**ACADEMIA MILITAR DAS AGULHAS NEGRAS**
**ACADEMIA REAL MILITAR (1810)**

**ALEXANDER DAMITZ PINHEIRO**

# A INFLUÊNCIA DA INTERNET DAS COISAS PARA A GUERRA CIBERNÉTICA

**Resende**
**2018**

**ALEXANDER DAMITZ PINHEIRO**

# A INFLUÊNCIA DA INTERNET DAS COISAS PARA A GUERRA CIBERNÉTICA

Trabalho de Conclusão de Curso apresentado à Academia Militar das Agulhas Negras como parte dos requisitos para a Conclusão do Curso de Bacharel em Ciências Militares, sob a orientação do Cap Com Nelcinei de Freitas Valente.

**COMISSÃO AVALIADORA**

**Cap Com Nelcinei de Freitas Valente – Orientador**

**Resende**

**2018**

À minha família, em especial aos meus pais, Alexandre Pinheiro e Luciane Damitz Pinheiro, responsáveis pelos valores e ensinamentos que hoje trago comigo e pelo apoio incondicional prestado até o momento; e ao meu irmão, Luciano Damitz Pinheiro, que sempre esteve ao meu lado nos momentos mais difíceis da formação.

## AGRADECIMENTOS

Ao meu Pai, Alexandre Pinheiro, Capitão do Exército, o qual me auxiliou de maneira ímpar na escolha do tema e na conclusão desta pesquisa, abdicando do seu tempo para que pudesse passar o máximo dos seus conhecimentos e aprendizados, fornecendo assim as melhores ferramentas para a realização do trabalho. Sempre motivando pelo exemplo.

Ao meu orientador Capitão Valente, pelo tempo desprendido e dedicado em prol da conclusão deste trabalho, bem como pelos seus conhecimentos que, com muita boa vontade, foram a mim transmitidos e que de muito auxiliaram a minha pesquisa. A todos os professores e instrutores que, de uma forma geral, retiraram minhas dúvidas e contribuíram com seus conhecimentos para o resultado final deste trabalho.

## RESUMO

Com o avanço da tecnologia da informação e comunicações (TIC) aliado a popularização da internet, pessoas estão constantemente acrescentando coisas a ela e fazendo com que essas coisas interajam de uma maneira ligeiramente automática. A Internet das Coisas (IoT) visa esta interoperabilidade. No entanto, também esta sujeita a ação de elementos mal intencionados, os quais podem comprometer um sistema informatizado. Consequentemente isso influencia sensivelmente a Guerra Cibernética (GC) no que tange os métodos de ataque e defesa. Com a presença desses dispositivos no âmbito do Exército Brasileiro (EB), é importante que as suas implicações sejam observadas por ocasião do planejamento das operações. Sendo assim, verificou-se a necessidade de analisar a influência da IoT para a GC no EB, com foco nas funções de combate, valendo-se do apoio de livros, artigos científicos, publicações e trabalhos relacionados ao assunto. Este trabalho de conclusão de curso apresenta alguns conceitos importantes a respeito dos assuntos acima citados, bem como propõe uma análise da presença de elementos de IoT no âmbito do EB, com foco nas suas implicações sobre a GC inserida no planejamento das funções de combate.



**Palavras-chave:** Internet das coisas, guerra cibernética, exército brasileiro, funções de combate.

**ABSTRACT**

With the advancement of information and communication technology (TIC) coupled with the popularization of the internet, people are constantly adding things to it and making those things interact in a slightly automatic way. The Internet of Things (IoT) aims at this interoperability. However, it is also subject to the action of malicious elements, which can compromise a computerized system. Consequently, this significantly influences the Cyberwarfare (GC) with regard to methods of attack and defense. With the presence of these devices within the scope of the Brazilian Army (EB), it is important that their implications are observed when planning operations. Therefore, it was verified the need to analyze the influence of IoT to the GC in the EB, focusing on the combat functions, using the support of books, scientific articles, publications and related works. This course conclusion paper presents some important concepts regarding the above mentioned subjects, as well as proposes an analysis of the presence of IoT elements within the scope of the EB, focusing on its implications on the GC inserted in the planning of combat functions.

**Key words:** Cyberwafare, internet of things, brazillian army, combat functions.

## LISTA DE FIGURAS

**LISTA DE TABELAS**

## LISTA DE ABREVIATURAS

| | |
|---|---|
| $C^2$ | Comando e Controle |
| DoS | *Denial-of-Service* |
| EB | Exército Brasileiro |
| GC | Guerra Cibernética |
| IDS | Sistema de Detecção de Intrusos |
| IERC | *European Research Cluster on the Internet of Things* |
| IoT | Internet das Coisas |
| IPS | Sistema de Prevenção de Intrusos |
| ITIL | *Information Technology Infrastructure Library* |
| ITU | *International Telecommunication Union* |
| $M^2$ | Movimento e Manobra |
| M2M | *Machine to Machine* |
| MIT | *Massachusetts Institute of Technology* |
| OWASP | *Open Web Applicantion Security Project* |
| RFID | *Radio Frequency Identification* |
| SI | Segurança da Informação |
| SIC | Segurança da Informação e Comunicação |
| SSL | *Secure Socket Layer* |
| TI | Tecnologia da Informação |
| TIC | Tecnologia da Informação e Comunicações |
| TLS | *Transport Layer Security* |
| VPN | *Virtual Private Network* |

**SUMÁRIO**

# 1 INTRODUÇÃO

O tema deste trabalho de conclusão de curso versa sobre a influência que a inserção de dispositivos ligados a Internet das Coisas (do inglês, *Internet of Things* – IoT) pode exercer sobre a GC, campo de pesquisa inserido na área de redes de computadores, com foco nas consequências para o EB, em especial nas funções de combate.

Atualmente, aplicações desenvolvidas para máquinas, acionam outros dispositivos sem que necessariamente haja uma mecânica com um usuário. Esta realidade presente na internet é responsável pela geração de um volume de dados bastante significativo. A previsão para 2020 é que hajam mais de 50 bilhões de dispositivos conectados a rede mundial de computadores (CISCO, 2011).

Esse fluxo de dados é muitas vezes descontrolado, possibilitando que, em muitos casos, elementos mal intencionados explorem vulnerabilidades em sistemas computacionais causando, entre outras coisas, negação de serviços e roubos de informações sensíveis.

A Internet das Coisas, como o próprio nome diz, significa agregar, associar e fazer comunicar entre si todos os objetos e coisas em uma rede de computadores, particularmente a Internet. De acordo com o livro de Shelby e Bormann (2009), podemos conectar *smartphones*, sensores pessoais, automação predial, logística, transporte, medidores de energia elétrica inteligente, infraestrutura de redes, entre outros (SHELBY; BORMANN, 2009).

A Cisco define IoT como a união de pessoas, processos, dados e tudo que pode tornar as conexões em rede mais relevantes e valiosas.. A IoT transforma informações em ações que criam novos recursos, experiências mais ricas e oportunidades econômicas sem precedentes para empresas, indivíduos e países. Isso faz com que rede torne-se ubíqua, onipresente ou pervasiva (que pode ser encontrado em todos os lugares). Ela está tão integrada e natural ao cotidiano que os usuários não preocupam-se com o que acontece nos bastidores da internet, porém todo profissional de TI (Tecnologia da Informação) precisa ter essa noção (CISCO, 2014).

A GC é entendida como uma série de ações para uso ofensivo e defensivo de sistemas de comunicações em rede para negar, explorar, corromper ou destruir valores do adversário. Tem a finalidade de obter vantagens tanto na área militar quanto na área civil (BRASIL,2007). Portanto, é fortemente influenciada pelo aumento de dispositivos conectados a rede e pelo tráfego massivo de dados nessas redes. Isto traz claras consequências à forma como o EB se prepara e planeja a execução de suas ações, tendo por base as suas funções de combate como forma de solucionar os problemas militares.

Em vista disso, este trabalho visa identificar as possíveis vulnerabilidades e as consequências da inclusão de dispositivos IoT no Exército, relacionados com os aspectos da GC.

Seu estudo é relevante para o meio militar, uma vez que o aprofundamento desses conhecimentos significa um aperfeiçoamento na prevenção e na segurança de ativos de rede, administradores e usuários dos serviços de rede corporativos e operacionais do EB e, consequentemente, em um melhor emprego dos dispositivos de IoT na Força Terrestre. Tais ações objetivam um melhor preparo das técnicas de proteção utilizadas pela GC, favorecendo o êxito da Força Terrestre, independentemente do cenário em que esteja atuando.

## 1.1 PROBLEMÁTICA

Com o alto volume de dados, inclusive pessoais, sendo trafegados e analisados na rede, a autenticação de usuários, o controle de acesso e a criptografia de dados devem ser aprimoradas para evitar que informações sejam comprometidas, ou, ainda, que os sistemas sejam invadidos. No EB, pelo fato da temática ainda ser bastante recente, ainda não existem pesquisas específicas que tratem a respeito da IoT no âmbito da GC como um fator primordial a ser levado em conta no planejamento de qualquer operação, com fins à prevenção de problemas de SIC no decurso do emprego desses meios.

Assim, é oportuno problematizar a questão: quais as peculiaridades dos ativos de IoT com relevância para emprego operacional militar frente a um cenário cibernético com limites irrestritos de atuação?

## 1.2 OBJETIVOS

Os objetivos do trabalho a ser realizado podem ser assim descritos:

### 1.2.1 Objetivo geral

O objetivo geral deste trabalho será realizar um estudo sobre as consequências que os dispositivos componentes da IoT possam trazer para a GC dentro do EB

### 1.2.2 Objetivos específicos

Com a finalidade de viabilizar a consecução do objetivo geral deste trabalho, foram formulados os objetivos específicos, abaixo relacionados, que permitirão o entendimento dos assuntos apresentados neste estudo:

a) descrever os aspectos gerais sobre GC;
b) apresentar o conceito e os princípios da GC;
c) apresentar de maneira breve, exemplos de ferramentas de ataque e de defesa usada pela GC;
d) definir o conceito de IoT;
e) apresentar suas aplicações atuais e aspectos de segurança relevantes;
f) apresentar e definir as Funções de Combate dentro do EB;
g) apresentar o ITIL;
h) analisar a influência da IoT para a GC;
i) propor situações em que a IoT influencie a GC no âmbito das Funções de Combate.

