ESCOLA DE GUERRA NAVAL
CC TIAGO ARAUJO CHAPETTA

TECNOLOGIA E GUERRA CIBERNÉTICA

Rio de Janeiro
2020

ESCOLA DE GUERRA NAVAL

C-EMOS 2020

TECNOLOGIA E GUERRA CIBERNÉTICA

Rio de Janeiro

2020

C-EMOS 2020

TECNOLOGIA E GUERRA CIBERNÉTICA

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

Orientador: C-EMOS 2020

Rio de Janeiro

Escola de Guerra Naval

2020

RESUMO

Neste trabalho, pretendemos verificar como a evolução da tecnologia impacta a dinâmica dos conflitos militares modernos por meio da análise das guerras cibernéticas, com foco nas ocorridas a partir do ano 2000. Para tanto, a metodologia do trabalho se valeu da pesquisa e análise de publicações, obras, artigos e acessos a sites especializados relacionados a guerra cibernética, segurança da informação e defesa cibernética. Foi feita uma genealogia sobre as guerras cibernéticas seguindo a linha metodológica de Michel Foucault. Dessa forma, a genealogia tem o papel de base de conhecimentos, composta por fatos (ataques ocorridos) e definições, que permitirão responder à questão que orienta o objetivo definido: a evolução da tecnologia impactou os conflitos ocorridos a partir do ano 2000? Como conclusão, pudemos verificar que os ataques apresentados, por si só, já se revelaram ciberarmas poderosas, que possibilitaram o início de uma nova corrida armamentista no mundo cibernético. A genealogia, além de contribuir para dar suporte às questões relacionadas à essa corrida, também permitiu analisar os conflitos cibernéticos quanto a violência, vulnerabilidades, continuidade, dentre outras, e ainda apresentar algumas mudanças geradas por essa revolução ocasionada pela evolução da ciência da informação.

Palavras-chave: Ciberespaço. Cibernética. Guerra. Stuxnet.

LISTA DE ABREVIATURAS E SIGLAS

A2/AD -	*Anti-Access/Area Denial*
APTs -	Ameaças persistentes avançadas
ARP -	Aeronaves remotamente pilotadas
C4 -	Sistemas de Comando, Controle, Comunicações e Computação
CCDCOE -	*Cooperative Cyber Defense Center of Excellence*
CISA -	Agência de Segurança Cibernética e de Infraestrutura
DDoS -	*Distribuited Denial of Service*
DoS -	*Denial of Service*
EUA -	Estados Unidos da América
FAB -	Força Aérea Brasileira
FBI -	*Federal Bureau of Investigation*
IA -	Inteligência artificial
IEC -	Infraestruturas Críticas
IoT -	Internet of Things
ISR -	Sistemas Digitais de Inteligência, Vigilância
MD -	Ministério da Defesa
NCW -	Sistema de Guerra Centrada em Rede
NSA	*National Security Agency*
ONA -	*Office of Net Assessments*
OTAN	Organização do Tratado do Atlântico Norte
RAM -	Revolução nos Assuntos Militares
SCADA -	Sistemas de Controle de Automação e Monitoramento Industrial
TI -	Tecnologias da informação
UAS -	*Unmaned Aerial System*
UIT -	União Internacional de Telecomunicações
USB -	Universal Serial Bus

SUMÁRIO

1 INTRODUÇÃO.....5

2 GUERRA E TECNOLOGIA: FUNDAMENTAÇÃO TEÓRICA.....9
2.1 A tecnologia e a guerra.....9
2.2 Cibernética e ataques cibernéticos.....13
2.3 Evolução tecnológica a partir de 2000.....15

3 TECNOLOGIA E GUERRA CIBERNÉTICA: APRESENTAÇÃO DOS FATOS.....17

3.1 Genealogia da Guerra Cibernética.....18
3.1.1 Os ataques mais relevantes para o entendimento dos eventos cibernéticos.....20
3.1.1.1 Primeiros Ataques conhecidos a partir do ano 2000.....21
3.1.1.2 Ataques realizados pela Rússia.....21
3.1.1.3 STUXNET (2010).....22
3.1.1.4 China e Coreia do Norte a partir de 2010.....27
3.1.1.5 Ataque sofrido pela Ucrânia (2015).....27
3.1.2 Outros grandes ciberataques da história.....28
3.1.3 Os meios de ataques cibernéticos em 2019.....30
3.1.4 Ferramentas Tecnológicas das Guerras Cibernéticas.....31
3.1.4.1 Inteligência Artificial na Cibernética.....31
3.1.4.2 Segurança na velocidade das técnicas do DevOps, Desenvolvimento e Operações..33

4 ANÁLISE DAS GUERRAS CIBERNÉTICAS EXAMINANDO AS CIBERARMAS EM 2020.....37

4.1 Ataques cibernéticos.....38
4.1.1 Suposto ataque da Rússia à Londres, EUA e Canadá.....38
4.1.2 Ataque atribuído à China pelos EUA.....39
4.2 Manual de Tallin.....43

5 CONCLUSÃO.....46

REFERÊNCIAS.....49

1 INTRODUÇÃO

A evolução tecnológica é fruto da característica de adaptação do ser humano e de sua capacidade de resolução de problemas para superar dificuldades que lhe são impostas pelo meio onde vive. Podemos verificar que, com o passar do tempo, principalmente a partir do século XIX, a tecnologia tem avanços extraordinários, mas é possível constatarmos que os maiores ocorreram no século XX, com o advento do computador e da internet. A evolução dessas tecnologias, sua popularização e a ligação de redes internacionais permitiram o acesso de usuários das diversas partes do mundo e a integração dos diversos povos. A internet tornou-se um fator imprescindível para o desenvolvimento da sociedade, levando-se em conta a grande quantidade de informações que armazena e integra. Nesse espaço cibernético, há grande tráfego e processamento de dados, e importantes transações são realizadas, desde troca de mensagens instantâneas e operações comerciais até troca de informações sigilosas entre pessoas e Estados.

Com o surgimento dessa área de conhecimento, a tecnologia da informação toma conta do cotidiano das sociedades, permite o desenvolvimento técnico-científico, intervém nas transformações sociais, econômicas, políticas e favorece o processo de globalização do mundo, devido ao contínuo desenvolvimento de tecnologias inovadoras e de meios de comunicações, além da interligação do espaço físico às conexões estabelecidas no ciberespaço (KOOPS, 2016 *apud* CARVALHO, 2019). Nesse ambiente circulam informações e são realizadas as comunicações, o que possibilitou a interferência e o surgimento de novos ataques feitos por atores que estariam interessados em obter conhecimento e informações (DUIC *et al.*, 2017 *apud* CARVALHO, 2019). Dessa forma, e diante dessas possibilidades de

operações no espaço cibernético, as relações humanas mudaram consideravelmente, e os conflitos entre os Estados também sofreram alterações em sua dinâmica.

As guerras, que antes eram potencializadas pelo poderio bélico, passaram a utilizar-se dos benefícios de pesquisas na área de ataques cibernéticos dos Estados. Os pesquisadores observaram, nas falhas de segurança das tecnologias, o aparecimento de riscos estratégicos dos Estados, a possibilidade de ataques virtuais a estruturas inimigas e, por outro lado, a necessidade de defesa das infraestruturas nacionais, surgindo, então, uma nova modalidade de guerra denominada "guerra cibernética". Para Creveld (2004, p. 540, *apud* NOGUEIRA, 2018, p. 7), "a ascensão do Estado tornou-se inseparável da ascensão da tecnologia moderna".

É fato que a internet revolucionou o mundo. A conectividade alcançou Estados, atores não estatais e indivíduos, além de gerar uma interdependência global, incluindo a dependência militar das redes de computadores e do ciberespaço, tornando-se de grande interesse político.

Um dos problemas identificados é o crescente número de conexões às redes de computadores e à internet e o avanço tecnológico envolvido para possibilitar essas conectividades. Esse ambiente complexo inspira novas ameaças, sendo a mais debatida na atualidade, a guerra cibernética, que pode causar danos incalculáveis ao mundo real. A fim de verificar os impactos do avanço tecnológico nas guerras cibernéticas no mundo, foi proposta a seguinte questão: a evolução da tecnologia impactou os conflitos ocorridos a partir do ano 2000?

Com a visível dinâmica da evolução tecnológica, da alta conectividade das redes de dados, do mundo cada vez mais globalizado e dos consequentes riscos de ameaças no espaço cibernético, surge a necessidade dos Estados encontrarem novos meios de manter a sua autonomia e soberania. Desse modo, as análises dos diversos ataques no espaço

cibernético se tornaram imprescindíveis. Então, esses conflitos descritos na literatura e suas características serão utilizados como base bibliográfica para esse texto, em que estabelecemos a seguinte hipótese: o modo de realizar conflitos tem acompanhado a evolução tecnológica a partir do ano 2000.

A motivação para a pesquisa se deve ao número crescente de ciberataques ocorridos e ao desenvolvimento em ritmo exponencial da tecnologia da informação, considerando que por trás da possibilidade de uma nova arma cibernética, há sempre uma tecnologia que lhe dá suporte. A curiosidade científica a respeito do quanto as novas tecnologias contribuirão para a ocorrência de eventos cibernéticos também estimularam a pesquisa sobre o tema.

A relevância do estudo está em ressaltar a importância do desenvolvimento de novas tecnologias e seu potencial para a criação de armas cibernéticas, além do investimento na segurança dos Sistemas de Tecnologia de Informação e na identificação e entendimento de suas vulnerabilidades.

O propósito deste trabalho, portanto, foi observar como a evolução da tecnologia impactou a dinâmica dos conflitos militares modernos por meio da análise das principais guerras ocorridas neste milênio. Pretendemos também descrever como os Estados utilizam as tecnologias para se defender de possíveis ataques, preventivamente, evitando ameaças nas diversas áreas do poder. Para isso, empregamos o método exploratório, a partir do qual foram feitos levantamentos de documentos e de experiências, apresentação de casos selecionados e uma sucinta abordagem histórica da evolução da guerra em função do desenvolvimento tecnológico. A pesquisa bibliográfica foi realizada em livros, artigos científicos e fontes confiáveis na internet.

À vista disso, o trabalho está estruturado da seguinte forma: no segundo capítulo, descreveremos os fundamentos teóricos, abordando como as novas tecnologias da informação

influenciaram o modo de se fazer as guerras. Apresentaremos os fatos relevantes à pesquisa no capítulo três, ressaltando a importância do avanço tecnológico para o desenvolvimento das guerras cibernéticas por meio de sua genealogia, e apresentando ataques que são relevantes para a pesquisa, com foco nos ocorridos a partir do ano 2000. No capítulo quatro, faremos a análise das guerras cibernéticas, examinando os casos atuais. Por fim, no capítulo cinco, as nossas conclusões serão evidenciadas.

2 GUERRA E TECNOLOGIA: FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, serão abordados alguns dispositivos e sistemas que contribuíram para mudanças na forma de se fazer guerra entre Estados em função da evolução tecnológica. Pretendemos avaliar a relação entre a guerra cibernética e a tecnologia utilizada na produção dessas armas. Para tal, discorreremos sobre conceitos e fatos históricos, a fim de melhorar o entendimento dessa pesquisa. Na primeira seção, discutiremos a valorização do emprego da tecnologia na guerra; os conceitos referentes à cibernética e à guerra cibernética serão apresentados na segunda seção; e na terceira, faremos um breve resumo da evolução tecnológica a partir do ano 2000, que interferiu nas estratégias e táticas de guerra, propiciando o surgimento do que denominamos "espaço cibernético".

2.1 A tecnologia e a guerra

A partir da Segunda Guerra Mundial (1939-1945), os militares souberam da importância do caráter estratégico da ciência e da tecnologia na guerra moderna. Esse reconhecimento teve seu auge no Projeto Manhattan, que introduziu a era nuclear. Dessa maneira, a ciência e a tecnologia se tornam componentes essenciais às estratégias de guerra (CAVAGNARI FILHO, 2002).

A inovação tecnológica influenciou as organizações militares e impôs mudanças nas estratégias de defesa e de ataque nas guerras, atingindo também a política, a economia e a sociedade. Segundo Barry e Grinter (1998 *apud* LUNA, 2016), essas transformações foram denominadas por Andrew Marshall[1] como "Revolução nos Assuntos Militares" (RAM). Por

1 Diretor do Gabinete de Avaliação Precisa (ONA - *Office of Net Assessments in the Office of the Secretary of Defense,* tradução do autor).

conseguinte, as profundas mudanças na natureza da guerra causadas pela aplicação de novas tecnologias, juntamente com as mudanças significativas nas doutrinas militares e nos conceitos de combate e organizacionais, alteraram decisivamente a natureza e o comportamento das operações militares (LUNA, 2016, p. 3).

As mudanças militares em consequência das evoluções tecnológicas foram de tamanha importância para o estudo das guerras, que se tornaram um marco historiográfico para os pesquisadores de revoluções na história. Como exemplo, podemos citar as guerras do Afeganistão (2001-) e do Iraque (2003-2011), que foram consideradas RAM pelos Estados Unidos da América (EUA) (LUNA, 2016).

