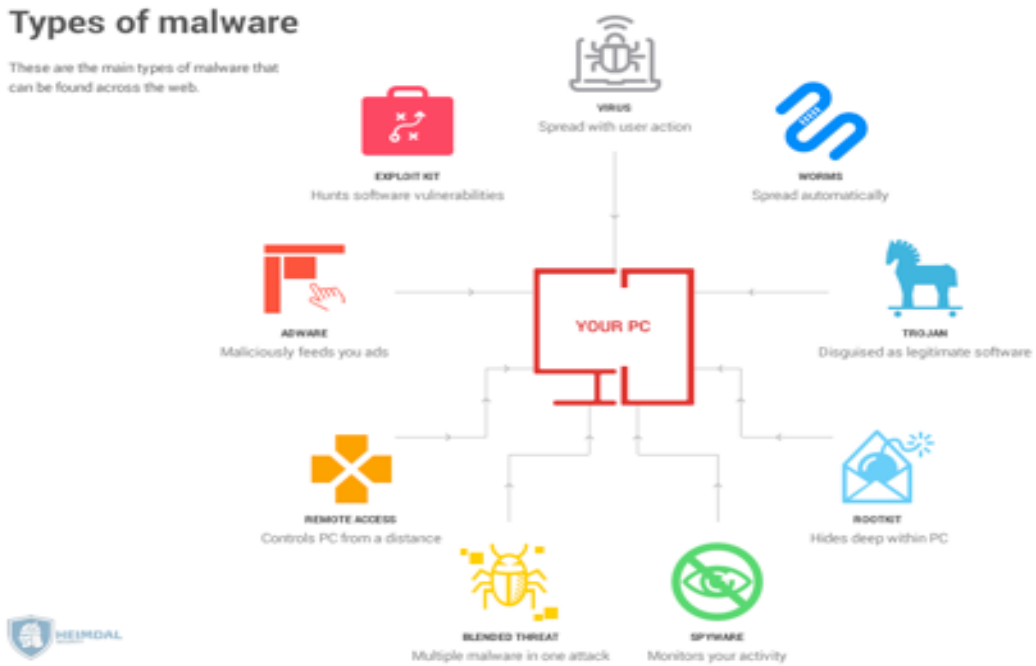


FIGURA 1 – Tipos de *malware* presentes no ECiber
Fonte: HEIMDAL SECURITY, 2017

# ANEXO B

DADOS ESTATÍSTICOS

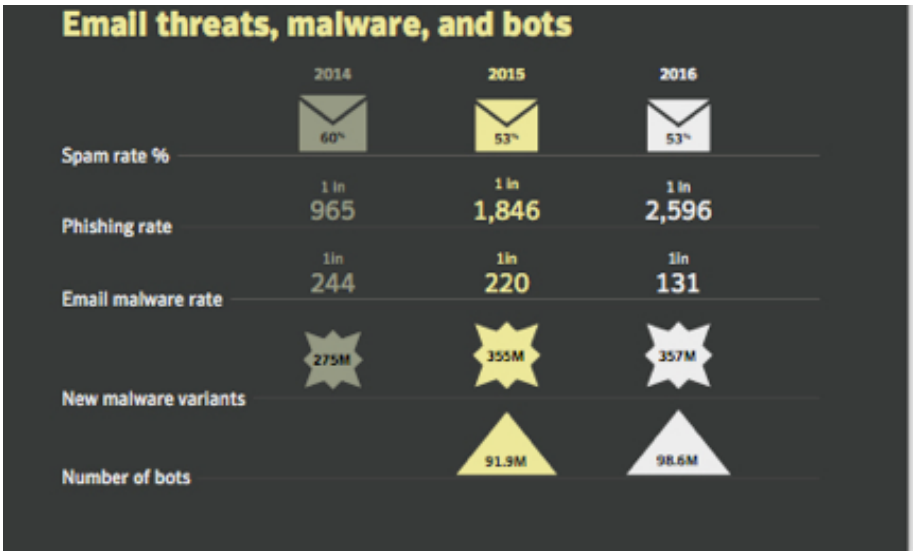


FIGURA 2 – Códigos maliciosos enviados por e-mail de 2014 a 2016.
Fonte: SYMANTEC, ITSR vol. 22 p.9, 2017.

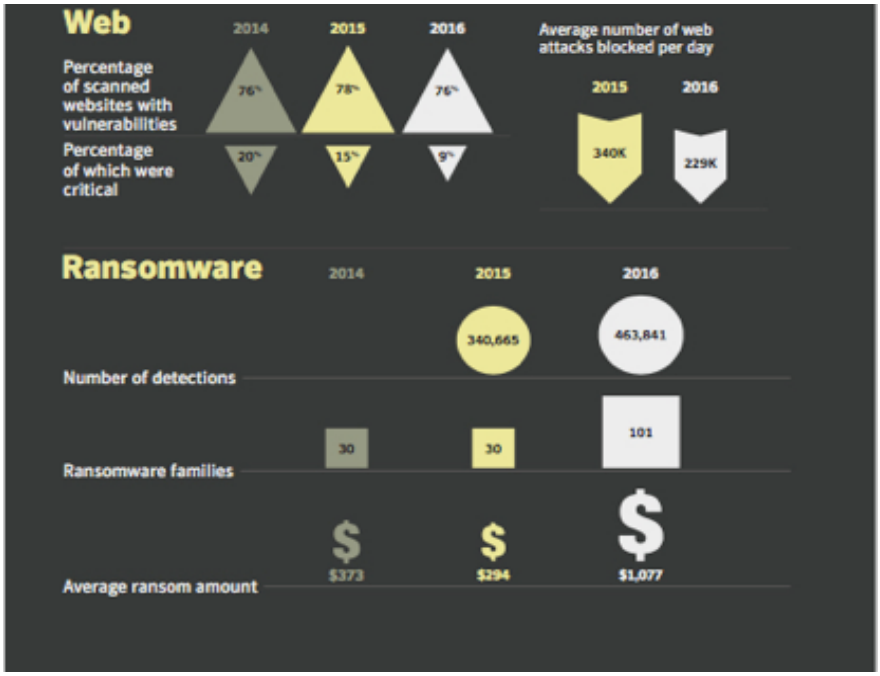


FIGURA 3 – Dados sobre o emprego do *ramsomware* entre 2014 e 2016.
Fonte: SYMANTEC, ITSR vol. 22 p.10, 2017.