## 1.3 JUSTIFICATIVA

A conexão de qualquer ativo computacional em uma rede de computadores permite a identificação do tráfego deste ativo e, consequentemente, torna possível a reconstituição dos dados por qualquer elemento que esteja vigiando a rede. Tratando-se de internet, onde o “o mundo” navega, a ação deliberada de não empregar recursos de segurança expões tráfegos restritos e privados à exploração por elementos não autorizados. Apesar de a maioria dos usuários aceitar esse risco, não se pode levar esse entendimento para os processos de tomada de decisão da Força Terrestre.

Portanto, cresce de importância a adoção de medidas para mitigar os riscos de exploração cibernética e aumentar a segurança no emprego de tais dispositivos.

## 1.4 METODOLOGIA

Para essa monografia foi utilizado o método da pesquisa bibliográfica que é definida como o tipo de pesquisa que "procura explicar um problema a partir de referências teóricas, publicadas em livros, dissertações e teses" (CERVO, A. et. al, 2007, p. 60).

Foram realizadas buscas em livros atualizados, artigos científicos e trabalhos acadêmicos sobre pesquisas realizadas nas instituições de ensino nacionais e internacionais. Os relatórios e dados com previsões de especialistas na área de tecnologia, informação, inovação e economia foram obtidos de fontes de instituições, órgãos regulamentadores e empresas especializadas nos assuntos. Além disso, foram usados manuais do EB e artigos científicos para conceituar tópicos importantes do assunto tratado neste trabalho.

## 1.5 ORGANIZAÇÃO DO TRABALHO

O presente trabalho será confeccionado em quatro capítulos sendo estes:

Capítulo 1: Breve introdução incluindo apresentação da problemática, dos objetivos, da justificativa, da metodologia e delimitação do problema;

Capítulo 2: Contendo referencial teórico sobre a IoT, a GC, ITIL e as funções de combate;

Capítulo 3: Sobre a influência da IoT sobre a GC em aspectos gerais no âmbito das funções de combate;

Capítulo 4: Conclusões e recomendações.

# 2 FUNDAMENTAÇÃO TEÓRICA

A fundamentação teórica objetivou trazer uma breve compreensão dos conceitos ligados a: GC, seus princípios e principais aspectos; IoT, seu surgimento, funcionamento e aspectos relevantes; as funções de combate do EB de modo a relacioná-las com os conceitos anteriores; e o ITIL como forma de guiar o planejamento nas funções de combate.

## 2.1 ASPECTOS GERAIS SOBRE GUERRA CIBERNÉTICA

Nos últimos anos a sociedade foi bastante beneficiada pela evolução tecnológica, a qual possibilitou uma integração ainda maior entre ambientes diferentes, sejam eles de trabalho, doméstico e comercial. Sobretudo, também trouxe inúmeros problemas relacionados a segurança da informação que trafega ou é armazenada no meio digital (BRAGA, 2011).

O ser humano em sua evolução utilizou diversos meios para representar o mundo real. Para realizar cálculos e contagens, usou os dedos das mãos, cordinhas com nós, ábacos e outros, até chegar às máquinas mecânicas (PACITTI, 2002, p. 87). Com esta evolução crescente, ameaças também surgiram para explorar estas novas descobertas e a SI deve estar muito bem implementada e massificada na mente dos usuários e profissionais de TI, a fim de evitar a ocorrência de incidentes que possam afetar a todos.

A ideia de digitalizar processos e informações se deu a partir da década de 30 do século XX, por meio de pesados investimentos norte-americanos em suas Universidades na área de eletrônica e computação, possibilitando a produção de calculadoras eletromecânicas, as quais foram inspiração para os computadores produzidos posteriormente na década de 50. Destaca-se a calculadora ENIAC (*Eletronic Numerical Integrator And Calculator*), que funcionava por meio de válvulas, uma verdadeira revolução para a época, sendo até mesmo considerada pelo exército americano com o *top secret* (WEIK, 1961).

Nesse momento, segundo Pacitti (2002, p. 90), surgiu o termo “cibernética”, popular nas décadas de 40 e 50, a fim de relacionar processos de comunicação e controle entre os seres vivos e as máquinas. No entanto, esse termo caiu em desuso mais tarde com o desenvolvimento da informática, inteligência artificial e robótica e demais teorias que antes eram conhecidos por cibernética, sendo assim, o conceito de informática, imperou sobre o termo cibernética.

Segundo Raphael Mandarino, em seu livro Segurança e Defesa do Espaço Cibernético, esse o termo foi resgatado e é amplamente utilizado, caracterizando o espaço cibernético como o conjunto de pessoas, empresas, equipamentos e interconexões dos sistemas de informação e das informações que por eles trafegam (MANDARINO, 2010, p. 41).

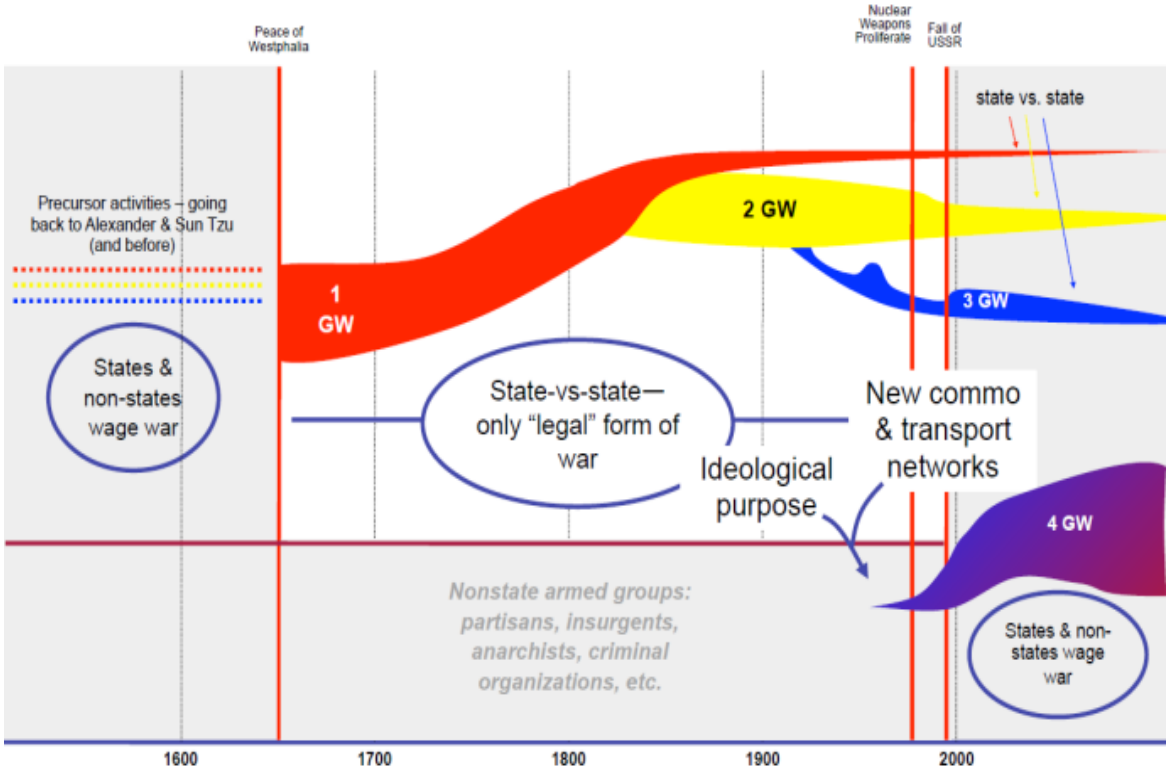


Figura 1: Linha do tempo e evolução dos conflitos

Fonte: (NIELSEN,2010)

A Figura 1 representa um gráfico da evolução dos conflitos em paralelo com a evolução tecnológica em TI. É possível identificar que já no começo do século XXI os conflitos já começavam a envolver redes de computadores, como exemplo, a Guerra Fria com a corrida espacial

Com o então advento dos computadores e a criação da internet, e também pela evolução no nível das linguagens de programação, houve uma popularização no uso da informática, pois proporcionou a redução de custos e dos meios necessários para diversas atividades. Além disso, foi possível a interconexão em nível global, ou seja, o fim das fronteiras no espaço cibernético (BRAGA, 2011).

Sobretudo, todas essas inovações mudaram a abordagem na área de segurança. Anteriormente, a preocupação era eminentemente física em relação aos ativos, era necessário apenas que o ambiente fosse isolado, controlado e fosse dotado de redundâncias no que se

refere a fonte de energia. Hoje, com a facilidade de disseminação de conhecimentos na área de informática, aumentou-se sensivelmente as vulnerabilidades de segurança no meio digital, pois permitiu que qualquer indivíduo possa acessar documentos e tutoriais que ensinam como realizar ataques e fazer explorações com o fim de obter vantagens, normalmente financeiras.

### 2.1.1 Guerra Cibernética

A Guerra Cibernética é uma modalidade de guerra incorporada recentemente à Doutrina Militar na qual o espaço cibernético e tecnologias de informação são o cenário principal. Ao contrário da guerra convencional, os conflitos não ocorrem fisicamente, mas sim no mundo virtual, sem que haja o contato propriamente dito entre os litigantes.

A lógica do espaço cibernético está vinculada a aspectos técnicos e não geográficos. Portanto ações cibernéticas podem percorrer grandes distâncias, por diversos territórios e em pouco tempo, dificultado o rastreamento e a identificação da origem e autoria de um ataque cibernético.

A fim de estabelecer um conceito norteador para essa recente modalidade, tendo em vista as diversas definições existentes hoje, será considerado o definido pelo Ministério da Defesa através do Manual MD35-G-01:

> Conjunto de ações para uso ofensivo e defensivo de informações e sistemas de comunicações 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).

Corroborando a definição do Ministério da Defesa, será usada também a definição mais recente adotada pelo Exército Brasileiro no Manual EB70-MC-10.232:

> GUERRA CIBERNÉTICA – corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar capacidades de C2 ao adversário, explorá-las, corrompê-las, degradá-las ou destruí-las, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de TIC para desestabilizar ou tirar proveito dos sistemas de informação do oponente e defender os próprios Sist Info. Abrange, essencialmente, as ações cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação às TIC (BRASIL, 2017, p. 18).

Sobretudo, também é importante definir o conceito de Segurança da Informação e Comunicações (SIC), tendo em vista que sua finalidade é assegurar os princípios da segurança da informação, ou seja, o objetivo das ações cibernéticas.