Para facilitar os estudos sobre as mudanças nos modos de se fazer a guerra e as consequências de sua modernização, Creveld (1991 *apud* LUNA, 2016) dividiu a história da guerra em idades, de acordo com suas características e avanços tecnológicos. Essas idades foram resumidas por Moura (2014 *apud* LUNA, 2016) e apresentamos aqui as características consideradas mais interessantes de acordo com o propósito desse trabalho:

a) Idade das Ferramentas (anos anteriores a 1500): é caracterizada pela possibilidade de armazenamento das informações com utilização da escrita;

b) Idade das Máquinas (1500-1830): o metal tem papel importante na invenção das armas de fogo, substituindo a madeira que até então era utilizada, o que foi considerado grande evolução tática. Os navios dos tipos caraça[2] e caravela começaram a ser utilizados e novos métodos de navegação foram empregados, o cálculo da longitude foi aperfeiçoado, as cartas obtiveram melhorias em sua elaboração e os equipamentos de navegação também evoluíram. Os navios a vela adquiriram maior capacidade de realizar manobras, maior capacidade de artilharia e um contingente de infantaria;

2 Navio a vela português usado para comércio entre os séculos XIV e XV.

c) Idade dos Sistemas (1830-1945): novas tecnologias foram empregadas na guerra e surgiram as ferrovias, possibilitando deslocamentos de maiores distâncias, e os telégrafos, ampliando a capacidade de comunicação. Com a invenção do aço, ele passa a ser a principal matéria-prima para confecção dessas tecnologias. Além disso, a inovação tecnológica adquire relevância, assumindo caráter institucional;

d) Idade da Automação (a partir de 1945): é reconhecida a importância das ciências da automação e do desenvolvimento tecnológico, com investimentos e pesquisas. Nesse período, que envolve a era da globalização, há uma explosão no desenvolvimento de novas tecnologias. Foram desenvolvidos os computadores e a internet, revolucionando o mundo e a forma como se dão as relações, integrando culturas e compartilhando informações gerais – e até as sigilosas – entre Estados. Os modos de execução das guerras são alterados, acompanhando esse avanço, surgem novas ideias, sistemas e costumes, dando a elas um novo significado, de acordo com seus objetivos e *modus operandi*. Liang e Xiangsui (1999 *apud* LUNA, 2016) classificou-as como: psicológicas, comerciais, financeiras, centrada em mídia, guerra cibernética, dentre outras. Nesses tipos, os danos causados podem ser comparados aos causados por operações de guerras.

Dentre as principais tecnologias de guerra, Moura (2014 *apud* LUNA, 2016) cita aquelas inovadoras, que foram consenso na utilização em combates entre os Estados desenvolvidos tecnologicamente: satélites artificiais que apresentam várias aplicabilidades, mas que no ambiente militar são destinados à coleta de informações de inteligência e comunicações; aeronaves remotamente pilotadas (ARP)[3], uma evolução mista dos drones de artilharia e dos

3 Nome dado pela Força Aérea Brasileira (FAB) para o termo Sistema Aéreo Não Tripulado (UAS - *Unmaned Aerial System*).

mísseis; e sistemas de sistemas, que são vários subsistemas integrados que funcionam com um objetivo comum em suas ações, apresentando diversas possibilidades de aplicações, tais como na defesa ou na ofensiva em guerras de informações, no controle do espaço aéreo, na computação avançada, dentre outras (MAIER, 2000 *apud* LUNA, 2016). Encontramos alguns exemplos de sistemas de sistemas no ambiente militar: Sistemas digitais de Inteligência, Vigilância e Reconhecimento (ISR); Sistemas de Comando, Controle, Comunicações e Computação (C4); Sistema de Guerra Centrada em Rede (NCW); e Sistema de Força de Precisão[4] e A2/AD (*Anti-Access/Area Denial*)[5] (LUNA, 2016).

Há, ainda, as tecnologias de rupturas aplicadas nas Estratégias de Guerra que utilizam conhecimentos do estado da arte da Ciência e Tecnologia e influenciam o ambiente e a sua utilização, tendo como exemplos: armas de energia, como a *laser weapon system (LAWS)*; as ciberarmas, como o vírus *flame* usado contra o Irã em 2010; e as armas de nanotecnologias (LUNA, 2016).

Enfim, podemos observar que as guerras estão adquirindo estratégias modernas apoiadas no avanço tecnológico, o que poderá caracterizar a chamada "guerra do futuro", em que o emprego das forças militares deverá ser minimizado, mas com potencial de danos equivalente ao de um combate militar regular, e as armas que até então só apareciam em obras de ficção, hoje podem ser realidade, desde que regulamentadas: drones programados para reconhecer perfis e atirar; máquina controlada remotamente participando de guerras a milhares de quilômetros de distância; ataque *hacker* acarretando o corte da luz de hospitais e derrubando a energia de uma base militar, com possível resposta a isso com armas nucleares; soldados equipados com óculos de realidade virtual que auxiliam a detectar o inimigo; e ataques cibernéticos (TRINDADE, 2019).

4 Termo originário do Inglês: *Precision Force* (tradução do autor).

5 Estrutura de proteção das forças por meio do impedimento de ganho de posição de vantagem pelo inimigo.

Considerando o objetivo do trabalho, apresentaremos os conceitos básicos relacionados a ataques cibernéticos na seção a seguir.

2.2 Cibernética e ataques cibernéticos

Cibernética, enquanto termo, teve origem no artigo *Cyberwar is coming!*, de Arquilla e Ronfeldt (1993), e origina-se etimologicamente do grego *kybernetikos*, que corresponde à governança ou à arte de governar (*kybernetike tekhne*) (LOBATO; KENKEL, 2015). É a ciência da comunicação e controle, pois "é a finalidade da cibernética desenvolver uma linguagem e técnicas que de fato nos capacitarão para atacar o problema de controle e comunicação em geral" (WIENER, 1989, p. 17 *apud* LOBATO; KENKEL, 2015). Além disso, ela inclui o estudo do homem, o que fez com que o desenvolvimento da tecnologia dos computadores fosse inspirado na observação dos aspectos da inteligência humana.

A partir disso, apresentaremos resumidamente o dinâmico desenvolvimento tecnológico ocorrido a partir do ano 2000, com amplo emprego da inteligência artificial (IA). Tais tecnologias foram essenciais para o desenvolvimento dos novos armamentos militares e contribuíram para a continuidade e a complexidade dos conflitos cibernéticos. A cibernética utiliza, ainda, outros conhecimentos, como os da linguagem, comunicação, mensagens entre humanos e entre humanos e máquinas, sistema nervoso, dentre outros.

As guerras cibernéticas se apresentaram, conforme Clarke e Knake (2010 *apud* NOGUEIRA, 2018, p. 8), como as "iniciativas empreendidas por um Estado-nação para invadir computadores ou redes de informação com o propósito de causar danos ou distúrbios". Isso pode ser entendido como conflito entre Estados no ciberespaço, tendo como principal

objetivo a informação e como principais alvos as infraestruturas críticas (IEC)[6], que incluem estrategicamente os sistemas sociais que controlam transportes e abastecimentos, os sistemas relacionados à energia e os sistemas financeiros. O Ministério da Defesa (MD) do Brasil possui a seguinte definição:

> conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores. Essas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil (BRASIL, 2015, p. 134).

Logo, a guerra cibernética tem como característica principal a ocorrência de ataques no ciberespaço, por agentes maliciosos, para obtenção de informações e procedimentos tecnológicos ou de alguns benefícios com as informações adquiridas. Esses agentes detectam as vulnerabilidades dos sistemas e os ataques são realizados sem que a sua autoria seja conhecida, já que é de difícil identificação (CAVELTY, 2011 *apud* LOBATO; KENKEL, 2015).

Ressaltamos que o assunto pesquisado está inserido no cenário das mudanças da guerra na modernidade, apontadas por Bousquet (2011 *apud* LOBATO; KENKEL, 2015), em que é evidenciada a importância da tecnologia na forma de guerrear atual, por meio da análise da ciberguerra. Para compreender isso, foi construída uma genealogia segundo os pensamentos de Foucault (1980 *apud* LOBATO; KENKEL, 2015).

A genealogia, enquanto metodologia, é um conceito complexo que já foi discutido por vários pensadores. Para Foucault (1980), a genealogia não se caracteriza pela descrição de um fenômeno a partir das suas origens, mas pela apresentação de características que permitam discutir convicções filosóficas e sociais, avaliar, ou deduzir alguns conhecimentos (LOBATO; KENKEL, 2015).

6 Infraestrutura Crítica – as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional. Definição do Gabinete de Segurança Institucional da Presidência da República (GSI/PR)

Portanto, elaborar uma genealogia da ciberguerra consistirá em encontrar os significados nos fatos e conceitos apresentados e, a partir de raciocínio lógico e análise, concluir sobre os seus avanços e a sua possibilidade de ocorrência em função da crescente evolução tecnológica.

2.3 Evolução tecnológica a partir de 2000

Dentre as muitas novas tecnologias surgidas neste milênio, citaremos aquelas que tiveram aplicações no desenvolvimento de armas cibernéticas. Podemos ressaltar o desenvolvimento da banda larga no ano 2000, que substituiu a internet discada; a evolução contínua dos computadores; a popularização da internet; a conexão por meio de dispositivos móveis, com a criação das redes 3G, 4G e 5G, sendo essa última não disponível em todos os Estados; o surgimento do *pen drive*, que substituiu o disquete e o CD-ROM e continua em processo de evolução quanto a sua capacidade de armazenamento e velocidade de transferência; e a popularização da computação na nuvem, que se refere à tecnologia que utiliza a internet para armazenar, compartilhar e disponibilizar dados (NOGUEIRA, 2018).

Os Estados desenvolvidos passaram a investir na aplicação de conhecimentos avançados, como visão computacional, aprendizado de máquina e IA, tanto para o desenvolvimento de tecnologias bélicas modernas – incentivando a indústria nas inovações tecnológicas que buscam e atingem alvos de forma autônoma – quanto para ataques e defesas no espaço cibernético – propiciando uma corrida armamentista (TRINDADE, 2019).

A IA ganha destaque neste século e, por meio de suas técnicas, vem colaborando com a construção de sistemas autônomos letais ou robôs autônomos letais, que substituiriam o operador em situações de maior perigo ou que provocassem danos diretamente aos adversários, o que alguns denominam como “parte suja dos conflitos”. Esses robôs são

capazes de realizar operações de seleção e ataques de alvos sem a participação de humanos. Podemos citar, como exemplo, a construção de mísseis que escolhem seus alvos sem a interação humana.

EUA, China, Rússia, Reino Unido, Israel e Coreia do Sul são considerados Estados que investem fortemente no desenvolvimento dessas armas que dispensam a participação humana para agir. Segundo Trindade (2019), esses dispositivos "Matam sem a participação de humanos", no entanto, seu emprego é um tema polêmico e tem sido objeto de discussão em órgãos relacionados aos direitos humanos. Porém, os dirigentes desses Estados poderosos parecem não se importar muito com essas discussões e estão mais preocupados com o poder e suas soberanias.

Nos conflitos cibernéticos, a IA exerce um papel importante por meio da utilização do aprendizado de máquina – que é essencial para reconhecimento de padrões –, da teoria do aprendizado computacional e da sua contribuição aos sistemas de *Internet of Things* (IoT)[7] – que, devido à grande conectividade digital de objetos com a internet, tornou-se uma seara atraente para ataques.

7 *Internet of things*: Internet das coisas é um conceito que trata da conexão de objetos de uso cotidiano à internet (tradução do autor).

3 TECNOLOGIA E GUERRA CIBERNÉTICA: APRESENTAÇÃO DOS FATOS

Neste capítulo, o objetivo é verificar a influência do avanço tecnológico na ciberguerra. Para tal, alguns ataques serão apresentados, com destaque, principalmente, aos que ocorreram a partir de 2000, impactando fortemente sociedades e organizações, e constituindo-se em fato importante devido ao emprego de cibertecnologias como armas capazes de destruir redes críticas, causar danos físicos ou alterar o desempenho de sistemas cruciais. O exemplo do vírus *Stuxnet* (2010) é o mais conhecido ataque cibernético que causou danos físicos, por isso e por sua importância e projeção internacional, ele será apresentado com mais detalhes para enriquecer o trabalho e auxiliar nas respostas às nossas questões.

A partir dessas informações, pretendemos analisar os seguintes aspectos: principais vulnerabilidades virtuais; possibilidades de continuidade e os significados da ciberguerra; o avanço tecnológico na atual era (Era da Informação); e se a tecnologia associada à guerra contribuirá para a erradicação da violência nas guerras.

Sendo assim, analisaremos a questão dos conflitos cibernéticos, evidenciando a evolução da ciência da informação e da comunicação, e verificando como esses conhecimentos influenciaram as guerras. Além disso, discutiremos até que ponto os Estados, políticas governamentais e forças armadas que detêm esses conhecimentos e os empregam, adquirem alguma vantagem nos conflitos internacionais, contribuindo, dessa forma, para uma nova corrida armamentista no mundo. Será observado, também, se o desenvolvimento de novas tecnologias interfere nas relações estratégicas e táticas das guerras e o quanto é importante para que o espaço cibernético se torne novo campo de batalha entre os Estados.

Para alcançar o objetivo, faremos uma genealogia das guerras cibernéticas, que funcionará como uma base de conhecimentos, em que serão apresentados conceitos e alguns dos conflitos cibernéticos mais importantes historicamente e mais divulgados pelos meios de comunicação. Ao final, tal genealogia, com os seus fatos e suas regras, deverá permitir, por inferência, responder às questões dessa pesquisa.

3.1 Genealogia da Guerra Cibernética

No que diz respeito ao amplo e complexo conceito de genealogia, adotaremos a perspectiva teórica-metodológica do filósofo Michel Foucault, que não se preocupa com a história a partir da origem dos acontecimentos, mas em contar a história a partir de crenças filosóficas e sociais, da compreensão dos fatos e práticas vividas pelos indivíduos, analisando como determinados saberes surgem em uma sociedade, investigando as condições em que esses conhecimentos são executáveis (FOUCAULT, 1980 *apud* LOBATO; KENKEL, 2015). Assim, por meio da genealogia, pretendemos entender o papel da cibernética quando introduzida como base do desenvolvimento das guerras, influenciando o pensamento militar a seu respeito, e analisá-la quanto à coerência em direção ao objetivo proposto.