> Segurança da Informação e Comunicações (SIC) – ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e informações.
>
> Disponibilidade – propriedade segundo a qual a informação deve ser acessível e utilizável sob demanda por uma pessoa física ou por determinado sistema, órgão ou entidade.
>
> Integridade – propriedade segundo a qual a informação não deve ser modificada ou destruída de maneira não autorizada ou acidental.
>
> Confidencialidade – propriedade segundo a qual a informação não deve estar disponível ou ser revelada a pessoa física, sistema, órgão ou entidade não autorizados ou não credenciados.
>
> Autenticidade – propriedade segundo a qual a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física ou por um determinado sistema, órgão ou entidade (BRASIL, 2017, p. 19).

Na visão do EB, ainda conforme o definido no Manual EB70-MC-10.232 sobre GC, as capacidades operativas da GC são três: a proteção cibernética, o ataque cibernético e a exploração cibernética.

> • Exploração Cibernética – Ser capaz de conduzir ações de busca ou coleta nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados. Deve-se, preferencialmente, evitar que essas ações sejam rastreadas e sirvam para a produção de conhecimento ou para a identificação das vulnerabilidades desses sistemas.
> • Ataque Cibernético – Ser capaz de conduzir ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes de computadores e de comunicações do oponente.
> • Proteção Cibernética –Ser capaz de conduzir ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de guerra cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente (BRASIL, 2017, p.26).

As ações de exploração e ataque cibernéticos normalmente são atividades conjuntas, com o objetivo de controlar as informações, obter dados sensíveis e comprometer sistemas indispensáveis do inimigo, consequentemente prejudicando sua capacidade de combater. Todavia as ações defensivas de proteção cibernética usam procedimentos e dispositivos com o objetivo de se opor as medidas empregadas pelos oponentes.

### 2.1.2 Princípios da Guerra Cibernética

Além dos tradicionais princípios da guerra de grandes pensadores como Sun Tzu, Clausewitz, Lydell Hart e Caminha, foram elaborados por Parks e Duggan (2001), oito princípios específicos de GC:

- Princípio do Efeito Cinético: A GC causa efeitos no mundo cinético;
- Princípio da Mutabilidade e Visibilidade: Não existem leis de comportamento imutáveis no Mundo Cibernético;
- Princípio do Disfarce: Alguma entidade no Mundo Cibernético possui a autoridade, acesso ou habilidade necessários para pôr em prática qualquer ação que um atacante deseje realizar; o objetivo do atacante é assumir a identidade dessa entidade, de alguma forma;
- Princípio da Dualidade do Armamento: As ferramentas da GC são de natureza dual;
- Princípio da Compartimentação: Tanto o atacante, como o defensor de um sistema, controlam uma pequena parcela do Ciberespaço que utilizam;
- Princípio da Usurpação: Quem controlar a parte do Ciberespaço que o oponente utiliza, pode controlar o oponente;
- Princípio da Incerteza: O Ciberespaço não é consistente, nem confiável; e
- Princípio da Proximidade: limitações físicas de distância e espaço não se aplicam ao Mundo Cibernético.

### 2.1.3 Ferramentas de Ataque

Devido ao avanço tecnológico e a difusão das redes de computadores, os ataques cibernéticos tornaram-se comuns, complexos e perigosos. Consequentemente evidencia-se a importância de se fazer uma análise a respeito das ferramentas que podem ser utilizadas a fim de atingir uma infraestrutura digital.

#### 2.1.3.1 *Denial-of-Service* (DoS)

Os ataques de negação de serviço são feitos com o propósito de tornar o sistema indisponível através do consumo total da largura de banda de uma rede ou por indisponibilidade de recursos. O ataque consome toda a capacidade operativa do sistema, ou seja, as requisições dos usuários válidos deixarão de ser respondidas em tempo oportuno.

Um exemplo disso é que com o equipamento apropriado, pode-se enviar uma grande quantidade de trafego aleatório na mesma frequência de um roteador sem fio, fazendo com que a rede fique indisponível (DUARTE, 2003).

Portanto, a gravidade deste ataque está ligada ao tempo no qual o sistema ficou fora do ar, gerando perda de credibilidade e trabalho físico em identificar e reagir a essa modalidade de ataque.

#### 2.1.3.2 Engenharia Social

A engenharia social é uma forma de ataque que usa a persuasão e o poder da influência para que um indivíduo se passe por alguém que na verdade ele não é. Como resultado, o indivíduo pode utilizar as pessoas para obter informações e dados sem mesmo usar a tecnologia (MITNICK; SIMON, 2003).

A fim de diminuir a probabilidade de ser uma vítima desse tipo de ataque é imprescindível que haja uma constante divulgação da política de segurança da organização, palestras sobre o assunto, cursos de capacitação, regras severas de segurança e monitoramento e filtragem do conteúdo que trafega na rede (PEIXOTO, 2006).

#### 2.1.3.3 Varredura de Rede

É a utilização de sistemas que realizam varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador (ALECRIM, 2013).

#### 2.1.3.4 Interceptação de Conexão

São dispositivos ou programas de computador utilizados para capturar e armazenar dados que estão trafegando em uma rede de computadores. Pode ser usado por um invasor para capturar informações sensíveis (como senhas de usuários), em casos onde estejam sendo utilizadas conexões inseguras, ou seja, sem criptografia (DUARTE, 2003).

### 2.1.4 Ferramentas de Defesa

Como uma via de mão dupla, com o surgimento dos ataques cibernéticos aumentaram as buscas por ferramentas que barrassem ou, pelo menos, mitigassem tais problemas. Com isso, foram criados diversos meios de proteção frente a esses novos desafios a fim de proteger a infraestrutura digital de empresas e nações. A seguir serão apresentadas algumas dessas ferramentas

#### *2.1.4.1 Firewall*

Conforme Alecrim (2013), o *Firewall* é somente uma camada da segurança, é necessário utilizá-lo com outra solução, de acordo com a necessidade do que deve ser protegido. A sua missão consiste basicamente em bloquear tráfego de dados indesejados e liberar acesso de acordo com suas políticas de segurança, como mostra a Figura 2.

É baseado em *hardware* ou *software*, o qual analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas de acordo com regras pré-definidas. (ALECRIM, 2013)


Figura 2: Exemplo de funcionamento de um Firewall
*Fonte: (ALECRIM, 2013)*

### 2.1.4.2 Sistema de Detecção de Intrusos (IDS)

É um dos elementos imprescindíveis em um sistema de segurança. Sua função é monitorar uma rede ou um elemento presente nela, com o objetivo de encontrar comportamentos que sejam considerados maliciosos.

Existem dois tipos de IDS, o sistema passivo, na qual a anomalia é detectada, registrada e um alerta é enviado ao administrador do sistema; e o sistema reativo, no qual o IDS atua bloqueando a ameça tão logo ela seja observada (GASPAR; JESUS; SILVA, 2008).

### 2.1.4.3 Antivírus

É um programa de computador que detecta, evita e atua na neutralização ou remoção de programas mal-intencionados, como vírus e *worms*. (MICROSOFT, 2012)

### 2.1.4.4 Sistema de Prevenção de Intrusos (IPS)

É um sistema de segurança ativo que fornece segurança em todas as camadas do sistema. Funciona por meio de políticas e regras de tráfego de rede que são capazes de emitir alertas em caso de tráfego suspeito. Sobretudo, também permite que o administrador execute ações relacionadas ao alerta que foi dado (MORAES, 2012).

### 2.1.4.5 Rede Virtual Privada (VPN)

A VPN é uma rede que permite acesso privado de dados, através de uma rede pública já existente, de modo que a comunicação entre dois pontos se dá por meio de um túnel em que os dados ficam ocultos para elementos não autorizados (FRANZIN; ROSSI, 2000).

### *2.1.4.6 Anti-DDoS*

O *Anti-DDoS* é uma ferramenta de segurança criada com a finalidade de detectar e eliminar ataques de negação de serviço. Para isso, utiliza a análise comportamental, assinaturas de tráfego, limitação de taxa e outras técnicas que identificam e bloqueiam o tráfego malicioso (NETWORK BOX, 2011).

Uma das formas de funcionamento do *Anti-DdoS* está ilustrada na Figura 3, onde são realizadas análises em diversos níveis da conexão com o objetivo de identificar tráfegos maliciosos.

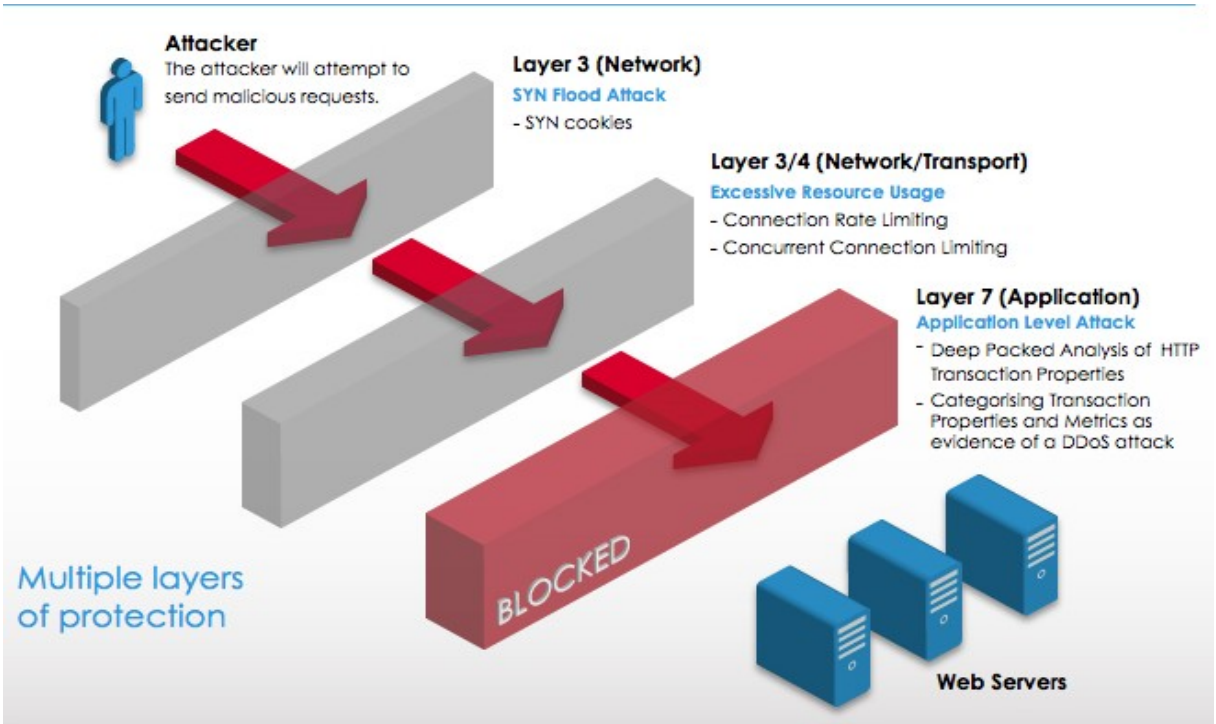


Figura 3: Anti–DDoS
*Fonte:(NETWORK BOX, 2011)*

## 2.2 INTERNET DAS COISAS

O termo IoT foi usado pela primeira vez em 1999 por Kevin Ashton e sua equipe do MIT (*Massachusetts Institute of Technology*), no momento da exposição de um projeto que mostrava o uso do RFID (*Radio Frequency Identification*) para monitorar produtos em uma linha de produção (ASHTON, 2009).

Atualmente a principal forma de comunicação da Internet é humana, e segundo Peter Waher, a IoT pode ser considerada como a futuro da Internet, a qual realiza aprendizagem máquina a máquina (M2M, do inglês *Machine to Machine*) fornecendo conectividade para tudo e todos (WAHER, 2015).

A primeira definição expõe um aspecto importante para a IoT, que é a necessidade de integração automática e por meio de qualquer rede a outros elementos.

Conforme Guillemin e Friess (2009) “A Internet das Coisas permite que pessoas e coisas estejam conectadas a qualquer hora, em qualquer lugar, com qualquer coisa, com qualquer outra pessoa e idealmente usando qualquer caminho/rede e qualquer serviço”.

A Figura 4 ilustra os impactos dessa conexão e integração entre dispositivos.

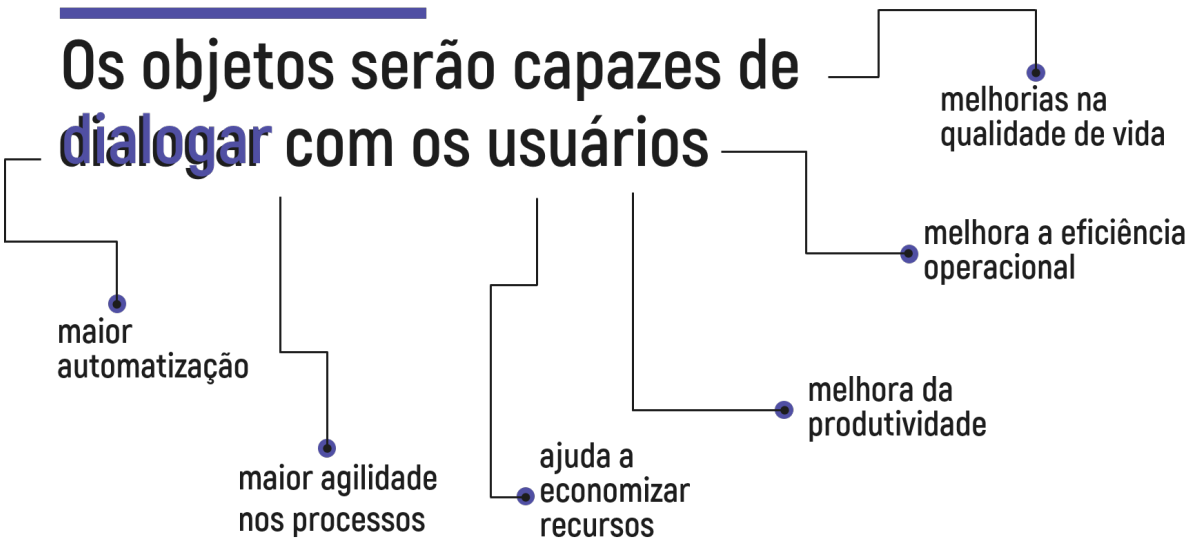


*Figura 4: Possibilidades da IoT*
*Fonte: (PROOF, 2017)*

Já segundo a IERC (*European Research Cluster on the Internet of Things*), a IoT pode ser definida por uma combinação de tecnologias e perspectiva sociais. Ou seja, a IoT é um fenômeno de um número constantemente crescente de objetos interconectados que está gradualmente mudando e melhorando a vida das pessoas (KRCO, 2012).

A União Internacional de Telecomunicações (ITU, do inglês *International Telecommunication Union*) define a IoT como:

> "Uma infraestrutura global para a sociedade da informação, permitindo serviços avançados através da interconexão (física e virtual) de coisas baseadas em tecnologias interoperáveis de informação e comunicação, existentes e em evolução" (ITU, 2012).

A premissa da IoT é fornecer uma conexão automática e segura, permitindo troca de dados entre dispositivos e aplicações do mundo real, momento no qual contará com inteligência suficiente para se comunicar e tomar decisões com objetos conectados a Internet. Consequentemente trará significativos benefícios pessoais, profissionais e econômicos a indivíduos, empresas e nações (FAN; CHEN, 2010).

### 2.2.1 Aplicações Atuais

A crescente popularização das redes de computadores e da Internet fez com que a IoT recebesse uma atenção especial, tendo em vista as inúmeras possibilidades de aplicações, empregos no cotidiano e o seu potencial para mudar a forma como a sociedade vive. A Figura 5 ilustra as possibilidades de aplicação da IoT em diferentes ambientes e meios.


Figura 5: Exemplos de aplicações de IoT
*Fonte: (NOKIA, 2016)*

Na Tabela 1 são apresentados alguns modelos de emprego da IoT, exemplificando algumas das diversas formas de aplicação e o seu impacto no cotidiano (MANYIKA et. al, 2015).

Tabela 1: Formas de emprego da IoT

| **Emprego** | **Exemplos** |
|---|---|
| Indústrias | Gestão de operações, manutenção preditiva. |

| | |
|---|---|
| Cidades | Segurança e saúde pública, controle de tráfego, gestão de recursos. |
| Humanos | Melhoria do bem-estar, monitorar e controlar doenças. |
| Varejo | Pagamento automático, otimização de leiaute, gestão inteligente de relacionamento com o consumidor. |
| Externa | Determinar rotas de logística, veículos autônomos, navegação. |
| Locais de Trabalho | Gestão de operações, manutenção de equipamentos, saúde e segurança. |
| Veículos | Manutenção baseada em condição, seguro reduzido. |
| Domicílio | Gestão de energia, automação de segurança e tarefas. |
| Escritórios | Redesign organizacional e monitoramento de trabalhador, realidade aumentada para treinamento. |

Fonte: The Internet of Things: Mapping the value beyond the hype (MANYIKA et. al, 2015, p. 3)

### 2.2.2 Aspectos de Segurança

O OWASP tem por objetivo expor ao mundo falhas e correções na área de segurança de *software*, cira rotineiramente uma lista levantando quais são os dez principais problemas no âmbito de segurança para IoT, sendo que o tratamento dado a cada problema tende a ser bastante prático. Além disso, serviu para nortear os aspectos de segurança relevantes da IoT para este trabalho (MAGALHÃES, 2016).

Para a construção da lista a Fundação baseou-se nos seguintes elementos: Dispositivos de IoT, a nuvem, aplicações para dispositivos móveis, ambientes e interfaces de rede, software, uso de criptografia e autenticação, segurança física e porta USB (OWASP, 2014).

Magalhães (2016), em sua Monografia, realizou a análise dos dez itens levantados pela OWASP. A partir dessa análise, temos:

1. Interfaces Web Inseguras: Algumas interfaces web apresentam falhas de segurança em ambas as faces, externa e interna. Por meio de credenciais fracas e enumeração de contas do sistema um indivíduo pode facilmente explorar a interface. Um exemplo disso é a requisição, pelo usuário, de uma nova senha, na qual o sistema não bloqueia o número de tentativas, possibilitando que sejam feitas diversas tentativas até que sejam encontrados usuário e senha válidos.

As formas mais comuns para impedir que hajam esses problemas são: modificar os valores padrões de usuário e senha, não expor credenciais no tráfego interno ou externo; impor políticas de uso de senhas fortes e limitar o número de tentativas de acesso.

2. Autenticação e Autorização Insuficientes: Para esse risco, os principais vetores de ataque são: uso de senhas fracas, credencias desprotegidas, método de recuperação de senhas medíocre ou inexistência de um eficaz controle de acesso. Essas vulnerabilidades podem ter originar-se desde interfaces web móveis até a nuvem, a qual é utilizada em inúmeras aplicações de IoT.

A fim de mitigar os riscos de um ataque bem-sucedido recomenda-se o uso de senhas fortes, revogação de credenciais vulneráveis, requisição de autenticação em aplicativos, dispositivos e servidores e a realização de auditorias nas credenciais cadastradas.

3. Serviços de Rede Inseguros: Nas redes nas quais os dispositivos de IoT estão inseridos, existem inúmeros serviços ativos. Tais serviços trazem vulnerabilidades que tornam fácil a exploração de dispositivos desprotegidos. Alguns exemplos são os ataques de negação de serviço e os de interferência na qual há perda ou corrupção de informações transmitidas.

A fim de diminuir a probabilidade de sucesso do atacante, torna-se imprescindível a verificação das portas dos serviços em atividade para que sejam habilitadas somente as que são realmente necessárias.

4. Falta de Transporte Criptografado: Os principais objetivos da criptografia para que haja transporte seguro de dados, são a garantia de que o tráfego de informações terá confidencialidade, integridade, autenticidade e não-repúdio. Quando algum desses objetivos é negligenciado podem ocorrer problemas na transmissão, incidindo em vazamento ou perda de dados. Um exemplo disso é a configuração de uma rede *wireless* sem a criptografia, a qual tornará todo o tráfego visível, possibilitando que um usuário não permitido consiga ter acesso ao conteúdo do que está trafegando.

Para evitar esse problema as informações não devem ser transmitidas na forma de texto claro e deverão sem empregados os protocolos *Transport Layer Security* (TLS) *Secure Socket Layer* (SSL).

5. Problemas de Privacidade: A Internet das Coisas gera uma quantidade significativa de dados através dos dispositivos que a compõem. Essas informações podem percorrer diversas redes e aplicativos até serem armazenadas na nuvem. Diante disso, surge a preocupação com a privacidade, tendo em vista que os dados fogem do escopo de controle do usuário.