A maioria dos avanços ocorridos em determinadas épocas acontecem de modo cumulativo, isto é, há o acréscimo de novos saberes aos limiares dos já existentes. Os avanços da tecnologia da informação e da comunicação também são cumulativos, mas ocorrem em intervalos em que os conceitos de novos conhecimentos não se concatenam aos limites dos conceitos anteriores. O consenso é que atualmente a tecnologia da informação pode ser considerada como conhecimento científico renovador, devido às mudanças que provoca no

modo de pensar e na visão de mundo, implicando em transformações sociais, econômicas e políticas (KUHN, 2006 *apud* ROCHA, 2014).

Desde o final do século XX, a tecnologia da informação está em constante evolução e influencia na mudança das dinâmicas dos conflitos, havendo um aumento das linhas de pesquisa referentes à guerra entre Estados. Foi a partir dessas pesquisas, que surgiu a possibilidade da existência de conflitos virtuais, que aconteceriam no local denominado "espaço cibernético". Esse espaço não é constituído somente pela internet, tampouco apenas por um domínio virtual, fazem parte dele as redes de computadores, intranets, tecnologias de celular, sistemas e cabos de fibra ótica (SINGER, 2014 *apud* AYRES; GRASSI, 2020).

Um ataque cibernético pode ser definido, portanto, como um ataque que, no espaço cibernético, explora as vulnerabilidades existentes, podendo gerar danos que são equiparados a ataques militares de guerras regulares, por meio de interrupção, degradação, negação, corrupção, adulteração ou destruição de informações ou de sistemas computacionais (LOBATO; KENKEL, 2015 *apud* AYRES; GRASSI, 2020).

No que diz respeito aos termos "ciberguerra" e "guerra cibernética", podemos dizer que correspondem às guerras cujos ataques são realizados no espaço cibernético. Porém, os termos são polêmicos e vêm sendo atribuídos a uma variedade de episódios: ataques cibernéticos, espionagem cibernética, crime cibernético ou terrorismo cibernético. A ciberguerra é consequência da explosiva evolução da ciência da informação na década 1980 e do amplo desenvolvimento das tecnologias da informação (TI) na década de 1990, quando as organizações incluíram a tecnologia em sua administração. Essas mudanças conduziram à alteração dos pensamentos sobre a natureza dos conflitos, com a mudança das estruturas e das estratégias militares (LOBATO; KENKEL, 2015).

Para Clarke e Knake (2010, p. 73 *apud* AGOSTINI, 2014), a possibilidade de uma guerra cibernética está relacionada a três itens: falhas na estruturação da internet, erros

intencionais ou não em *hardwares* e *softwares* e a crescente tendência de colocação em rede computacional de sistemas de IEC. Podemos verificar, ainda, que a internet, que sustenta a cibernética, é apoiada nos pilares facilidade de uso, segurança e privacidade (BAKER *et al* 2013, p. 14 *apud* AGOSTINI, 2014), porém, apesar da internet contemplar a simplicidade e a facilidade de comunicação, ela é insuficiente quanto à segurança. E isso é realmente um problema.

O conceito de "guerra" foi definido por Clausewitz (2010, p. 145 *apud* FEITOSA, 2017, p. 18) como "a luta durante certo lapso de tempo entre forças armadas de dois ou mais Estados, sob a direção dos respectivos governos". O autor também apresentou alguns itens que devem caracterizar uma guerra, como ser violenta, ser instrumental (ter início, meio e fim), ter um propósito político e não ser apenas um ato isolado.

No século XXI, a ciberguerra ganhou projeção após alguns ataques cibernéticos contra a Estônia (2007), a Geórgia (2008) e o Irã (2010). Porém, outros eventos também são citados nesse trabalho para ratificar que as vulnerabilidades do ciberespaço foram e continuam sendo um campo fértil para ataques entre os Estados. Essa percepção corresponde tanto à realidade, que os ataques de negação de serviço (DoS)[8] que foram feitos à Estônia e à Geórgia e as destruições físicas causadas pelo vírus *Stuxnet* foram só uma pequena parte introdutória da complexa evolução dos meios utilizados nas ciberguerras que já ocorreram (LOBATO; KENKEL, 2015).

3.1.1 Os ataques mais relevantes para o entendimento dos eventos cibernéticos

Alguns ataques que temos conhecimento ocorreram com o objetivo de interceptar atividades legítimas, como navegar em uma *web browser* para roubar documentos oficiais e

8 *Denial of Service* (tradução do autor).

militares sigilosos, produções intelectuais, além de espionar o governo. Nas próximas subseções, apresentaremos os ataques que, segundo Gama Neto (2017), são relevantes para o entendimento dos eventos cibernéticos, auxiliando nas respostas às questões atuais.

3.1.1.1 Primeiros Ataques conhecidos a partir do ano 2000

Nesta subseção, citaremos alguns ataques que tiveram importância na história do desenvolvimento das guerras cibernéticas que ocorreram no período de 2001 a 2006:

a) *Cold Red* (2001): vírus que atacou as redes de computadores com sistema operacional Microsoft, desativando *sites,* incluindo o da Casa Branca (VARELLA, 2020);

b) *Anonymous* (2003): originou-se do grupo de *hackers* especializados em ataques a *sites,* especialmente os governamentais, empresariais e religiosos (VARELLA, 2020); e

c) NASA (2006): preocupou-se com o bloqueio de e-mails com anexos para evitar que *hackers* atrapalhassem os planos de lançamento de ônibus espaciais por meio de ataque a rede de computadores da Agência Espacial (VARELLA, 2020).

3.1.1.2 Ataques realizados pela Rússia

A Rússia é o Estado que mais utilizou a internet como arma de ataque contra adversários em conflito. Abaixo, citamos os principais ataques russos:

a) Estônia (2007): a data do ataque, 27 de abril, foi o marco do que passou a ser denominado "guerra cibernética". Os ataques foram do tipo negação de serviço *Distribuited Denial of Service* (DDoS) e realizados a sites do governo, bancos e principais jornais estonianos, por redes *botnets*[9] (NOGUEIRA, 2018); e

b) Georgia (2008): nas semanas anteriores à guerra entre Rússia e Geórgia, ocorreu grande ataque de DDoS contra os sítios eletrônicos da Geórgia. O governo de Tbilisi culpou a Rússia pelos ataques na internet ocorridos em 20 de julho. Esses ataques pretenderam dar suporte à invasão russa e, assim que os disparos começaram na Geórgia, as principais infraestruturas foram atacadas virtualmente. O resultado foi a desativação de 54 sítios eletrônicos georgianos, dos setores relacionados à imprensa e às áreas de comunicação (NOGUEIRA, 2018).

Cabe ressaltar que, segundo Handler (2012, *apud* NOGUEIRA, 2018), é possível considerar que os locais que foram alvos virtuais também seriam escolhidos como os primeiros alvos a serem atingidos em uma guerra convencional.

3.1.1.3 STUXNET (2010)

Stuxnet foi um vírus cujo ataque mais repercutiu na comunidade internacional. Essa arma cibernética foi utilizada para atacar a rede da usina nucelar do Irã, interferindo no programa nuclear daquele Estado. Produzido com meios tecnológicos complexos, foi considerado o maior da história e, por isso, para enriquecimento do trabalho e para que auxilie em

9 Uma rede de computadores ligados à internet.

nossas conclusões, o apresentaremos detalhadamente. Para compreender o seu funcionamento, analisaremos dados do seu surgimento e o impacto que causou.

Em Natanz, região central do Irã, no início de 2010, o presidente Mahmoud Ahmadinejad e engenheiros ativaram mais de 8000 centrífugas de enriquecimento de urânio, o que viabilizaria a produção das primeiras bombas atômicas do país. Porém, surpreenderam-se ao verificarem que centenas daquelas centrífugas tinham parado de funcionar sem aparentar algum indício do que estava acontecendo. Não sabiam o que tinha provocado o problema que atrasaria os planos da produção da bomba atômica iraniana.

Após alguns meses, na Bielorrússia, o vírus foi detectado por Sergey Ulasen – que trabalhava em uma empresa desenvolvedora de antivírus, a *VirusBlokAda* – ao examinar o computador de um cliente iraniano. O computador entrou em um procedimento de reinicialização, desligando e reiniciando várias vezes, sem obedecer aos comandos das operadoras que tentavam controlá-lo. O vírus não possui origem conhecida, mas, por sua complexidade, acredita-se que tenha sido desenvolvido com apoio de alguma instituição governamental, os principais suspeitos citados na literatura são EUA e Israel (SANTOS; VERSIGNASSI, 2016).

Os técnicos de Ulasen constataram que o vírus se aproveitava de vulnerabilidades do tipo *Zero Day*[10], armas comuns que, segundo Zetter (2011 *apud* FEITOSA, 2017), eram aproveitadas pelos *hackers*, que as utilizavam para atacar e espalhar as fragilidades na segurança dos *softwares* desconhecidas pelos profissionais que trabalham com antivírus. A tarefa de detectar vulnerabilidades em *softwares* não é simples. O sistema *Microsoft Windows*, segundo especialistas, apresentava quatro falhas de segurança até então desconhecidas, e uma delas estava no arquivo LNK, ou *links* de *shell*, que são caminhos do *Windows* que propiciam o acesso a lugares distintos (FALLIERE *et al.*, 2011 *apud* FEITOSA, 2017). Em 12 de julho de 2010, a empresa *VirusBlokAda* tentou avisar à *Microsoft* sobre a fragilidade e divulgou que

10 Os ataques “Zero Days” ocorrem quando uma vulnerabilidade é atingida em um período entre a data descoberta da ameaça e a data da correção.

havia detectado o vírus numa postagem de um fórum de segurança. Logo depois, cópias do código do *malware*[11] foram distribuídas entre empresas de segurança da informação.

Esse vírus altamente destrutivo atua especificamente no sistema operacional desenvolvido pela *Siemens*, chamado Sistemas de Controle de Automação e Monitoramento Industrial (SCADA), que controla as centrífugas de urânio com uma configuração apropriada para cada uma, e o ataque só acontecia a computadores que possuíam uma placa de rede específica. O *Stuxnet* não pretendia atingir qualquer computador, visava apenas o ataque às configurações dos computadores das usinas iranianas, mas mesmo assim se propagou, atingindo pelo menos 100 mil computadores no mundo, em quantidades diferentes nos diversos locais, sendo que 60% das infecções se deram no Irã.

O desafio consistia em penetrar nos computadores das instalações nucleares. A estratégia foi contaminar muitos computadores pessoais apostando que alguns deles seriam de funcionários da empresa, que levariam o vírus para as instalações nucleares por meio de seus *pen drives* infectados. Ou seja, o vírus chegava aos computadores por dispositivos *Universal Serial Bus* (USB), que infectavam o sistema silenciosamente, simplesmente ao se inserir o *pen drive* no computador. Quando um dispositivo USB infectado era inserido em um computador, o conteúdo do dispositivo era escaneado pelo *Explorer*, o código de exploração era ativado e transferia para o computador um grande arquivo que no início encontrava-se criptografado, espalhando comandos não detectados no computador alvo segundo *Zetter* (2011 *apud* FEITOSA, 2017).

Os prejuízos causados por essa arma cibernética no Irã foram bastante consideráveis, mas o governo só admitiu os danos em junho de 2010, quando o vírus foi descoberto na Bielorrússia por meio da análise de cópias do código encontradas por técnicos nos computadores infectados de usuários comuns. Diante disso, não havia como o governo

11 Programa para roubo de dados.

iraniano negar o ataque. E ele só foi possível devido à total dependência das redes de IEC dos sistemas de informação do tipo SCADA (SANTOS; VERSIGNASSI, 2016).

Para a obtenção do urânio (U-235) com alto grau de pureza, é necessário o funcionamento de milhares de centrífugas, e as de Natanz realizavam 1.064 giros por segundo. O que o *Stuxnet* fez foi acelerar os giros em cerca de 40%, por 15 minutos somente, para não levantar suspeitas e não deixar com que isso fosse detectado pelos engenheiros responsáveis. Os engenheiros e técnicos só perceberam algo anormal ao ouvirem o barulho das centrífugas em alta velocidade, que foi acompanhado por uma explosão. Ficaram intrigados por não terem disparado nenhum botão vermelho de emergência, o programa impedia que isso acontecesse. Ou seja, tudo foi uma surpresa para os engenheiros que não sabiam por que isso estava acontecendo (SANTOS; VERSIGNASSI, 2016).

Segundo Sanger (2012 *apud* FEITOSA, 2017), os estadunidenses pretendiam atrasar a intenção dos iranianos de possuir uma bomba atômica. Assim, conforme o que foi divulgado por Gibney[12] e Snowden citados por Feitosa (2017), o projeto do governo estadunidense *Olympic Games* era de interromper, ainda que não definitivamente, o objetivo nuclear iraniano e persuadir Israel de que as armas cibernéticas seriam soluções mais eficientes e vantajosas em termos de custos. Washington e Tel Aviv entram em acordo e iniciaram a execução do plano. (FEITOSA, 2017).