A ausência de criptografia no transporte, autenticação insegura, serviços de rede mal configurados e excesso de dados colhidos podem servir como porta de entrada para ataques. A fim de garantir a privacidade das informações, devem ser verificados quais dados que estão sendo colhidos com foco na sua real necessidade, a forma de proteção e o controle de acesso a esses ativos. Sobretudo, deve haver total transparência ao usuário quanto ao que está sendo coletado.

6. Interface com a Nuvem Insegura: Na Internet das Coisas, inúmeros dados e informações de controle de dispositivos e sensores são armazenados na nuvem. Por esse motivo é imprescindível que o acesso a esses dados seja realizado de forma segura. Esse processo envolve controles de autenticação, criptografia e mecanismos que previnem falsificação de requisições a usuários no sistema da nuvem.

Portanto, deve ser feita a verificação de usuário e senhas e a sua troca de maneira periódica, além disso também é importante a implementação de proteção contra tentativas de força bruta com a detecção de requisições não usuais.

7. Interfaces Móveis Inseguras: Senhas e credenciais são utilizadas nas interfaces móveis, tendo em vista que muitos utilizam a nuvem para o armazenamento de dados. Ou seja, deve-se também utilizar mecanismos contra adulteração de aplicativos móveis e deve ser feita a restrição do uso de aplicativos apenas em sistemas operacionais móveis confiáveis, a fim de que não as informações de acesso não sejam comprometidas.

8. Configurações Insuficientes de Segurança: Esse problema decorre da insuficiência de meios para que o usuário possa adequar os controles de segurança a realidade que está inserido. Os vetores de ataque se originam na ausência de criptografia, falta de autenticação em dois fatores, inexistência de controle de acesso e desconhecimento do usuário. Nesse caso, cresce de importância a separação dos grupos de usuários, administrativos e regulares, uso de criptografia dos dados armazenados e trafegados, uso de políticas de senhas fortes, disponibilização de *logs* de acesso, notificações aos usuários e conscientização sobre o compartilhamento de informações de acesso em meios inseguros.

9. *Softwares* e *Firmwares* Inseguros: As atualizações de softwares e *firmwares* são imprescindíveis para a correção de falhas de segurança, no entanto a negligência ou a impossibilidade da realização dessa tarefa traz um grande problema aos dispositivos e sistemas da IoT, pois podem, por exemplo, disponibilizar em código aberto informações sensíveis de uma atualização, como credenciais, tal falha pode ser verificada com editores hexadecimais que verificam os dados binários do dispositivo.

A fim de mitigar esses riscos, é importante realizar as atualizações através de meios confiáveis, com o uso de funções *hash* e de *boot* seguro nos dispositivos, por exemplo.

10.Segurança Física Insuficiente: O acesso ao dispositivo abre uma janela para ataques e explorações sem fronteiras. Com o intuito de barrar esse tipo de método, devem ser aplicadas técnicas para dificultar o acesso a esses ativos. Para isso, é imprescindível que os dados armazenados estejam cifrados, o controle de acesso seja efetivo e portas externas, como USB, permaneçam bloqueadas e com o seu uso controlado (MAGALHÃES, 2016).

## 2.3 ITIL

A prática de gerenciamento de serviços em TI teve seu ápice nos anos 80, época em que teve início o desenvolvimento exponencial da tecnologia. Com foco nas necessidades de negócio uma abordagem mais radical em relação aos serviços foi necessária para lidar com a crescente gama de problemas sofridos por empresas – agora dependentes de um setor de TI consistente – para desenvolver seus negócios (CESTARI FILHO, 2011).

Ao mesmo tempo, a ITIL (*Information Technology Infrastructure Library*) foi desenvolvida pelo *Office of Government Commerce*, ou OGC, órgão do governo do Reino Unido na década de 1980, que buscava métodos mais eficientes para lidar com esta nova realidade, tendo em vista que o nível de qualidade de serviços de TI não era bom o suficiente. A biblioteca funcionou tão bem que foi rapidamente adotada também pelo setor privado.

A ITIL evoluiu para uma estrutura comum visando o gerenciamento de serviços de TI, permitindo às empresas identificar, definir, comunicar e implementar suas práticas nas organizações de TI. Consequentemente, a ITIL acaba ajudando estas organizações a alinharem-se com os objetivos de negócio de seus clientes (FUJII, 2015).

Constitui-se de um compêndio de livros baseados em um conjunto de conceitos e práticas e é organizado em cinco elementos conhecidos como Ciclo de Vida de Serviço, cada uma com sua função específica, voltadas para o desenvolvimento e gerenciamento de serviços na área de TI.. Os elementos são (CESTARI FILHO, 2011):

- Estratégia de Serviço, define as características principais da organização e de seus serviços;
- Desenho do serviço, fornece orientação para a concepção e desenvolvimento de serviços que atenderão aos objetivos da empresa;

- Transição de Serviço, fornece um guia para a transição de um serviço novo ou modificado em um serviço pronto para ser lançado;
- Operação de Serviço, foca na entrega e na manutenção do serviço;
- Aperfeiçoamento Contínuo de Serviço que cuida das práticas para avaliar e melhorar a qualidade dos serviços.

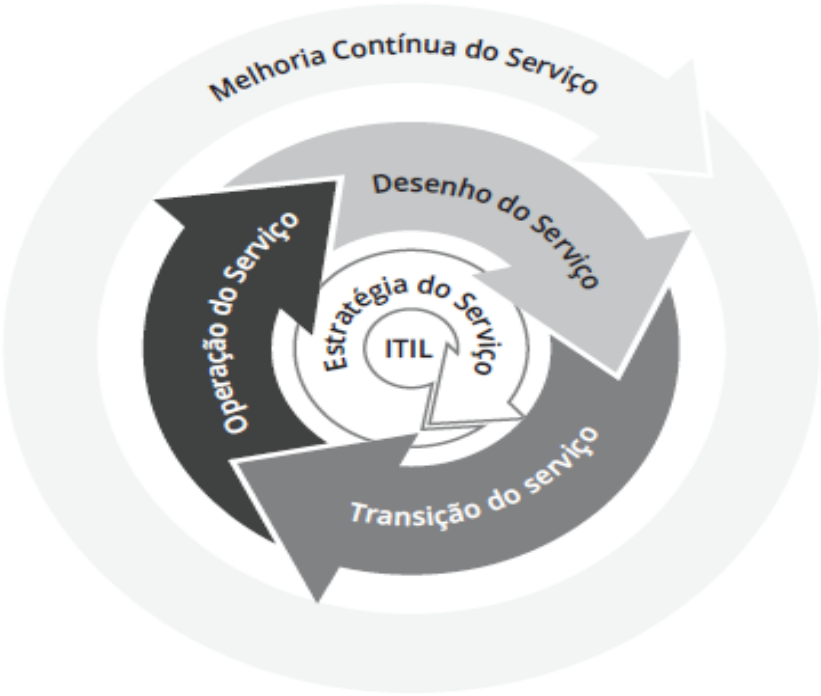


*Figura 6:* Ciclo de vida de acordo com o modelo ITIL
Fonte:(CESTARI FILHO, 2011)

A Figura 6 apresenta o ciclo de vida do serviço e como os elementos deste processo interagem entre si.

A fim de respeitar o escopo do trabalho, será abordado somente o elemento relacionado ao projeto do serviço, tendo em vista que a pesquisa decorre das consequências da inserção de elementos em uma rede, sem que haja uma doutrinação correta para tal.

O projeto de serviços provê direcionamento sobre como projetar e desenvolver serviços e processos de gerenciamento de serviços. Cobre princípios e métodos para transformar objetivos estratégicos em portfólio de serviços e ativos estratégicos. Inclui novos serviços para manter ou aumentar o valor para os clientes ao longo do ciclo de vida do serviço, a continuidade dos serviços, a entrega dos serviços dentro das metas acordadas e a aderência a padrões e à legislação (CESTARI FILHO, 2011).

Esse elemento é composto de diversos processos, dentre eles, o que se enquadra com maior efetividade na pesquisa é o gerenciamento de segurança da informação, que visa controlar a provisão de informação e evitar seu uso não autorizado.

Para que esse aspecto seja cumprido com aproveitamento, segundo Cestari Filho (2011) devem ser seguidos os seguintes objetivos:

- Garantir que o acesso à informação seja fornecido de maneira correta (confidencialidade dos dados);
- Garantir que a informação seja entregue completa, precisa e protegida contra a modificação (integridade dos dados);
- Disponibilizar a informação e deixá-la disponível para uso quando requerida, preparando os sistemas de TI para que possam resistir aos ataques e prevenindo contra falhas de segurança (disponibilidade dos dados);
- Garantir a confiabilidade das transações (troca de informações) que existem na corporação e entre parceiros (autenticidade).


Figura 7: Componentes básicos de segurança
Fonte: (CESTARI FILHO, 2011)

Ou seja, a correta associação desse elemento proposto pelo ITIL, ao serviço disponibilizado pelas TIC no EB, serve como base para a implementação de dispositivos IoT com um menor impacto na GC, contribuindo para o correto planejamento e emprego da força.

## 2.4 FUNÇÕES DE COMBATE

Segundo a definição apresentada na Diretriz para a Base de Transformação da Doutrina Terrestre, publicada pelo Estado-Maior do Exército em 2013, temos que uma Função de Combate é um conjunto de atividades, tarefas e sistemas, integrados para uma finalidade comum, que orientam o preparo e o emprego dos meios no cumprimento de suas missões, assegurando que todos os aspectos necessários à condução das operações tenham sido abordados no planejamento.

Portanto, constitui um processo eficaz que permite ao Estado-Maior identificar e relacionar as tarefas que cada missão impõe, de forma que reúna as missões e as formas de atuação, selecionando as mais adequadas, por fim, integrando e sincronizando a execução dessas atividades e tarefas (BRASIL, 2013).

Além disso, a Diretriz subdivide as Funções de Combate em seis 6 aspectos, são eles:

> Comando e Controle: conjunto de atividades, tarefas e sistemas inter-relacionados que permitem aos comandantes o exercício da autoridade e a direção das ações. A função mescla a arte do comando com a ciência do controle. As demais funções de combate são integradas por meio de atividades da Função de Combate Comando e Controle.
>
> Movimento e Manobra: conjunto de atividades, tarefas e sistemas inter-relacionados, empregados para deslocar forças, de modo a posicioná-las em situação de vantagem em relação às ameaças. “Movimento” é o deslocamento ordenado de forças visando ao cumprimento de uma missão, em condições nas quais não se prevê interferência do oponente. “Manobra” é o deslocamento de uma tropa que esteja em contato ou que tenha a previsão de contato com uma força oponente.
>
> Inteligência: conjunto de atividades, tarefas e sistemas inter-relacionados empregados para assegurar a compreensão sobre o ambiente operacional, as ameaças, os oponentes (atuais e potenciais), o terreno e as Considerações Civis. Com base nas diretrizes do comandante, executa as tarefas associadas às operações de Inteligência, Vigilância e Reconhecimento.
>
> Fogos: conjunto de atividades, tarefas e sistemas inter-relacionados que permitem o emprego coletivo e coordenado de fogos cinéticos, orgânicos da Força ou conjuntos, integrados pelos processos de planejamento e coordenação de fogos.
>
> Logística: conjunto de atividades, tarefas e sistemas inter-relacionados para prover apoio e serviços, de modo a assegurar a liberdade de ação e proporcionar amplitude de alcance e de duração às operações. Engloba as Áreas Funcionais de apoio ao material, apoio ao pessoal e apoio de saúde.
>
> Proteção: conjunto de atividades, tarefas e sistemas inter-relacionados empregados na preservação da força, permitindo que os comandantes disponham do máximo poder de combate para emprego. As tarefas permitem identificar, prevenir e mitigar ameaças às forças e aos meios vitais para as operações, de modo a preservar o poder de combate e a liberdade de ação. Permitem, também, preservar populações civis (BRASIL, 2013, p.26).

# 3 A INFLUÊNCIA DA INTERNET DAS COISAS PARA A GUERRA CIBERNÉTICA

A IoT está se incorporando aos mais variados dispositivos e sistemas do planeta, como por exemplo, os dispositivos móveis, medidores de estacionamento, termostatos, monitores cardíacos, pneus, estradas e prateleiras de supermercados. Essa popularização traz consigo problemas de privacidade, segurança e possibilidade de exploração cibernética (BUTTLER, 2017).

Sobretudo, como citado anteriormente, o principal objetivo na GC é a informação. Tal informação deve possibilitar efeitos capazes de ultrapassar o domínio cibernético. A utilização de softwares e hardwares com a finalidade de controlar redes de dados só possui algum sentido se afetarem atores também fora desse campo, esta é a razão pela qual o emprego da GC é possível em diversos campos da atividade humana, desde que dependam de recursos de computação e informática para se desenvolverem e tenham alguma influência na consecução de um propósito final.

Além disso, segundo Egídio e Ukei (2015), a IoT atuará em amplo espectro nas infraestruturas de um país. Consequente será responsável por uma quantidade quase que imensurável de dados e o Estado dependerá do seu funcionamento contínuo. São exemplo de aplicabilidade: transporte e logística, saúde, vendas em varejo, cidades e indústrias inteligentes e, sobretudo, na gestão de recursos (água, energia, gás, etc.), segurança e conforto (EGÍDIO; UKEI, 2015).

Ou seja, com o emprego da IoT nos mais diversos processos de um Estado, aumenta a probabilidade de ações ofensivas contra suas infraestruturas críticas, com a paralisação, destruição parcial ou total de seus sistemas que são justamente os efeitos desejados nos domínios físico e cognitivo da guerra. Sendo o domínio cognitivo entendido como aquele que encontra as percepções e a compreensão sobre o significado, interpretação e utilização da informação (ALBERT; HAYES, 2003).

## 3.1 A INFLUÊNCIA DA INTERNET DAS COISAS PARA A GUERRA CIBERNÉTICA NO ÂMBITO DAS FUNÇÕES DE COMBATE

Tendo em vista a grande expansão de dispositivos e sistemas conectados a rede mundial de computadores, cresce de importância a análise da sua influência na Força Terrestre, sobretudo no âmbito da Guerra Cibernética, a partir do momento em que esses

elementos constituam peças importantes dentro da estrutura de atuação do Exército no tempo de paz e, principalmente, em tempo de guerra.

Nesta seção é feita uma abordagem qualitativamente probabilística acerca da influência que dispositivos IoT, utilizados pela Força Terrestre, causariam à Guerra Cibernética, com as condicionantes peculiares de cada Função de Combate.

### 3.1.1 Comando e controle

Segundo o Manual EB20-MC-10.205, a função de combate C² compreende o conjunto de atividades mediante as quais se planeja, dirige, coordena e controla o emprego das forças e os meios em operações militares, constituindo o elo que une os escalões superior e subordinado. Sendo que o comando integra as atividades com as quais o comandante impõe sua autoridade e impõe sua vontade em forma de ordens. Já o controle integra as atividades com as quais o comandante conduz as operações, dirigindo e coordenando as forças e meios destinados ao cumprimento da missão (BRASIL, 2015).

Um dos modelos existentes para execução do C² é o ciclo OODA, segundo ele, qualquer ação integrante de um processo decisório é parte de uma das quatro fases: observar, orientar-se, decidir e agir. O ciclo é um processo contínuo, todas as suas fases ocorrerão em paralelo. O comandante recebe informações, forma sua consciência situacional e toma decisões sobre as operações futuras, enquanto operações correntes são executadas por meio de ações dos escalões subordinados. Portanto, a percepção das informações e do ambiente torna-se mais próxima do real, à medida que os ciclos estejam apoiados em processos e em estruturas eficientes e seguras (BRASIL, 2015).

Além disso, as atividades de C² incluem: conduzir o processo de planejamento; operar posto de comando; realizar a gestão do conhecimento e da informação; participar da integração de esforços entre civis e militares; estabelecer e manter a disciplina; coordenar ações para informar e influenciar; e conduzir a gestão dos espaços cibernético e eletromagnético. Dentre essas atividades, será abordada em especial somente a condução da gestão do espaço cibernético, tendo em vista que é a atividade que se liga diretamente com a problemática da IoT, podendo ser facilmente explorada no âmbito da GC.

A GC tem como objetivo obter e explorar uma vantagem sobre inimigos no ciberespaço, para negar ou degradar o uso deste, e proteger redes e sistemas de C² da força. Nesse contexto, uma eventual fragilidade nos sistemas e redes da Força Terrestre pode

permitir que um ator mal intencionado comprometa esses meios, comprometendo o ciclo e consequentemente, refletindo resultados negativos para as demais funções de combate, tendo em vista ser responsável pela integração destas.

O inevitável cenário que acompanha a violação do processo decisório do comandante é que este último não conseguirá exercer o comando da sua tropa e tampouco o controle da mesma, impedindo que as atividades operativas sejam conduzidas conforme o planejado. Atrasará ou impedirá, portanto, o fluxo das ordens em todos os escalões fazendo com que a tropa não consiga acompanhar a evolução constante do espectro de conflitos.

### 3.1.2 Movimento e manobra

De acordo com o Manual do Exército Brasileiro EB20-MC-10.203, a função de combate M² é aplicada para a execução de operações militares, buscando obter, manter e/ou aprimorar a capacidade de deslocar ou dispor forças de forma a colocar o adversário em desvantagem, a fim de atingir os resultados que de outras formas seriam onerosos em pessoal e material. Auxilia na obtenção da superioridade, aproveitamento do êxito alcançado e liberdade de ação, bem como para reduzir as próprias vulnerabilidades. Além disso, busca destruir a coesão inimiga utilizando-se de variadas ações localizadas e inesperadas (BRASIL, 2015b).

Alguns aspectos devem ser observados pela função de combate M²: a profundidade do espaço de batalha, a sincronização e a integração das atividades. Dentre esses aspectos, a sincronização será utilizada como exemplo para uma situação particular em que haja um comprometimento nessa função de combate pelo uso de dispositivos conectados a rede.

Para que seja possível o uso do princípio da surpresa é imprescindível que haja a sincronização das ações. A sincronização das ações só é possível com a utilização efetiva do C², por meio de seus dispositivos e sistemas. Tendo em vista a crescente popularização de *smartwatches* e *smartphones* e seu uso pelos militares, eles podem ser alvo de uma possível exploração cibernética.

Sabendo-se que as informações geradas e trafegadas entre esses dispositivos são inúmeras e que em sua totalidade possuem sistemas de geolocalização, estas podem comprometer o sigilo da localização de postos de comando e áreas de estacionamento, a partir do momento em que estão sendo usados no campo de batalha como forma de auxílio a sincronização de ações e como facilitadores do C². Denuncia, portanto, a posição de tropas e

de meios desdobrados no terreno, comprometendo o efeito surpresa, favorecendo a atuação do adversário que, estando de posse dessas informações, estará um passo a frente nas ações dentro do teatro de operações.

### 3.1.3 Inteligência

Conforme o Manual do Exército, EB20-MC-10.207, a função de combate inteligência tem por missão apoiar o planejamento, a preparação, a execução e a avaliação das operações. Serve de base para o desenvolvimento das operações, ao apoiar o processo decisório, numa atividade contínua e dinâmica, assegura a compreensão sobre o ambiente operacional, as ameaças (atuais e potenciais), os oponentes, o terreno e as considerações civis. As tarefas dessa função de combate são esforços organizados para a orientação, obtenção, análise, produção e difusão de informações sobre a área de operações (terreno e considerações civis), o inimigo, as ameaças ou forças oponentes; e as condições meteorológicas (BRASIL,2015c).

A estrutura de inteligência deve incluir sistemas, procedimentos e organizações de inteligência capazes de gerar conhecimento de maneira oportuna. Uma estrutura de Tecnologia da Informação e das Comunicações (TIC) adequada complementa a função de combate. Partindo desse aspecto, o uso de TIC como meio de obtenção de informações é altamente eficaz, tendo em vista que a maioria dos dados produzidos atualmente trafega por redes de computadores. Muitas vezes esses dados são gerados até mesmo sem o conhecimento dos usuários por meio de dispositivos móveis ou sensores.

Esse alto volume de dados pode ser usado no levantamento de informações pela inteligência, com uso de diversas técnicas provenientes da GC, como por exemplo a engenharia social, pois muitos dos usuários não se atém a autenticidade dos outros indivíduos na rede e acabam por fornecer dados, até mesmos sigilosos, sem que sejam necessárias ações que envolvam o maior emprego de pessoal e material.