De acordo com Feitosa (2017), em relação ao vírus, podemos observar que não necessita da internet para se espalhar já que a propagação é feita por portas USB, utiliza *rootkit*[13] em nível de *kernel*[14] com certificações verdadeiras, e fica disfarçado e de forma adormecida no computador alvo, que ao ser ativado, prolifera, acessando os programas,

12 Philip Alexander "Alex" Gibney é um diretor e produtor estadunidense, documentário “Zero Days” (2016).

13 É um programa que acessa de maneira ilícita um sistema informatizado.

14 Núcleo, tem como função ligar o *hardware* ao *software*, permite o acesso seguro aos programas distintos.

roubando informações e reprogramando os controladores, não expondo as mudanças realizadas.

O ataque com esse vírus provocou alterações de comportamentos em alguns Estados. (FEITOSA, 2017). Para Vieira (2016), em sua avaliação sobre o documentário *Zero Days*, Israel se posicionou contrariamente ao emprego de armas nucleares entre os Estados próximos, principalmente o Irã, preocupando-se com o perigo que o armamento representaria para o país. Por isso, Israel interessou-se em participar do projeto *Stuxnet*. Netanyahu, segundo Gibney, passou a apressar os serviços de inteligência em relação à conclusão do projeto, levando a unidade 8.200[15] a decidir sem a participação dos estadunidenses, e transformou o *worm* em um programa ainda mais agressivo e com capacidade de transferência de informações entre máquinas imperceptível. A versão final do vírus foi alcançada com a tomada de várias decisões e, conforme Falliere *et al.* (2011 *apud* FEITOSA, 2017), foi denominada de "monstruosa".

De acordo com Gibney, o presidente dos EUA, Barack Obama, em 2008, deu prosseguimento à operação, sendo o termo *Stuxnet* divulgado mundialmente, deixando dúvidas sobre a autoria, se de Israel ou dos EUA. O vírus infectou sistemas além de Natanz. Os especialistas que participaram do documentário de Gibney, que eram da equipe de projeto da *National Security Agency* (NSA)[16], ficaram indignados com as atitudes às escondidas dos israelenses, o que é ratificado por Vieira (2016), ao afirmar que a arma desenvolvida pela agência se espalhava aleatoriamente pelo mundo, ameaçando a economia e pondo vidas em riscos (FEITOSA, 2017).

O vírus era diferente de qualquer outro conhecido. Ele não só roubava informações de determinados computadores, como também ultrapassava os equipamentos eletrônicos-digitais e causava danos físicos em outros equipamentos controlados por computadores. O

15 Unidade especial ligada ao serviço de inteligência israelense.
16 Agência de Segurança Nacional dos EUA (tradução do autor).

worm Stuxnet despertou interesse em novas pesquisas de *malware*. Assim, em maio de 2012, a empresa União Internacional de Telecomunicações (UIT) e os Laboratórios Kaspersky descobriram um novo vírus que foi projetado para espionagem e ficou conhecido por vários nomes: *Flame, Skywiper* e *Worm.Win32* (FEITOSA, 2017).

Os EUA nunca assumiram a autoria do *Stuxnet*, no entanto, foi encontrado, em 2013, um documento do poder executivo estadunidense assinado por Obama, no qual são descritas as regras para o emprego de armas cibernéticas. Um dos pontos que se destaca é quanto à determinação do uso de uma arma cibernética, que só poderia ser utilizada se autorizada pelo presidente da república (FEITOSA, 2017).

3.1.1.4 China e Coreia do Norte a partir de 2010

De acordo com Duda Teixeira (2015 *apud* GAMA NETO, 2017), China e Coreia do Norte são responsáveis por espionagem e ataques cibernéticos efetuados contra os EUA, Coreia do Sul, Japão e outros Estados, para roubo de informações. Os EUA tiveram dados de quatro milhões de funcionários do governo estadunidense roubados, por, supostamente, *hackers* chineses. A China foi quem mais conseguiu informações dos EUA, sobretudo aquelas que auxiliam no desenvolvimento das estatais chinesas, que são, principalmente, as atividades que dizem respeito à tecnologia e pesquisas espaciais.

Ressaltamos que tanto a China quanto a Coreia do Norte são considerados os Estados mais difíceis de sofrerem ataques cibernéticos, pelo fato de realizarem um alto grau de controle de suas redes, podendo isolarem-se das demais redes (CLARKE; KNAKE, 2010 *apud* GAMA NETO, 2017).

3.1.1.5 Ataque sofrido pela Ucrânia (2015)

Hackers russos realizaram um ataque utilizando-se de *malwares* para provocar um apagão elétrico na Ucrânia, interrompendo abastecimento de energia de centenas de casas. O presidente ucraniano, Petro Poroshenko, responsabilizou a Rússia por uma guerra cibernética contra o seu país, pois havia recebido um comunicado do governo russo em dezembro do ano anterior (ROHR, 2017).

John Hultquist[17] disse ter sido a primeira vez que foi registrado um ataque pela internet que causou queda de energia. E houve, ainda, um segundo ataque cibernético, com características muito semelhantes ao primeiro, em Kiev, capital da Ucrânia, com um apagão parcial no dia 17 de dezembro de 2017. (KUCHLER; BUCKLEY, 2016).

3.1.2 Outros grandes ciberataques da história

Apresentaremos, nesta subseção, outros significativos ataques da história, com o objetivo de complementar a linha do tempo dos ciberataques:

a) Em 2008, o Pentágono descobriu um programa em um *pen drive* que foi utilizado nos computadores em uma base no Oriente Médio, roubando dados do Departamento de Defesa e enviando-os para o exterior. O ataque tem a autoria desconhecida, mas que foi atribuída a *hackers* de uma empresa estrangeira, sendo considerado pelos militares estadunidenses como o pior ataque sofrido pelas Forças até aquele momento. O Pentágono, em 2010,

17 Chefe do departamento de espionagem cibernética da *iSight Partners*, nos Estados Unidos da América, que avalia ameaças de computador.

reconheceu o ciberespaço como novo ambiente de guerra (VARELLA, 2020);

b) O governo de Israel, em 2009, teve seus *sites* invadidos enquanto ocorria o conflito com o Hamas na Faixa de Gaza. Nesse ataque, 15 milhões de e-mails por segundo foram emitidos para computadores do governo, tornando-os inoperantes por algum tempo. A autoria foi atribuída a *hacker* pago pelo Hamas (VARELLA, 2020);

c) Em 2011, em Mahdi, um *malware* foi introduzido como anexo de e-mails, invadindo cerca de 800 computadores do governo, embaixadas e empresas do Irã, Israel, Afeganistão, Emirados Árabes Unidos e África do Sul (VARELLA, 2020);

d) Em NotPetya, em 2017, foi atribuído à Rússia o *malware* que infectava os *softwares* de declarações de impostos da Ucrânia e que, ao ser utilizado em computadores, criptografava e inutilizava os dados (TRINDADE, 2019);

e) Também em 2017, em Wannacry, um *malware* atacava criptografando dados de redes com sistema operacional *Windows*, além de exigir quantias para a liberação da chave criptográfica e, consequentemente, para a liberação do funcionamento das redes. O ataque foi atribuído à Coreia do Norte (TRINDADE, 2019);

f) Em Shamoon, no ano de 2012, em um ataque relacionado ao Irã, o *malware* roubou senhas e excluiu dados de 35.000 computadores da *Saudi Aramco*, uma empresa de petróleo da Arábia Saudita, e impediu que os computadores reiniciassem (TRINDADE, 2019);

g) Em fevereiro de 2016, um grupo de *hackers* transferiu US$ 81 milhões do Banco Central de Bangladesh, num dos considerados mais eficientes roubos

> cibernéticos. O *Lazarus*, um grupo de espionagem e sabotagem cibernética, foi considerado responsável (TRINDADE, 2019).

Nogueira (2018) relata uma palestra ministrada pelo pesquisador e professor de Relações Internacionais Bernardo Wahl no Campus Party, no Brasil, em 2017. Nela, Wahl destacou que a Revolução Cibernética ocorre dentro de alguns conceitos de guerra, sendo somente alterados os planejamentos estratégicos. Para Whal, as armas cibernéticas são ferramentas digitais ilegais e não evidentemente violentas, pois as possibilidades de morte são baixas, não satisfazendo a uma exigência para que seu uso se enquadre nos conceitos de guerra interestatal, elas podem causar danos e deixar um país impotente militar ou economicamente. No entanto, tais resultados encontram-se em um estado transitório, que não permitem determinar se de guerra ou de paz, permanecendo num ambiente sombrio. Esse estado obscuro quanto à regulamentação e às reações dessas operações de guerra interessa a muitos governantes, pois permite as reações de acordo com os seus interesses.

3.1.3 Os meios de ataques cibernéticos em 2019

Em 2019, foi detectado o *ransomwar*[18], que atacou eficientemente e prioritariamente negócios específicos, governos locais e organizações de saúde. Os atacantes estão se aperfeiçoando com o objetivo de aumentar seu alcance. Portanto, a partir de 2020, são esperados maiores danos diante do aumento das imposições dos atacantes (CHECK..., 2019).

18 _____ É um tipo de *software* que impede o acesso ao sistema infectado, por meio de bloqueios, exigindo resgates em criptomoedas para liberação do acesso. Caso o pagamento não seja realizado, os arquivos podem ser destruídos ou publicados.

O e-mail foi o principal método de ataques de *phishing*[19] em 2019, mas também foi possível detectar outros vetores de ataque, como SMS, mensagens em redes sociais e plataformas de jogos. No primeiro semestre do ano, foi constatado o aumento de 50%, sobre os valores de 2018, de ataques de *malware* de *mobile banking*. São previstas novas versões desses *malwares* que poderão ser adquiridas por qualquer pessoa interessada, sem muitas exigências, bastando possuir o recurso financeiro (CHECK..., 2019).

3.1.4 Ferramentas Tecnológicas das Guerras Cibernéticas

Neste item, destacaremos algumas ferramentas tecnológicas que foram utilizadas no desenvolvimento de armas cibernéticas.

3.1.4.1 Inteligência Artificial na Cibernética

A IA e o aprendizado de máquina vêm se destacando dentre as ciências da tecnologia da informação com grande tendência à aplicação na criação de novas tecnologias. Em se tratando de tecnologias cibernéticas, suas técnicas são amplamente utilizadas para o desenvolvimento de soluções de problemas nas indústrias da cibersegurança, porém participa também dos contextos de ameaças, isto é, serve a defensores e a invasores (MISTRY, 2018). Há técnicas de IA de reconhecimento de padrões que "aprendem" os comportamentos recorrentes nos dados da rede e nos *feeds*[20] de inteligência. Assim, os especialistas podem detectar e interromper ameaças e corrigir adequadamente.

19 É o meio pelo qual hackers tentam conseguir informações pessoais dos usuários por meio dos e-mails.

20 São listas de atualização de conteúdo de um determinado sítio.

O aprendizado de máquina é utilizado para detectar incoerências no modo cada vez mais rápido como o *malware* criptografa os arquivos alvos e permite o bloqueio de arquivos indesejáveis antes que atinjam seus objetivos. Ter a certeza de que os arquivos interceptados são realmente "maliciosos" é também uma tarefa desafiadora. Então, essas ferramentas de IA costumam ser usadas em conjunto com análises temporais de execução para ratificar que o bloqueio foi feito devidamente. Os sistemas de segurança cibernética usam técnicas de IA que "aprendem" com as experiências e identificam padrões anormais quando aparecem no ecossistema de segurança cibernética. Essas ferramentas permitem que sejam atualizados continuamente e melhorados à medida em que disponibilizam *feedbacks* das análises de ameaças (MISTRY, 2018).

Por outro lado, as tecnologias de IA podem também ser usadas para ataques cibernéticos impactantes. O *WannaCry*, *malware* que interrompeu um terço das operações do Serviço Nacional de Saúde da Inglaterra, apresentou falhas quanto ao tempo despendido para ser percebido logo após a infecção. Segundo especialistas, tal problema não ocorreria caso fossem utilizadas técnicas de "aprendizagem" de IA na rede alvo. Os invasores teriam acesso ao comportamento do usuário e a outros recursos que dificultariam a identificação do *malware*. Logo, a IA aumenta a possibilidade de ações que contribuem efetivamente para a cibersegurança, mas cria novas vulnerabilidades para ataques de adversários. As técnicas mais sofisticadas de IA e aprendizado de máquina são utilizadas em sistemas, garantindo-lhes boa segurança, mas, em contrapartida, as empresas empregarão esses mesmos conhecimentos de aprendizado de máquina e IA para implementar um cenário de ameaças (MISTRY, 2018).

No futuro, temos a certeza de que os algoritmos de IA em dinâmica evolução vão continuar a ser empregados, tanto pelos invasores – buscando vulnerabilidades, desenvolvendo *malwares* cada vez mais sofisticados e tornando cada vez mais real a possibilidade de utili-

zação para ciberataques – quanto pelos defensores – para a cibersegurança, implementando as soluções para aquelas ameaças, preventivamente ou interceptando os ataques.

No festival de ciência e tecnologia *Kaspersky Geek Picnic*[21], o futurólogo francês Jean-Christophe Bonis, ao se referir às principais armas tecnológicas do século XXI, afirmou:

> Nelson Mandela escreveu em 1995 que a arma principal do século XXI será a informação, que substituirá armas nucleares e outras armas de destruição em massa do século XX. Mas, na minha opinião, tais armas serão sistemas de inteligência artificial, pois para funcionar, ao invés de bomba atômica, não precisam nem de urânio, nem de usinas, nem outras coisas difíceis de receber, mas somente de silício e eletricidade (CIENTISTAS..., 2017).

A fala do futurólogo, portanto, ratifica a importância da IA nos conflitos da atualidade.

3.1.4.2 Segurança na velocidade das técnicas do DevOps[22], Desenvolvimento e Operações

Atualmente, a arquitetura resiliente e baseada em nuvem é utilizada e tem se mostrado promissora, pois executa os recursos armazenados e os devolve ao usuário por meio de *software*. Muitas cargas de trabalho de organizações são executadas na nuvem e a segurança dos dados em servidores virtualizados precisa ser muito bem idealizada, já que esses dados são processados por centrais de outras empresas, que podem estar em diversos locais (CHECK..., 2019).

As ameaças à computação na nuvem incluem as já existentes na computação moderna: *malwares* e outros ataques, como as ameaças persistentes avançadas (APTs)[23]. O ata-

21 *Kaspersky Geek Picnic*: O maior festival internacional científico e popular dedicado às tecnologias modernas, à ciência e à criatividade.

22 É uma metodologia da linha de desenvolvimento de *software* que utiliza a comunicação para integrar desenvolvedores (dev) de *software* e profissionais de infraestrutura (ops) de TI. Disponível em: <https://gaea.com.br/o-que-e-devops-conceito/>. Acesso em: 2 out. 2020.

23 APT é um ataque de longo prazo que visa localizar e explorar informações altamente confidenciais.

que visa atrapalhar as defesas de rede, atingindo as vulnerabilidades no *stack*[24] de computação, adulterando e divulgando os dados sem autorização (RED HAT, 2020).

Não há ainda uma solução eficiente que garanta essa segurança, mas, segundo os pesquisadores do *Check Point* (2019), é importante que as pessoas que trabalham nas organizações desses serviços mantenham seus conhecimentos atualizados para evitar os novos riscos, já que as organizações têm na nuvem o principal ambiente para a execução da maioria de sua carga de trabalho.

De acordo com esses pesquisadores, o nível de segurança na nuvem ainda é considerado baixo, sendo realizada de forma que chamaram de "reflexão tardia nas implementações na nuvem". Eles sugerem soluções mais confiáveis, empregando recursos computacionais, como arquiteturas flexíveis, roteadores e *switches* que permitam que os sistemas se adaptem dinamicamente de acordo com a demanda de recursos computacionais do usuário e tecnologias com alto grau de resiliência, ou seja, que sejam capazes de se auto-organizarem ao se depararem com situações difíceis, para que consigam suportar a carga de trabalho. Afinal, são máquinas virtuais que trabalham sobre centenas de redes, acessando milhares de volumes de disco.

É preciso manter uma postura atenta e crítica, garantindo que todos os pontos cruciais da solução sejam permanentemente verificados quanto às falhas. Dessa forma, os serviços na área de TI têm que estar preparados para a segurança e o aumento significativo da base de amostragem, ilimitadamente, sendo esperado que essa adaptação se faça com a rapidez e a iteratividade do DevOps (ARRUDA, 2013).

A interconectividade das infraestruturas em rede se constitui em uma vulnerabilidade que permite avistar a possibilidade da ciberguerra, por causa da quantidade de perturbações que podem atingir as redes, podendo gerar problemas em cascata, que fugiriam do con-

24 *Stack*: um conjunto de soluções, também conhecido como pilha de soluções ou pilha de *software*.

trole dos administradores da rede ou dos governos. Nesse sentido, "os avanços na tecnologia da informação e da comunicação assim aumentaram o potencial para um desastre maior nas infraestruturas críticas por ter aumentado enormemente a possibilidade de riscos locais se transformarem em riscos sistêmicos" (CAVELT, 2011, p. 13 *apud* LOBATO; KENKEL, 2015). Sendo assim, a possível conexão de milhares de novos aparelhos à internet (o uso de dispositivo IoT) com suas conexões de redes e armazenamento de informações em nuvem cria também fragilidades quanto à segurança que os dispositivos IoT exigem. A estimativa é que cerca de 50 bilhões de dispositivos e sensores deverão estar conectados à internet, em todo o mundo, até o final de 2030 (SECTIGO, 2020).

O relatório do estudo e o infográfico publicados pela Sectigo[25] (2020) apresentam a evolução e a complexidade de muitas das vulnerabilidades e ataques a dispositivos IoT, além das ciberdefesas desenvolvidas pelas organizações para combatê-los. Para tanto, a Sectigo realizou um estudo nomeado “Evolução dos Ataques”, em que verificou os ataques cibernéticos e as tecnologias de segurança que foram desenvolvidas como resposta, a partir de 2005, mostrando que a evolução dessa tecnologia indica uma corrida armamentista. Os ataques (IoT) foram classificados em três épocas distintas, de acordo com algumas das características apresentadas a seguir:

a) A Era da Exploração (2005-2010): exploração do potencial com o objetivo de danificar a IEC e a vida; IoT inicial desconsiderou a segurança, estabelecendo seguranças rudimentares; e os ataques se limitaram a *malwares* e vírus que atacavam sistemas que utilizavam o *Windows (SECTIGO, 2020);*

b) A Era do Aproveitamento (2011-2018): os cibercriminosos se preocuparam com o potencial lucrativo e prejudicial de atacar a IoT; os ataques foram disparados para atingir maior número de alvos, causando danos mais expressi-

25 Empresa de soluções automatizadas de gerenciamento de identidade digital e segurança na *web*.

vos; e em relação à preocupação com a segurança, as organizações se prepararam para enfrentar o ataque com o auxílio dos *hackers white hat*[26], que mostram possíveis vulnerabilidades da IoT e, com seus conhecimentos, auxiliam na defesa preventivamente. Com as defesas fortalecidas, os cibercriminosos buscam formas novas de ataques (SECTIGO, 2020);

c) A Era da Proteção (2019): os governos começaram a se preocupar com a criação e a promulgação de regras para proteger os ativos da IoT; a insegurança da conectividade dos dispositivos é um complicador, porque as vulnerabilidades encontradas podem permitir a criação de *botnets* e usá-las para crimes cibernéticos; e o relatório "451 Research Enterprise IoT Budgets and Outlook2" mostra que as organizações estão aplicando 51% dos seus recursos em pesquisas em tecnologias e em programas voltados para a segurança (SECTIGO, 2020).

Alan Grau[27] enfatizou a importância de garantir a segurança dos sistemas IoT, tanto para estruturas pessoais quanto para as governamentais. Segundo ele, há uma espécie de batalha de "gatos e ratos" entre os cibercriminosos e as empresas e governos. Enquanto os últimos se esforçam na proteção da conectividade das coisas, os cibercriminosos aprimoram as suas técnicas de ataque aos alvos vulneráveis. Para Alan Grau, esse é o início da Era da Proteção. (SECTIGO, 2020).

26 *White hat*: refere-se a um hacker ético ou especialista em segurança de computadores.

27 Alan Grau, vice-presidente de soluções de IoT / Embedded da Sectigo.

4 ANÁLISE DAS GUERRAS CIBERNÉTICAS EXAMINANDO AS CIBERARMAS EM 2020

No começo de 2020, com o aumento das tensões entre EUA e Irã e a ocorrência de ciberataques no mundo, começou a ser cogitada, nas redes sociais, a possibilidade de acontecer a 1ª Ciberguerra Mundial. Fabio Assolini, pesquisador de segurança da *Kaspersky,* em entrevista ao TecMundo no dia 27 de fevereiro de 2020, quando questionado sobre essa expectativa, afirmou estar certo de que os próximos conflitos vão ter um forte potencial digital, seja por ação das pessoas dos países engajados ou por resposta governamental (ASSOLINI, 2020).

O fato de os Estados e as infraestruturas estarem conectadas é um facilitador para os ciberataques. Outro atrativo é a negativa da origem do ataque, isto é, os ataques são feitos e a origem sempre é negada. De acordo com Assolini (2020), nenhum país nunca assumiu a autoria de um ataque e os governos se beneficiam disso. Ainda segundo o autor, os ataques já ocorridos são suficientes para que se tenha uma ideia do que pode vir a acontecer. Ele afirmou que os países com maior poderio bélico – como EUA, China e Rússia – reconheceram a importância da incorporação da cibernética à guerra e investiram fortemente em pesquisas e treinamento, adquirindo *know how* em técnicas de ataque e de defesa.

Assolini (2020) citou a Coreia do Norte como exemplo de um país que não tem grande poderio bélico, mas que preferiu investir na área cibernética. Em relação ao Brasil, afirmou que ainda somos pouco desenvolvidos ciberneticamente, mas que estamos apresentando grandes melhoras e temos investido mais nesses conhecimentos, embora continuemos com uma defesa ainda não proativa, apenas reagindo a incidentes já acontecidos. Segundo ele, os sistemas de defesa têm que ser proativos e a utilização dos sistemas redundantes[28] funcio-

28 Sistemas redundantes: utilizam a repetição de componentes críticos para o funcionamento de um serviço, ampliando a confiabilidade. Em caso de falha que desabilite o siste-

nais é essencial. Discorreu ainda sobre a tendência de aumento de ataques com "indisponibilidade de serviço", cujo dano é aumentado por reações instintivas e erradas de usuários, que quando se deparam com o problema, reagem desconectando o computador da internet. Lembrou que o *Stuxnet* atuou em sistemas não conectados à internet.

Perguntado sobre o que é mais difícil: atacar ou defender, o autor esclareceu que o ataque é mais fácil tecnicamente, pois basta encontrar brechas nas ferramentas tecnológicas utilizadas. Para a defesa, por outro lado, o especialista tem que entender as técnicas empregadas pelo atacante, avaliar e desenvolver os recursos defensivos. Entretanto, enfatizou a necessidade de investimento dos governos nas duas estratégias (ASSOLINI, 2020).

4.1 Ataques cibernéticos

Apresentaremos, neste item, as análises referentes a dois ataques cibernéticos ocorridos recentemente, nos quais houve acusação de tentativa de roubo de propriedade intelectual.

4.1.1 Suposto ataque da Rússia à Londres, EUA e Canadá

Nada mais atual em termos de ataques cibernéticos do que a informação adquirida por meio dos noticiários que, no dia 16 de julho deste ano, houve acusações do Reino Unido, EUA e Canadá de que um grupo de *hackers* russos teria atacado organizações britânicas, canadenses e estadunidenses para roubar os resultados de suas pesquisas sobre o desenvolvimento de uma vacina contra o Sars-Cov-2 (REINO..., 2020).

ma primário, um outro sistema secundário o substitui.

Não há ainda muitas informações disponíveis sobre o ataque do dia 16 de julho de 2020, mas Mariana Pereira, diretora de marketing da *Darktrace*,[29] que assessora muitas empresas envolvidas com a área da saúde, em entrevista para a GloboNews, dia 17 de maio de 2017, informou que outros ataques semelhantes aconteceram ao sistema de saúde de Londres, e que logo foram percebidos pelos técnicos. Viram que algo estranho ocorria nos sistemas e que a velocidade com que se espalhou pelas estruturas computacionais de hospitais e organizações ligadas à saúde mundo afora era incrível. Segundo ela, foi utilizada uma vulnerabilidade conhecida e complexa do ecossistema digital, porque foi direcionada às conexões IoT, que apresentam muitos pontos de fragilidade que podem ser atingidos.

Quanto à previsão do ataque, considerando que a vulnerabilidade não era desconhecida, ela ressaltou que, como em qualquer outro caso de exploração de ponto vulnerável, não foi possível reagir com as defesas já existentes, tendo em vista que os ataques estão cada vez mais inovadores e sofisticados. Ressaltou que os sistemas de defesa se apoiam em conhecimentos de IA e continuam buscando novas atividades nessa área que estão fora dos padrões comuns, mas que não existe um manual básico com orientações de defesa. Sabe-se que a IA mantém os defensores um passo à frente e funciona como o sistema imunológico humano que defende o corpo de intrusos inoportunos, defendendo o ecossistema virtual da mesma forma nesses processos que não podem ser acompanhados pelos humanos (PEREIRA, 2017).

4.1.2 Ataque atribuído à China pelos EUA

No dia 21 de julho, o Serviço de Inteligência dos EUA, por meio do Departamento de Justiça, do *Federal Bureau of Investigation* (FBI), da Agência de Segurança Cibernética e de Infraestrutura (CISA) e da divisão do Departamento de Segurança Interna, responsabilizaram

29 *Darktrace*: empresa de segurança da informação em Londres.

dois *hackers* chineses, a serviço da inteligência do governo chinês, por ciberataques para tentar roubar pesquisas e propriedades intelectuais relativas à pesquisa para produção de vacinas para a Covid-19. Alguns ataques àquelas instituições já haviam sido percebidos desde 3 de janeiro, e teriam sido feitos por *hackers*, pesquisadores e estudantes (CHINA..., 2020).

O ataque não foi assumido pelas autoridades chinesas, o que pode ser um complicador nas relações já complexas entre os dois países, com as acusações dos EUA à Pequim de retardar informações sobre a epidemia e, portanto, considerando a China "responsável" pela disseminação do vírus pelo mundo e, consequentemente, pela morte de centenas de milhares de pessoas, além de responsabilizá-la pela atual crise econômica (CHINA..., 2020).

Ainda não foram mostradas evidências dos ataques, mas os órgãos de defesa dos EUA se comprometeram a divulgar fatos específicos das ameaças. Afirmam que a atuação dos chineses coloca em risco a segurança das curas encontradas. A China respondeu que defende severamente a segurança cibernética e é alvo de ataques cibernéticos: “Combatemos firmemente todos os tipos de ataques cibernéticos conduzidos por *hackers*. Estamos liderando o mundo no tratamento da Covid-19 e na pesquisa de vacinas. É imoral atacar a China com boatos e calúnias na ausência de qualquer evidência” (CHINA..., 2020).