### 3.1.4 Fogos

Segundo o Manual EB20-MC-10.206, a função de combate fogos compreende um conjunto de tarefas e sistemas inter-relacionados que permitem a aplicação e o controle de

fogos integrados pelos processos de planejamento e coordenação. Está relacionada, portanto, às tarefas e aos sistemas que provém o uso coletivo e coordenado das capacidades de fogos indiretos, de defesa antiaérea e dos fogos conjuntos, permeando os processos de busca e aquisição de alvos, planejamento e coordenação de operações. Portanto, novamente a sincronização das ações torna-se um fator determinante, permitindo a eficácia e a oportunidade para a sua aplicação, além da proteção à tropa e à população civil, particularmente nas operações no amplo espectro (BRASIL, 2015d).

Conforme o Manual, essa função de combate deve manter três capacidades críticas:

> [...]Aquisição de alvos – É a detecção e localização de um alvo com detalhamento suficiente para permitir o efetivo emprego de armas. [...] Discriminação de alvos – É o processo de aplicação de um sistema, ação ou função para identificar e priorizar determinado alvo quando vários estão presentes. […] Engajamento de alvos – É o processo de aplicação de um sistema de armas, recurso, ação ou função contra um alvo para alcançar um efeito letal ou não letal em apoio aos objetivos do comando (BRASIL, 2015d).

Com a expressiva presença das TIC no planejamento e execução dos fogos, sobretudo na aquisição e engajamento de alvos, torna-se relevante o estudo das prováveis vulnerabilidades que esses sistemas podem apresentar, uma vez que estarão conectados em rede e estão certamente sujeitos a algum tipo de exploração cibernética.

Em uma situação hipotética, o uso na aquisição de alvos de cartas digitais, sistemas de geolocalização por satélite e reconhecimento por aeronaves não tripuladas, pode maximizar o poder de combate da força e favorecer o seu êxito. Em contrapartida, caso esses meios estejam comprometidos, podem fornecer informações inconsistentes, muitas vezes adulteradas intencionalmente pelo adversário na fonte ou durante o tráfego na rede entre os escalões, culminando no engajamento incorreto dos alvos. Isto onera a tropa em pessoal e material, quando não compromete áreas de concentração de civis ou de interesses para a Força.

### 3.1.5 Logística

De acordo com o Manual do Exército Brasileiro, EB20-MC-10.204, temos que a função de combate logística desempenha papel fundamental no sucesso das operações militares, devendo ser coerentemente planejada e executada desde o tempo de paz, bem como estar sincronizada com todas as ações planejadas. Em todas essas situações, deve ser

meticulosamente coordenada para assegurar que os recursos sejam disponibilizados aos usuários em todos os níveis. Além disso, integra o conjunto de atividades, as tarefas e os sistemas inter-relacionadas para prover apoio e serviços, de modo a assegurar a liberdade de ação e proporcionar amplitude de alcance e de duração às operações. Para tanto engloba as áreas funcionais de apoio de material, apoio ao pessoal e apoio de saúde (BRASIL, 2014).

Na logística, a organização será pautada pela flexibilidade, adaptabilidade, modularidade, elasticidade e sustentabilidade, levando-se em conta o caráter difuso das ameaças, a não linearidade dos conflitos e a execução de ações sucessivas e/ou simultâneas nas operações no amplo espectro.

Essa situação gera um desafio para essa função de combate, pois é imprescindível que conceda meios de modo a manter as forças na continuidade das operações, independentemente das características do cenário em que os meios estão sendo desdobrados. Para isso, são utilizados diversos meios informatizado para auxiliar no controle e na gestão da logística. Como exposto nos capítulos anteriores, todo ativo conectado à rede torna-se um alvo em potencial para a GC.

Como forma de exemplificar essa situação, suponha-se que sejam utilizadas câmaras frigoríficas (para armazenamento de alimentos) conectadas a rede, a fim de que sejam controladas e administradas remotamente e seu estado possa ser verificado em tempo real, pela utilização de sensores, tendo em vista a popularização de dispositivos IoT. Em sua essência, essa câmara deve manter a temperatura em um valor fixo a fim de manter o seu conteúdo em condições de ser utilizado. No entanto, caso sejam realizados ataques de negação de serviço e de interceptação de tráfego, um agente mal intencionado poderá em um horário em que haja pouco controle físico, como por exemplo, no período noturno, desligar ou aumentar a temperatura da câmara sem que o gerente do dispositivo tenha conhecimento, pois os dados de controle estariam adulterados.

O resultado dessa ação pode causar a queda do moral da tropa e a sua consequente retirada do combate, inibindo a continuidade das operações e comprometendo o êxito da força.

### 3.1.6 Proteção

Conforme o Manual do Exército, EB20-MC-10.208, a função de combate proteção reúne o conjunto de atividades empregadas na preservação da força, a fim de que os

comandantes disponham do máximo poder de combate para emprego. As tarefas permitem identificar, prevenir e mitigar ameaças às forças e aos meios vitais para as operações, de modo a preservar o poder de combate e a liberdade de ação. Permitem, também, preservar populações e infraestruturas civis (BRASIL,2015e).

Além disso, é importante destacar os cinco princípios da proteção, são eles:

> ABRANGÊNCIA– devem ser considerados e utilizados todos os meios disponíveis para incrementar tarefas e atividades de proteção com o objetivo de proporcionar o máximo de segurança às forças em campanha.
> INTEGRAÇÃO– deve ser buscada a integração dos esforços de proteção entre os diversos elementos de todos os escalões desdobrados na área de operações, bem como as ações desenvolvidas pelas demais forças de combate que possam proporcionar, mesmo que indiretamente, segurança aos meios.
> COMPLEMENTARIDADE– as atividades de proteção deverão ser concebidas de forma escalonada, criando resistências sequenciais que causem desgaste progressivo à ameaça ou reduzam os riscos a que possam estar submetidas as forças em campanha.
> REDUNDÂNCIA– deverá ser prevista mais de uma medida para fazer face a determinada ameaça, com prioridade para os meios ou áreas críticas para a manobra.
> PERMANÊNCIA– as tarefas da força de combate proteção ocorrem durante todo o tempo da campanha e acompanham a flutuação do combate, variando de intensidade, local e meios prioritários a serem protegidos (BRASIL,2015e).

Tendo por base estes cinco princípios, a GC atua em favor dessa função de combate executando medidas de proteção cibernética, imprescindíveis para o uso efetivo das redes de informação em todas as outras funções. Para isso, são empregados tecnologias de proteção nos hardwares, a utilização de aplicativos de segurança de rede e de procedimentos executados pelos respectivos operadores, tudo isso em sincronia com os elementos de comando e controle (BRASIL,2015e).

A correta aplicação da proteção cibernética ajuda a mitigar os problemas que poderiam ocorrer nas demais funções comentadas acima, principalmente através da aplicação fiel dos princípios da proteção, com foco na abrangência e na redundância, a fim de que todos os ativos de rede estejam seguros.

# 4 CONCLUSÃO

A pesquisa baseou-se na influência que a inserção de dispositivos ligados a IoT pode exercer sobre a GC, campo de pesquisa inserido na área de redes de computadores, com foco nas consequências para o EB. Especial atenção foi dada às funções de combate, tendo em vista a importância em identificar os tipos de vulnerabilidades e os processos para mitigar os riscos de exploração cibernética e aprofundar os conhecimentos de como aumentar a segurança de tais dispositivos, sobretudo pelo fato de que são uma novidade no contexto atual e deverão ser levados em conta no processo de decisão da força no escopo das funções de combate.

O objetivo geral deste trabalho foi realizar um estudo sobre as consequências que os dispositivos conceitualmente conhecidos como IoT podem trazer para a Guerra Cibernética dentro do Exército Brasileiro. Foi possível, por meio desta pesquisa, observar que os dispositivos de IoT devem ser tidos como um fator a ser levado em consideração no planejamento de cada uma das funções de combate, atingindo o objetivo proposto.

Para tanto foi necessário cumprir os seguintes objetivos específicos: descrição dos aspectos gerais sobre Guerra Cibernética; apresentação do conceito e dos princípios da Guerra Cibernética; exemplificação de ferramentas de ataque e de defesa usadas pela Guerra Cibernética; definição do conceito de Internet das Coisas; apresentação das suas aplicações atuais e aspectos de segurança relevantes; apresentação e definição das Funções de Combate dentro do Exército Brasileiro; análise da influência da Internet das Coisas para a Guerra Cibernética; apresentar o ITIL e, por fim, propor situações em que a Internet das Coisas influencie a Guerra Cibernética no âmbito de cada uma das sete Funções de Combate.

Foi observado que nos manuais e nas doutrinas referentes, tanto à GC como às funções de combate, não há a previsão para o planejamento do emprego de dispositivos IoT, nem mesmo é comentado o seu conceito, sendo essa uma das primeiras consequências para a GC. Sendo a definição muito recente e não existindo referências na doutrina, o planejamento torna-se bastante dificultado. Com a evolução constante das ferramentas de ataque e defesa e dos protocolos de conexão, a atuação da GC torna-se ineficaz, uma vez que não conseguirá atuar a frente das ações do inimigo e, consequentemente, permitirá que o sistema seja comprometido.

Além disso, foi observado que com a presença de elementos de IoT no âmbito das operações do EB, o planejamento de cada uma das funções de combate deve levar em conta

esses dispositivos, caso contrário, como exposto no desenvolvimento, as consequências podem comprometer toda uma operação, favorecendo assim o adversário.

Também foi observada que a adoção das chamadas “melhores práticas” (*best pratices*) permite seguir um modelo estruturado que melhora sensivelmente os controles permitindo um adequado tratamento dos riscos (ALVES, 2006), como abordado através do ITIL na pesquisa em questão. Para isso, seria importante uma estratégia de aproximação com estabelecimentos de ensino para sensibilizá-los da relevância dessas práticas para o currículo dos militares envolvidos em atividades de planejamento que cruzem com as questões abordadas no trabalho. No caso específico EB a preocupação com a segurança cibernética deve ser constante e também presente nas escolas de formação, logicamente adequados em profundidade de acordo com os níveis de usuários ou profissionais de TI.

Foi possível também caracterizar os elementos de IoT de forma que permitisse o entendimento das formas de exploração cibernéticas que poderão sofrer, as consequências do seu emprego para a GC e analisar a influência que trará para o planejamento nas funções de combate.

Para a realização da pesquisa foi feita uma revisão bibliográfica sobre o tema, em diversas bibliotecas eletrônicas científicas, livros, revistas e, principalmente trabalhos relacionados, conceituando e contextualizando de forma a proporcionar ao leitor um entendimento básico sobre os assuntos abordados pela pesquisa que são a IoT, GC e as funções de combate do EB. Portanto, o trabalho é suportado essencialmente em pesquisa bibliográfica e com limitações devido à enorme abrangência do tema.