Diante dos fatos expostos, alguns pesquisadores citaram como prováveis os seguintes ataques para o ano de 2020**:**

a) A nova guerra fria cibernética – A guerra comercial entre EUA e China e a dissociação de suas economias indicam a possiblidade de ocorrência de nova *guerra fria* no espaço cibernético. Os ciberataques se darão como conflitos por procuração[30], comuns na Guerra Fria, para evitarem o enfrentamento entre as duas superpotências com armas nucleares (CHECK..., 2019);

30 Conflito armado em que dois países usam um terceiro como intermediário ou substituto para evitar lutas diretas entre si.

b) As *Fake New*s 2.0 (ou notícias "fraudulentas" 2.0) nas eleições nos EUA em 2020 – Os candidatos estadunidenses pretendem utilizar projetos com técnicas de IA para criar meios de influenciar nas eleições de 2020. Fato já constatado nas eleições de 2016 (CHECK..., 2019);

c) Ciberataques a empresas de IEC continuarão a aumentar e essas empresas de serviços continuarão sendo alvo de ataques, como os realizados nos EUA e na África do Sul em 2019 (CHECK..., 2019).

Os fundamentos para as guerras cibernéticas já estão determinados e os países admitem os sérios riscos à segurança nacional advindos da utilização de armas cibernéticas, tanto que ameaçam defender-se com ataques nucleares (TRINDADE, 2019). Como exemplo, apontamos o ataque físico de Israel à Gaza em 2019, citado na revista Época Negócios em 08 de maio do mesmo ano. Esse, segundo a *Wired*[31], foi o primeiro caso de ataque como resposta que foi assumido pelas Forças Armadas de Israel ao bombardearem um prédio que eles diziam ser ocupado por um grupo de *hackers* do Hamas, embora já tivessem conseguido eliminar o vírus.

A Forças Armadas israelenses alegaram o seguinte sobre o ataque: "Nós frustramos uma tentativa de ofensiva cibernética do Hamas contra alvos israelenses. Após o sucesso de nossa operação de defesa cibernética**,** atingimos um prédio onde os agentes do Hamas trabalham. HamasCyberHQ.exe foi removido" (O QUE..., 2019). No que diz respeito às implicações, existem duas visões sobre as consequências do ataque:

a) Alguns pesquisadores o veem como evolução da chamada **guerra híbrida** – guerras cibernética e física – que estaria abrindo perigoso precedente para modos de reação contra *hackers*;

31 *Wired* é uma revista norte-americana publicada mensalmente e com sede em São Francisco, Califórnia, que cobre temas como tecnologia, ciência, entretenimento, *design* e negócios, seus diferentes subtópicos e seu impacto na sociedade, cultura, economia e política.

b) Outros pesquisadores veem como um incidente pontual que aconteceu naquele contexto.

EUA, Rússia e China são países desenvolvidos tecnologicamente, e estão na liderança no que se refere a armas virtuais, seguidos de Israel e Reino Unido. Segundo Adam Segal, diretor do programa de políticas digitais e de ciberespaço do *think tank Council on Foreign Relations*[32], França e Alemanha também se incluem nessa corrida armamentista. Essas potências ainda não se atacaram, mas sabem dos prejuízos que uma pode causar a outra. Os EUA, por exemplo, já identificaram a presença de *hackers* russos em seus sistemas de IEC, podendo atacar o sistema de fornecimento de energia que atende a milhões de estadunidenses. A partir disso, os estadunidenses investem na criação de ações cibernéticas nas redes russas e se preparam para uma reação à altura, com danos proporcionais aos sofridos, quando necessário. Estabelece-se, assim, uma corrida armamentista (TRINDADE, 2019).

Jake Williams[33] afirma que os países criam armas cibernéticas, mas nem sempre as usam. O *hacker* está ciente dos danos reais que podem ser causados quando um ataque cibernético é instalado no sistema de infraestrutura e declara que "ainda que um *hacker* tenha estabelecido acesso a um sistema, isso não significa que ele irá executar alguma ação. Ele pode estar apenas reunindo dados de inteligência, por exemplo" (O QUE..., 2019).

Os ataques têm que ser avaliados antes de serem realizados, pois as organizações industriais e militares modernas também estão se equipando com armas com mesmo potencial de dano, utilizando tecnologias semelhantes e conexão na mesma rede global. Logo, a resposta pode funcionar de modo semelhante, não valendo a pena efetuá-los (CHINA..., 2020).

É possível perceber que, apesar de alguns ataques e algumas tecnologias para ataques e propostas de defesas terem sido apresentados, vários questionamentos ainda continuam

32 Um *think tank* em Nova Iorque, EUA, voltado para a política externa e assuntos internacionais.

33 Jake Williams, ex-membro da Agência de Segurança Nacional dos EUA.

sem resposta. É nesse momento que a *Cyber Intelligence,* ou Inteligência Cibernética, entra em ação. Ela tem o objetivo de orientar as organizações para que consigam, da melhor forma, detectar e analisar as ameaças virtuais, e propor ações proativas eficientes e eficazes. Portanto, a Inteligência Cibernética é responsável pela produção de conhecimentos, prevendo possíveis ameaças virtuais, considerando todo o ciberespaço, visando à tomada da melhor decisão quando detectados ataques e desferindo as melhores defesas de modo imediato (WENDT, 2011).

Em vista disso, podemos perceber que a guerra se modificou com o passar do tempo em função do avanço tecnológico, seus novos elementos passaram a ser valorizados e as tecnologias ganharam importância para a nova batalha no campo cibernético. Mudaram as armas, as táticas, os meios, as relações civis e militares. Assim, o setor cibernético se torna um dos mais importantes neste século.

4.2 Manual de Tallin

Com essa realidade, identificados os fatores que fundamentam a ciberguerra, a regulação internacional das ações e reações e as penalizações no ciberespaço ganham importância, pois é necessário que se imponham limites e se estabeleça o que são atos repressivos juridicamente legais quando diante de ataques cibernéticos.

Até o momento, não foram estabelecidas resoluções ou leis internacionais que especifiquem como lidar com as ciberguerras (DIPERT, 2010 *apud* AYRES, 2020), como acontece com as guerras tradicionais, em que tratados e acordos regulam como elas devem ocorrer. Devido à indefinição do que seja a ciberguerra, e ainda pela dificuldade em se ter a precisão de identificar o agressor, não foi determinada uma forma de ação internacional, isto é, não há

uma segurança jurídica que oriente uma tomada de decisão nos casos desses ataques (FERNANDES, 2012 *apud* AYRES, 2020).

A proposta de uma regulamentação foi apresentada em 2009, logo após ser detectado o *Stuxnet*. O *Cooperative Cyber Defense Center of Excellence* (CCDCOE) reuniu especialistas para que fosse formulado o *Tallinn Manual on the International Law Applicable to Cyber Warfare,* que instrui como será o emprego do Direito Internacional no julgamento dos atos da guerra cibernética. O grupo era formado por 20 advogados civis e militares de países da Organização do Tratado do Atlântico Norte (OTAN)[34], por peritos especialistas em Segurança Cibernética, por representantes do Cibercomando dos EUA e pelo Comitê Internacional da Cruz Vermelha (FEITOSA, 2017).

O resultado do trabalho foi um documento com 95 regras determinando como deveriam se dar os conflitos com armas advindas do emprego das TI, referindo-se a ataques, fazendo valer sobre eles os princípios do Direito Internacional. Seus autores ressaltaram que o documento final não pretende ser um conjunto de leis internacionais (SCHMITT, 2013 *apud* FEITOSA, 2017). Em entrevista concedida à ABC News[35], momentos antes da apresentação do manual, Michael Shmitt, advogado militar que liderou seu desenvolvimento, declarou: "Todo mundo está vendo a internet como o Oeste selvagem […] O que eles esquecem é que o direito internacional se aplica a armas cibernéticas como a qualquer outro tipo de arma." (FEITOSA, 2017, p. 44).

O texto elaborado não foi oficializado e não se constituiu em doutrina regular da OTAN, entretanto não havendo outro documento oficial, ele representa um consenso entre os especialistas, que servirá para dar legitimidade aos conflitos, principalmente, aqueles em que estão envolvidos os países membros da organização. De acordo com os autores, o manual está

34 OTAN é uma aliança militar entre os países da Europa e da América do Norte.

35 A entrevista concedida à ABC News pode ser consultada em: <http://abcnews.go.com/International/arming-virtual-battle-dangerousrules-cyberwar/story?id=18888675&page=2> ou em: <http://www.federalnewsradio.com/86/3038173/In-Depth-interviews---September- 14>. Acesso em: 2 nov. 2020.

baseado na interpretação do Direito Internacional vigente (SCHMITT, 2013 *apud* FEITOSA, 2017).

5 CONCLUSÃO

Nesse trabalho, pretendemos expor fatos e definições que nos permitissem responder à questão proposta como objetivo principal: a evolução da tecnologia impactou os conflitos ocorridos a partir do ano 2000? Para tal, no capítulo 2, discorremos sobre o emprego da tecnologia na guerra, expondo os conceitos relacionados à cibernética e à guerra cibernética. Fizemos, ainda, uma síntese da evolução tecnológica a partir do ano 2000, observando como ela influenciou nas estratégias e táticas de guerra, permitindo o surgimento do "espaço cibernético".

No capítulo 3, apresentamos os ataques cibernéticos contra a Estônia (2007), a Geórgia (2008), o Irã (2010), entre outros que despertaram grande interesse e levaram os Estados a entrarem em estado de atenção e a investirem em pesquisas para estarem prontos para detecção de possíveis ataques e para reações proativas diante da constatação deles. Observamos que a continuidade de ocorrências dos conflitos permite concluir que o ciberespaço expõe os países, tornando-os alvos de ciberguerras devido à sua grande vulnerabilidade em termos de segurança, por ter como base a internet. Além disso, pudemos constatar, por meio dos fatos apresentados referentes aos ataques de negativa de serviços contra a Estônia e a Geórgia, as limitações da capacidade de defesa cibernética desses países devido à insuficiência tecnológica para deter os ataques às suas redes.

Abordamos também o vírus *Stuxnet*, responsável por atacar a rede da usina nuclear iraniana. A partir de sua análise, foi possível concluir que a internet não precisa, necessariamente, ser utilizada para um ataque, visto que esse vírus foi espalhado pela inserção de *pen drives* em computadores particulares. A tecnologia utilizada foi o desenvolvimento de um programa de computadores que atingia o sistema operacional SCADA, utilizado pelas usinas de urânio no Irã em suas centrífugas. Pudemos observar, ainda, que as armas

cibernéticas não são claramente violentas, mas podem produzir grandes danos aos países e alteram os conceitos do que até então conhecemos como guerra e paz.

Dessa forma, compreendemos que os conflitos apresentados no terceiro capítulo tiveram extrema importância, porque se constituíram no ponto inicial para o que, atualmente, denominamos como “guerra cibernética”. E, por fim, concluímos o capítulo discorrendo sobre a importância da IA no aumento da ocorrência de ataques cada vez mais sofisticados, sendo necessários esses mesmos conhecimentos para que as ciberdefesas sejam elaboradas eficientemente. O aprendizado de máquina e IoT também se destacam nos ataques da atualidade.

Os ataques mais atuais, apresentados no capítulo 4, se tornaram cada vez mais sofisticados, de difícil detecção e interceptação, concretizados graças à evolução dinâmica da área do conhecimento da IA. Porém, ao observarmos o trabalho por inteiro, podemos inferir que uma ciberguerra ainda não ocorreu, pois os conflitos apresentados são constituídos por ataques cibernéticos não contínuos, não coordenados e não são instrumentais. Para que um conflito seja considerado uma guerra, é preciso que seja violento, instrumental, tenha um propósito político e não seja um ato isolado.

A constante evolução das tecnologias da informação e comunicação, suas prováveis vulnerabilidades, a virtualização dos serviços tendo como consequência a vulnerabilidade das IEC nacionais e o potencial destrutivo das armas cibernéticas tornaram a ciberguerra uma preocupação central no contexto da defesa nacional e indicam a existência de uma corrida armamentista, considerando que ela é utilizada para defesa e para ataque. À medida que se cria todo um aparato de defesa, atualmente com IA, os operadores “maliciosos” utilizam tecnologias semelhantes para novos ataques, que são favorecidos, por exemplo, pelos atuais sistemas de IoT, devido ao alto grau de conectividade apresentado.

A automatização dos conflitos tornou importante e essencial a preocupação com as seguranças cibernéticas dos países. Se os ataques vão ter continuidade ou não, é inconclusivo. Essa é a opinião também dos que a estudaram nos últimos anos. O que podemos esperar é que ataques cibernéticos continuem acontecendo e que as guerras tenham sempre um apoio sobre ferramentas tecnológicas, podendo adotar uma estratégia híbrida.

A ciberguerra possui características próprias, mas a que mais se destaca está relacionada ao "sonho" de que a tecnologia contribuirá para a erradicação ou a redução da violência, além da diminuição da letalidade em combates, pelo menos por aqueles que apresentam armas tecnologicamente superiores. Tais características exigem também necessidade de regulação dos comportamentos no ciberespaço, com demarcação dos limites dos Estados e descrição das ações legais e penalidades possíveis, para que haja repreensão dos ataques cibernéticos que atentem contra a soberania no ciberespaço.

A relação entre a guerra, os desenvolvimentos tecnológicos e a política foi e ainda está sendo alterada em função do avanço da tecnologia. Foi possível perceber que a guerra cibernética é representada por desenvolvimento técnico-científico cibernético, propiciado pela criação e evolução dos computadores, a conexão deles em redes e o desenvolvimento das ciências da informação e comunicação.

Podemos concluir, portanto, ratificando nossa hipótese de que o modo de realizar conflitos tem acompanhado a evolução tecnológica a partir do ano 2000, isto é, os avanços tecnológicos, na sociedade moderna, impactam a forma de fazer a guerra, e propiciam uma corrida armamentista no mundo, no ciberespaço, no último milênio. Neste trabalho, ficou evidente a relação entre guerra, ciência e tecnologia, constatada pela agregação da cibernética à guerra.

REFERÊNCIAS

AGOSTINI, Marcos Tocchetto. **A cibernética sob a ótica do fenômeno da guerra e da agenda de segurança**. 2014. 92 f. Monografia (Graduação em Relações Internacionais) - Departamento de Ciências Econômicas e Relações Internacionais, Universidade Federal de Santa Catarina, 2014. Disponível em: <https://repositorio.ufsc.br/handle/123456789/124695>. Acesso em: 13 maio 2020.

ARRUDA, Eduardo Nascimento de. **Identificando o grau de dependência da adesão à computação em nuvem**. 2013. 192 f. Dissertação (Mestrado em Engenharia Elétrica) – Programa de Pós-Graduação em Engenharia Elétrica, Universidade Federal de Pernambuco, Recife, 2013. Disponível em: <https://www.ufpe.br/documents/39830/1359036/241_EduardoArruda/1e79f5bf-1bb4-4070-8ea1-9308f93a066d>. Acesso em: 20 jun. 2020.

ASSOLINI, Fábio. A 3ª guerra mundial ou a 1ª guerra cibernética? **TecMundo**, São Paulo, 27 fev. 2020. Entrevista concedida a Felipe Payão. Disponível em: <https://www.tecmundo.-com.br/seguranca/150629-3-guerra-mundial-1guerra-cibernetica.htm>. Acesso em: 20 jun. 2020.

AYRES, Danielle; GRASSI, Jéssica. Ciberguerra*:* o que é e quais as suas possibilidades. **Politize**, Joinville, 2020. Disponível em: **<**https://www.politize.com.br/ciberguerra/>. Acesso em: 08 jul. 2020.

BAKER, Stewart *et al*. **Sob fogo cruzado**: infraestrutura crítica na era da guerra cibernética. [S. l.]: McAfee, 2013. p. 1-42. Disponível em: <http://www.mcafee.com/br/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf> *apud* AGOSTINI, Marcos Tocchetto. **A cibernética sob a ótica do fenômeno da guerra e da agenda de segurança**. 2014. 92 f. Monografia (Graduação em Relações Internacionais) - Departamento de Ciências Econômicas e Relações Internacionais, Universidade Federal de Santa Catarina, 2014. Disponível em: <https://repositorio.ufsc.br/handle/123456789/124695>. Acesso em: 13 maio 2020.

BARBOSA, Rubens. **Guerra cibernética.** [S.l]: Instituto Millenium, 2019. <https://www.institutomillenium.org.br/guerra-cibernetica/>. Acesso em: 12 maio 2020.

BARRY, R. Schneider; GRINTER, Lawrence E. **Battlefield of the future**: 21st Century warfare issues. Alabama: University Press of the Pacific, 1998 *apud* LUNA, Salomão Melquiades *et al*. Avanços da ciência e da tecnologia sobre guerra, sua modernização e novas estratégias: aspectos importantes para defesa da Amazônia Azul. In: SIMPÓSIO DE PESQUISA OPERACIONAL & LOGÍSTICA DA MARINHA, 18., 2016, Rio de Janeiro. **Desenvolvimento Logístico e Pesquisa Operacional: Base Sólida de Defesa da Amazônia Azul**. *Proceedings*... [S. l.]: [s. n.], 2016. Disponível em: <https://www.proceedings.blucher.com.br/article-details/avanos-da-cincia-e-da-tecnologia-sobre-a-guerra-sua-modernizao-e-novas-estratgias-aspectos-importantes-para-defesa-da-amaznia-azul-22731>. Acesso em: 20 jun. 2020.

VIGA – TECNOLOGIA EM INFRAESTRUTURA. **Já ouviu falar do Stuxnet, o maior vírus da história.** [S. l.]: Viga, 2017. Disponível: <https://viga.com.br/voce-ja-ouviu-falar-do-*Stuxnet*-o-maior-virus-da-historia/>. Acesso em: 01 jun. 2020.

BOUSQUET, Antoine J. **The scientific way warfare**: order and chaos on the battlefields of modernity. Nova York: Columbia University Press, 2009 *apud* LOBATO, Luisa; KENKEL, Kai Michael. A ciberguerra é moderna! Uma investigação sobre a relação entre tecnologia e modernização na guerra. **Contexto Internacional**, Rio de Janeiro, v. 37, n. 2, maio/ago. 2015. Disponível em: <https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-85292015000200629>. Acesso em: 1 out. 2020.

BRASIL. Ministério da Defesa. **MD35-G-01**: Glossário das Forças Armadas. Brasília: Ministério da Defesa, 2015. Disponível em: <https://bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf>. Acesso em: 6 nov. 2020.

CARREIRO, Marcelo. A guerra cibernética: *cyberwarfare* e a securitização da Internet. **Revista Cantareira**, Niterói, n.. 17, jul./dez., 2012. Disponível em: <https://periodicos.uff.br/cantareira/article/view/27898>. Acesso em: 13 jun. 2020.

CARVALHO, Alessandra Cordeiro. **Securitização do ciberterrorismo e o posicionamento estratégico de defesa cibernética dos Estados Unidos da América**. 2019. 101 f. Dissertação (Mestrado em Ciências Militares) - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2019. Disponível em: <http://bdex.eb.mil.br/jspui/handle/123456789/5620>. Acesso em: 20 maio 2020.

CAVAGNARI FILHO, Geraldo Lesbat. A tecnologia e a estratégia do Império. **Guerra e Ciência**, Campinas, 2002. Disponível em: <http://www.comciencia.br/dossies-1-72/reportagens/guerra/guerra15.htm>. Acesso em: 26 maio 2020.

CAVELTY, Myriam Dunn. **Cyber-security and threat politics**: US efforts to secure the information age. Milton Park: Routledge, 2009 *apud* LOBATO, Luisa; KENKEL, Kai Michael. A ciberguerra é moderna! Uma investigação sobre a relação entre tecnologia e modernização na guerra. **Contexto Internacional**, Rio de Janeiro, v. 37, n. 2, maio/ago. 2015. Disponível em: <https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-85292015000200629>. Acesso em: 1 out. 2020.

CHECK Point alerta para uma nova "guerra fria" cibernética em 2020. **Security Report**, [S. l.], 25 out. 2019. Disponível em: <https://www.securityreport.com.br/destaques/check-point-alerta-para-uma-nova-guerra-fria-cibernetica-em-2020/#.XyMPk2hKhPY>. Acesso em: 9 jul. 2020.

CHINA nega roubo de dados de vacinas da COVID-19 e afirma: 'EUA devem parar de caluniar e difamar'. **Sputnik Brasil**, 22 jul. 2020. Disponível em: <https://br.sputniknews.com/asia_oceania/2020072215856764-china-nega-roubo-de-dados-de-vacinas-da-covid-19-e-afirma-eua-devem-parar-de-caluniar-e-difamar/>. Acesso em: 12 maio 2020.

CIENTISTAS indicam qual será a principal arma tecnológica do século XXI. **Notícias ao Minuto**, São Paulo, 18 jun. 2017. Disponível em: <https://www.noticiasaominuto.com/tech/815434/cientistas-indicam-qual-sera-a-principal-arma-tecnologica-do-seculo-xxi>. Acesso em: 1 jul. 2020.

CLARKE, Richard; KNAKE, Robert. **Cyber war**: the next threat to national security and what to do about it. New York: HarperCollins. 2010 *apud* NOGUEIRA, Michel Gomes. **Estudo de caso sobre o conflito cibernético entre a Rússia e a Geórgia**. 2018. 41 f. Monografia (Graduação em História) - Instituto de Ciências Humanas, Universidade de Brasília, Brasí-

lia, 2018. Disponível em: <https://bdm.unb.br/bitstream/10483/22858/1/2018_MichelGomes-Nogueira_tcc.pdf>. Acesso em: 01 jul. 2020.

CLARKE, Richard; KNAKE, Robert. **Cyberwar**: the next threat to national security and what to do about it. New York: HarperCollins, 2010 *apud* GAMA NETO, Ricardo Borges. Guerra cibernética / guerra eletrônica – conceitos, desafios e espaços de interação. **Revista Política Hoje**, Recife, v. 26, n. 1, 2017, p. 201-217. Disponível em: <https://periodicos.ufpe.-br/revistas/politicahoje/article/view/9180>. Acesso em: 1 jul. 2020.

CREVELD, Martin V. **Ascensão e declínio do Estado**. São Paulo: Martins Fontes, 2004 *apud* NOGUEIRA, Michel Gomes. **Estudo de caso sobre o conflito cibernético entre a Rússia e a Geórgia**. 2018. 41 f. Monografia (Graduação em História) - Instituto de Ciências Humanas, Universidade de Brasília, Brasília, 2018. Disponível em: <https://bdm.unb.br/bitstream/10483/22858/1/2018_MichelGomesNogueira_tcc.pdf>. Acesso em: 1 jul. 2020.

CREVELD, Martin Van. **The transformation of war**. New York: The Free Press, 1991 *apud* LUNA, Salomão Melquiades *et al*. Avanços da ciência e da tecnologia sobre guerra, sua modernização e novas estratégias: aspectos importantes para defesa da Amazônia Azul. In: SIMPÓSIO DE PESQUISA OPERACIONAL & LOGÍSTICA DA MARINHA, 18., 2016, Rio de Janeiro. **Desenvolvimento Logístico e Pesquisa Operacional: Base Sólida de Defesa da Amazônia Azul**. *Proceedings*... [S. l.]: [s. n.], 2016. Disponível em: <https://www.proceedings.blucher.com.br/article-details/avanos-da-cincia-e-da-tecnologia-sobre-a-guerra-sua-modernizao-e-novas-estratgias-aspectos-importantes-para-defesa-da-amaznia-azul-22731>. Acesso em: 20 jun. 2020.

DIPERT, Randall. R. The ethics of cyberwarfare. **Journal of Military Ethics**, [S. l.], v. 9, n. 4, p. 384-410, 2010 *apud* AYRES, Danielle; GRASSI, Jéssica. Ciberguerra: o que é e quais as suas possibilidades. **Politize**, Joinville, 2020. Disponível em: **<**https://www.politize.com.br/ciberguerra/>. Acesso em: 8 jul. 2020.

DUIC, Igor *et al*. **International Cyber Security Challenges**. In: INTERNATIONAL CONVENTION ON INFORMATION AND COMMUNICATION TECHNOLOGY, ELECTRONICS AND MICROELECTRONICS (MIPRO), 40., 2017, Opatija. *Proceedings...* [S. l.]: IEEE, 2017 *apud* CARVALHO, Alessandra Cordeiro. **Securitização do ciberterrorismo e o posicionamento estratégico de defesa cibernética dos Estados Unidos da América**. 2019. 101 f. Dissertação (Mestrado em Ciências Militares) - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2019. Disponível em: <http://bdex.eb.mil.br/jspui/handle/123456789/5620>. Acesso em: 20 maio 2020.

EUA acusam hackers chineses de roubar dados sobre vacina contra a Covid-19. G1 Mundo, Rio de Janeiro, 21 jul. 2020. Disponível em: <https://g1.globo.com/mundo/noticia/2020/07/21/eua-acusam-dois-hackers-chineses-de-roubar-dados-sobre-projetos-de-vacina-contra-covid-19.ghtml>. Acesso em: 22 jul. 2020.

FALLIERE, Nicolas; O MURCHU, Liam; CHIEN, Eric. W32.*Stuxnet* dossier (version 1.4). [S. l.]: Symantec, 2011. Disponível em: <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_*Stuxnet*_dossier.pdf>. Acesso em: 15 jun. 2020.

FEITOSA, Caio Vinícius Cesar. **Ataques cibernéticos:** estudo de caso STUXNET. 2017. 59 f. Projeto Final (Tecnólogo em Sistemas de Computação). – Universidade Federal Fluminen-

se, Niterói/RJ, 2017. Disponível em: <https://app.uff.br/riuff/handle/1/5630>. Acesso em: 21 maio 2020.

FERNANDES, José Pedro. Teixeira. A ciberguerra como nova dimensão dos conflitos do século XXI. **Relações Internacionais**, Lisboa, n. 33, p. 53-69, mar. 2012 *apud* AYRES, Danielle; GRASSI, Jéssica. Ciberguerra*:* o que é e quais as suas possibilidades. **Politize**, Joinville, 2020. Disponível em: **<**https://www.politize.com.br/ciberguerra/>. Acesso em: 8 jul. 2020.

FOUCAULT, Michel. Nietzsche, genealogy, history. In: BOUCHARD, D. F. (Org). **Language, counter-memory, practice**: selected essays and interviews. Ithaca: Cornell University Press, 1980 *apud* LOBATO, Luisa; KENKEL, Kai Michael. A ciberguerra é moderna! Uma investigação sobre a relação entre tecnologia e modernização na guerra. **Contexto Internacional**, Rio de Janeiro, v. 37, n. 2, maio/ago. 2015. Disponível em: <https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-85292015000200629>. Acesso em: 1 out. 2020.