Contudo, tendo em vista a existência de poucos trabalhos relacionados com o tema e o material existente ser direcionado, essencialmente, ao mundo comercial/empresarial, a pesquisa foi dificultada no que se refere a obtenção de dados técnicos sobre o problema, pois nem mesmo os manuais referentes aos assuntos estudados abordavam situações refentes ao tema estudo, limitando o trabalho a proposição de problemas que poderiam ocorrer em um cenário de combate nas condições que foram apresentadas na pesquisa.

Outrossim, o conteúdo bastante recente dessa pesquisa serve como inspiração para trabalhos futuros para aprofundamento do problema, o qual seu estudo é de importância ímpar no planejamento das operações atuais e futuras do EB, inclusive para a segurança das informações que trafegam nas redes da Força Terrestre.

## REFERÊNCIAS

ALBERT, David S.; HAYES, Richard E. **Power to the Edge:** Command and Control in the Information Age. DoD Command and Control Research Program CCRP. 2. Washington, DC: Library of Congress Press. 2003.

ALECRIM, Emerson. **O que é firewall?** Conceito, tipos e arquiteturas. 2013. Disponível em: <http://www. infowester.com/firewall.php>. Acesso em: 21 mar. 2018.

ALVES, Gustavo Alberto. **Segurança da Informação:** uma visão inovadora da gestão. . Rio de Janeiro: Ciência Moderna. 2006.

ASHTON, K. **That 'Internet of Things' Thing**. 2009. Disponível em: <http://www.rfidjournal.com/articles/pdf?4986>. Acesso em: 10 jan. 2018.

BRAGA, Ricardo de Oliveira. **Segurança Cibernética e Defesa**. Escola Superior de Guerra. Rio de Janeiro, p. 30. 2011.

BRASIL. Estado-Maior do Exército. **EB70-MC-10.232:** Guerra Cibernética. 1 ed. Brasília: EGGCF. 2017.

BRASIL. Estado-Maior do Exército. **EB20-MC-10.203:** Movimento e Manobra. 1 ed. Brasília: EGGCF. 2015.

BRASIL. Estado-Maior do Exército. **EB20-MC-10.205:** Comando e Controle. 1 ed. Brasília: EGGCF. 2015.

BRASIL. Estado-Maior do Exército. **EB20-MC-10.206:** Proteção. 1 ed. Brasília: EGGCF. 2015.

BRASIL. Estado-Maior do Exército. **EB20-MC-10.207:** Inteligência. 1 ed. Brasília: EGGCF. 2015.

BRASIL. Estado-Maior do Exército. **EB20-MC-10.208:** Proteção. 1 ed. Brasília: EGGCF. 2015.

BRASIL. Estado-Maior do Exército. **EB20-MC-10.204:** Logística. 3 ed. Brasília: EGGCF. 2014.

BRASIL. Estado-Maior do Exército. **Bases para a Transformação da Doutrina Militar Terrestre**. 1 ed. Brasília: EGGCF. 2013.

BRASIL. Ministério da Defesa. **Manual MD35-G-01:** Glossário das Forças Armadas. 1 ed. Brasília: EGGCF. 2007.

BUTTLER, Peter. **CSO Magazine from International Data Group:** IOT Privacy. 2017. Disponível em: <https://www.idg.com/news>. Acesso em: 15 ago. 2017.

CERVO, A. et. al. **Metodologia científica**. 6 ed. São Paulo: Pearson Prentice Hall. 2007.

CESTARI FILHO, F. **ITIL v3 Fundamentos**. Rio de Janeiro: Escola Superior de Redes. 2011.

CISCO. **A internet de todas as coisas: conectando o que está desconectado**. 2014. Disponível em: <http://share.cisco.com/IoESocialWhitepaper/index-pt.php#/0/2>. Acesso em: 30 dez. 2017.

DUARTE, L. O.. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio802.11x.** Monografia defendida para obtenção do grau de Bacharel em Ciência da Computação. NESP/ IBILCE. São José do Rio Preto, p. 55. 2003.

EGÍDIO, Lucas; UKEI, Thiago. **Internet das Coisas (IoT):** Uma análise de aplicabilidade. São Paulo:USP. 2015

EVANS, Dave. **Internet das Coisas:** Como a próxima evolução da Internet está mudando tudo. 2011. Disponível em: <https://www.cisco.com/c/dam/global/pt_br/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf>. Acesso em: 04 dez. 2017.

FAN, T.; CHEN, Y. **A Scheme of Data Management in the Internet of Things.** 2012. Disponível em: <https://ieeexplore.ieee.org/document/5657908/>. Acesso em: 30 dez. 2017.

FRANZIN, M. A; ROSSI, O. **VPN ( Virtual Private Network)**. 2000. Disponível em: <http://www.gpr.com.br/download/vpn.pdf>. Acesso em: 21 dez. 2017.

FUJII, Robson F. **Governança de TIC:** um estudo sobre os frameworks ITIL e COBIT. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação). Universidade Estadual de Londrina. Londrina-PR, p. 59p. 2015.

GASPAR, A. E. O.; JESUS, K. L. S.; SILVA, M. C. **Um estudo sobre sistema detecção de intrusão**. Monografia de conclusão de curso apresentada no curso de Pós-Graduação em Suporte a Redes de Computadores e Tecnologia Internet. Universidade Federal do Pará. Belém, p. 33. 2008.

GUILLEMIN, P.; FRIESS, P, **Internet of Things Strategic Research Roadmap**, 2009. Disponível em: <http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2011.pdf>. Acesso em: 27 dez. 2017.

ITU, 2012. **New ITU standards define the Internet of Things and provide the blueprints for its development.** 2012. Disponível em:<https://www.alexandria.unisg.ch/252999/1/s12599-015-0383-3.pdf> Acesso em: 20 jan. 2018.

KRCO, Srdjan et al. **Inspirando a Internet das Coisas.** Alexandra: Flextime Language Center. 2012.

MAGALHÃES, Gabriel G. M. S. **Estudo de segurança nos principais protocolos da Internet das Coisas.** Universidade de Brasília. Brasília, p. 97. 2016.

MANDARINO, Raphael. **Segurança e defesa do espaço cibernético brasileiro**. 1 ed. Recife: Cubzac. 2010.

MANYIKA, J. et. al. **The Internet of Things:** Mapping the value beyond the hype. 2015. Disponível em: <http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>. Acesso em: 25 mar. 2018.

MICROSOFT. **O que é software antivírus?.** 2012. Disponível em: <http://www.microsoft.com/pt-br/security/resources/antivirus-whatis.aspx>. Acesso em: 24 fev.2018.

MITNICK, Kevin D.; SIMON, William L.. **A arte de Enganar:** Ataque de Hackers: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education. 2003.

MORAES, Alexandre. **Múltiplas camadas de defesa:** A complementaridade do Firewall e do IPS. 2012. Disponível em: <http://alexandremspmoraes.wordpress.com/2012/07/03/multiplas-camadas-de-defesa-a-complementaridade-do-firewall-e-do-ips/>. Acesso em: 15 dez. 2017.

NETWORK BOX. **Anti-DDoS (Distributed Denial of Service)**. 2011. Disponível em: <http://www. network-box.com/anti-ddos>. Acesso em: 10 dez. 2017.

NIELSEN, J. N.. **The Generational Warfare Model**. 2010. Disponível em: <https://geopolicraticus.wordpress.com/2010/10/26/the-generational-warfare-model>. Acesso em: 21 nov. 2017.

OWASP (Org.). **Internet of Things-Top Ten: The OWASP Internet of Things Top 10 Project**. Disponível em: <https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf>. Acesso em: 25 mar. 2018.

PACITTI, Tércio. **Do Fortran à internet:** construindo o futuro através da educação. 3. ed. São Paulo: Thomson. 2002.

PARKS, Raymon C.; DUGGAN, David P. **Principles of Cyber-warfare**. 2001. Disponível em: <https://www.researchgate.net/publication/224259524_Principles_of_Cyberwarfare>. Acesso em: 24 fev. 2018.

PEIXOTO, Mário César Pintaudi. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. 1 ed. Rio de Janeiro: Brasport. 2006.

Revista Proof. **Internet das Coisas (IoT) e seus desafios de segurança**. Disponível em: <http://www.proof.com.br/blog/iot-internet-das-coisas-desafios>. Acesso em: 24 mar. 2018.

SHELBY, Zach. BORMANN, Carsten. **6LoWPAN:** the wireless embedded internet. Reino Unido: John Wiley and Sons, Ltd. 2009.

WAHER, Peter. **Learning Internet of Things Paperback**. Birmingham, Mumbai: Packt Publishing Ltd. 2015.

WEIK, M. H.. **The ENIAC Story**. 1961. Disponível em: <http://ftp.arl.mil/~mike/comphist/eniac-story.html>. Acesso em: 28/11/2017.

# GLOSSÁRIO

M2M - É a tecnologia que conecta máquinas, dispositivos e aparelhos à internet sem utilizar fios, transformando-os em recursos inteligentes.

CIBERESPAÇO - Ambiente feito pelo homem para criação, transferência e uso de informação em vários formatos. Ciberespaço consiste em hardware eletronicamente energizado/acionado, redes de computadores, sistemas operacionais e padrões de transmissão.

REDE DE COMPUTADORES - Termo que designa a interconexão entre diversos computadores e outros dispositivos, por meio de cabos, rádio ou satélite. A rede pode ser definida como um grupo de pontos, estações e nós, interligados, e o conjunto de equipamentos que os conecta.

SEGURANÇA DA INFORMAÇÃO - É a proteção da informação contra diversos tipos de ameaças, garantindo a continuidade dos negócios (missão), minimizando os danos e maximizando o retorno dos investimentos e as oportunidades relativas ao ramo de atuação da Organização.

SISTEMAS DE INFORMAÇÃO - Sistemas de informação significam computadores, facilidades de comunicação, redes de comunicação e de computadores, informações e dados que podem ser armazenados, processados, restaurados ou transmitidos por aqueles, incluindo programas, especificações e procedimentos para suas operações, uso e manutenção.

TECNOLOGIA DE INFORMAÇÃO (TI) - TI é a aplicação integrada das tecnologias de comunicações e de computação na coleta, processamento, transmissão e armazenamento de informações. Também chamada por Tecnologia das Comunicações e da Informação (TCI).

*WORMS* - São programas maliciosos semelhantes aos vírus, diferenciando-se na forma de infecção. Os *worms* se autocopiam e se auto propagam.