GAMA NETO, Ricardo Borges. Guerra cibernética / guerra eletrônica – conceitos, desafios e espaços de interação. **Revista Política Hoje**, Recife, v. 26, n. 1, 2017, p. 201-217. Disponível em: <https://periodicos.ufpe.br/revistas/politicahoje/article/view/9180>. Acesso em: 1 jul. 2020.

HANDLER, Stephenie Gosnell. The new cyber face of battle: developing a legal approach to accommodate emerging trends in warfare. **Stanford Journal of International Law**, Stanford, Winter 2012 *apud* NOGUEIRA, Michel Gomes. **Estudo de caso sobre o conflito cibernético entre a Rússia e a Geórgia**. 2018. 41 f. Monografia (Graduação em História) - Instituto de Ciências Humanas, Universidade de Brasília, Brasília, 2018. Disponível em: <https://bdm.unb.br/bitstream/10483/22858/1/2018_MichelGomesNogueira_tcc.pdf>. Acesso em: 1 jul. 2020.

KOOPS, Bert-Jaap. Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research. In: AKHNAR, Babak; BREWSTER, Ben (eds.). **Combatting Cybercrime and Cyberterrorism**. Switzerland: Advanced Sciences and Technologies for Security Applications, 2016 *apud* CARVALHO, Alessandra Cordeiro. **Securitização do ciberterrorismo e o posicionamento estratégico de defesa cibernética dos Estados Unidos da América**. 2019. 101 f. Dissertação (Mestrado em Ciências Militares) - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2019. Disponível em: <http://bdex.eb.mil.br/jspui/handle/123456789/5620>. Acesso em: 20 maio 2020.

KUCHLER, Hannah; BUCKLE, Neil. Ataque de hackers derruba rede de energia da Ucrânia. **Folha de São Paulo: Mercado**, São Paulo, 7 jan. 2016. Disponível em: <https://m.folha.uol.com.br/mercado/2016/01/1726880-ataque-de-hackers-derruba-rede-de-energia-da-ucrania.shtml>. Acesso em: 20 jun. 2020.

KUHN, Thomas S. **O caminho desde a estrutura**: ensaios filosóficos, 1970-1993, com uma entrevista autobiográfica. São Paulo: UNESP, 2006 *apud* ROCHA, Luis Fernando. Teoria das representações sociais: a ruptura de paradigmas das correntes clássicas das teorias psicológicas. **Psicologia: ciência e profissão**, Brasília, v. 34, n. 1, p. 46-65, 2014. Disponível em: <http://dx.doi.org/10.1590/S1414-98932014000100005>. Acesso em: 12 jul. 2020.

LIANG, Qiao; XIANGSUI, Wang. **A guerra além dos limites**: conjecturas sobre a guerra e a tática na Era da Globalização. Beijing: Pla Literature and Arts Publishing House, 1999 *apud* LUNA, Salomão Melquiades *et al*. Avanços da ciência e da tecnologia sobre guerra, sua mo-

dernização e novas estratégias: aspectos importantes para defesa da Amazônia Azul. In: SIMPÓSIO DE PESQUISA OPERACIONAL & LOGÍSTICA DA MARINHA, 18., 2016, Rio de Janeiro. **Desenvolvimento Logístico e Pesquisa Operacional: Base Sólida de Defesa da Amazônia Azul**. *Proceedings*... [S. l.]: [s. n.], 2016. Disponível em: <https://www.proceedings.blucher.com.br/article-details/avanos-da-cincia-e-da-tecnologia-sobre-a-guerra-sua-modernizao-e-novas-estratgias-aspectos-importantes-para-defesa-da-amaznia-azul-22731>. Acesso em: 20 jun. 2020.

LOBATO, Luisa; KENKEL, Kai Michael. A ciberguerra é moderna! Uma investigação sobre a relação entre tecnologia e modernização na guerra. **Contexto Internacional**, Rio de Janeiro, v. 37, n. 2, maio/ago. 2015. Disponível em: <https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-85292015000200629>. Acesso em: 1 out. 2020.

LOBATO, Luisa; KENKEL, Kai Michael. Discourses of cyberspace securitization in Brazil and in the United States. Revista Brasileira de Política Internacional, Brasília, v. 58, n. 2, p. 23-43, 2015 *apud* AYRES, Danielle; GRASSI, Jéssica. Ciberguerra*:* o que é e quais as suas possibilidades. **Politize**, Joinville, 2020. Disponível em: **<**https://www.politize.com.br/ciberguerra/>. Acesso em: 8 jul. 2020.

LUNA, Salomão Melquiades *et al*. Avanços da ciência e da tecnologia sobre guerra, sua modernização e novas estratégias: aspectos importantes para defesa da Amazônia Azul. In: SIMPÓSIO DE PESQUISA OPERACIONAL & LOGÍSTICA DA MARINHA, 18., 2016, Rio de Janeiro. **Desenvolvimento Logístico e Pesquisa Operacional: Base Sólida de Defesa da Amazônia Azul**. *Proceedings*... [S. l.]: [s. n.], 2016. Disponível em: <https://www.proceedings.blucher.com.br/article-details/avanos-da-cincia-e-da-tecnologia-sobre-a-guerra-sua-modernizao-e-novas-estratgias-aspectos-importantes-para-defesa-da-amaznia-azul-22731>. Acesso em: 20 jun. 2020.

MISTRY, Bharat. Inteligência artificial: a faca de dois gumes da segurança cibernética. **Trend Micro**, [S. l.], 2018. Disponível em: <https://www.trendmicro.com/pt_br/about/newsroom/press-releases/2018/inteligencia-artificial.html>. Acesso em: 15 jun. 2020.

MOURA, José Augusto Abreu de. Estratégia naval e tecnologia. Notas de aula: Escola de Guerra Naval (EGN) - Programa de Pós-Graduação em Estudos Marítimos, Rio de Janeiro, 2014 *apud* LUNA, Salomão Melquiades *et al*. Avanços da ciência e da tecnologia sobre guerra, sua modernização e novas estratégias: aspectos importantes para defesa da Amazônia Azul. In: SIMPÓSIO DE PESQUISA OPERACIONAL & LOGÍSTICA DA MARINHA, 18., 2016, Rio de Janeiro. **Desenvolvimento Logístico e Pesquisa Operacional: Base Sólida de Defesa da Amazônia Azul**. *Proceedings*... [S. l.]: [s. n.], 2016. Disponível em: <https://www.proceedings.blucher.com.br/article-details/avanos-da-cincia-e-da-tecnologia-sobre-a-guerra-sua-modernizao-e-novas-estratgias-aspectos-importantes-para-defesa-da-amaznia-azul-22731>. Acesso em: 20 jun. 2020.

NOGUEIRA, Michel Gomes. **Estudo de caso sobre o conflito cibernético entre a Rússia e a Geórgia**. 2018. 41 f. Monografia (Graduação em História) - Instituto de Ciências Humanas, Universidade de Brasília, Brasília, 2018. Disponível em: <https://bdm.unb.br/bitstream/10483/22858/1/2018_MichelGomesNogueira_tcc.pdf>. Acesso em: 1 jul. 2020.

O QUE o ataque de Israel a hackers do Hamas significa para o futuro da guerra cibernética. **Época Negócios**, Rio de Janeiro, 8 maio 2019. Disponível em: <https://epocanegocios.globo.-

com/Mundo/noticia/2019/05/o-que-o-ataque-de-israel-hackers-do-hamas-significa-para-o-futuro-da-guerra-cibernetica.html>. Acesso em: 21 jun. 2020.

PEDRO, Antonio Fernando Pinheiro. **A nova ciber-ecologia.** [S. l.]: Ambiente Legal, 2013. Disponível em: <http://www.ambientelegal.com.br/ecologia-cibernetica/>. Acesso em: 10 jul. 2020.

PEREIRA, Mariana. Especialista conta como foi o ataque hacker ao sistema de saúde da Inglaterra. **Globo News**, Rio de Janeiro, 17 maio 2017. Disponível em: <https://g1.globo.com/globonews/estudio-i/video/especialista-conta-como-foi-o-ataque-hacker-ao-sistema-de-saude-da-inglaterra-5875891.ghtml>. Acesso em: 17 maio 2020.

RED HAT. **Como garantir a segurança na nuvem**. [S. l.]: Red Hat, 2020. Disponível em: <https://www.redhat.com/pt-br/topics/security/cloud-security>. Acesso em: 10 jul. 2020.

REINO Unido diz ter certeza de que Rússia tentou hackear dados de pesquisas de vacina contra covid-19. **G1 Mundo**, 19 jul. 2020. Disponível em: < https://g1.globo.com/mundo/noticia/2020/07/19/reino-unido-diz-ter-certeza-de-que-russia-tentou-hackear-dados-de-pesquisas-de-vacina-contra-covid-19.ghtml>. Acesso em: 27 jul. 2020.

ROCHA, Luis Fernando. Teoria das representações sociais: a ruptura de paradigmas das correntes clássicas das teorias psicológicas. **Psicologia: ciência e profissão**, Brasília, v. 34, n. 1, p. 46-65, 2014. Disponível em: <http://dx.doi.org/10.1590/S1414-98932014000100005>. Acesso em: 12 jul. 2020.

ROHR, Altieres. Saiba como age o vírus que invadiu usinas nucleares no Irã e na Índia. **G1,** Rio de Janeiro, 2 out. 2010. Disponível em: <http://g1.globo.com/tecnologia/noticia/2010/10/saiba-como-age-o-virus-que-invadiu-usinas-nucleares-no-ira-e-na-india.html>. Acesso em: 10 de junho de 2020.

ROHR, Altieres. Ucrânia tem segundo apagão elétrico causado por hackers. **G1 - Segurança Digital**, Rio de Janeiro,17 jan. 2017. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/ucrania-tem-segundo-apagao-eletrico-causado-por-hackers.html>. Acesso em: 17 jun. 2020.

RONDON, Thiago. Armas e formas de ataque das guerras cibernéticas. **Época Negócios**, Rio de Janeiro, 17 abr. 2018. Disponível em: <https://epocanegocios.globo.com/colunas/noticia/2018/04/armas-e-formas-de-ataque-das-guerras-ciberneticas.html>. Acesso em: 05 maio 2020.

ROSSATO, Isaac de Almeida *et al*. Importância do desenvolvimento cibernético para a defesa nacional no entorno estratégico. In: CONGRESSO ACADÊMICO SOBRE DEFESA NACIONAL, 14., 2019, Rio de Janeiro. **Anais**... Escola Naval: Rio de Janeiro, 2019. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xvi_cadn/aa_importanciaa_doa_desenvolvimentoa_ciberneticoa_paraa_aa_defesaa_nacionala_noa_entornoa_estrategico.pdf>. Acesso em: 5 maio 2020.

ROHR, Altieres. Saiba como age o vírus que invadiu usinas nucleares no Irã e na Índia. **G1 - Tecnologia e Games**, Rio de Janeiro, 2 out. 2010. Disponível em: <http://g1.globo.com/tecnologia/noticia/2010/10/saiba-como-age-o-virus-que-invadiu-usinas-nucleares-no-ira-e-na-india.html>. Acesso em: 01 jul. 2020.

SANGER, David. **Confront and conceal:** Obama's secret wars and surprising use of American power. New York: Crown Publishes, 2012 *apud* FEITOSA, Caio Vinícius Cesar. **Ataques cibernéticos:** estudo de caso STUXNET. 2017. 59 f. Projeto Final (Tecnólogo em Sistemas de Computação). – Universidade Federal Fluminense, Niterói/RJ, 2017. Disponível em: <https://app.uff.br/riuff/handle/1/5630>. Acesso em: 21 maio 2020.

SANTOS, Marcos Ricardo dos; VERSIGNASSI, Alexandre. Vírus entra em programa nuclear e salva o mundo. **Super Interessante**, [S. l.], 31 out. 2016. Disponível em: <https://super.abril.com.br/tecnologia/virus-entra-em-programa-nuclear-e-salva-o-mundo/>. Acesso em: 10 maio 2020.

SCHMITT, Michael N. (Ed.). **Tallinn Manual on the International Law applicable to Cyber Warfare**. Cambridge: Cambridge University Press, 2013 *apud* FEITOSA, Caio Vinícius Cesar. **Ataques cibernéticos**: estudo de caso STUXNET. 2017. 59 f. Projeto Final (Tecnólogo em Sistemas de Computação). – Universidade Federal Fluminense, Niterói/RJ, 2017. Disponível em: <https://app.uff.br/riuff/handle/1/5630>. Acesso em: 21 maio 2020.

SECTIGO. **Evolução dos ataques IoT.** [S. l.]: Ciso Advisor, 2020. Disponível em: <https://www.cisoadvisor.com.br/evolucao-dos-ataques-em-iot-indica-corrida-armamentista> Acesso em:10 out. 2020.

SILVA, Júlio Cezar Barreto Leite da. Guerra cibernética: a guerra no quinto domínio, conceituação e princípios. **Escola Guerra Naval**, Rio de Janeiro, v. 20, n. 1, p. 193-211, jan./jun. 2014. Disponível em: <https://revista.egn.mar.mil.br/index.php/revistadaegn/article/view/194>. Acesso em: 28 jun. 2020.

SINGER, P.; FRIEDMAN, Allan. **Cybersecurity and cyberwar**: what everyone needs to know. Oxford: University Press. 2014 *apud* AYRES, Danielle; GRASSI, Jéssica. Ciberguerra*:* o que é e quais as suas possibilidades. **Politize**, Joinville, 2020. Disponível em: **<**https://www.politize.com.br/ciberguerra/>. Acesso em: 8 jul. 2020.

TEIXEIRA, Duda. O 7x1 dos espiões chineses. Revista Veja, São Paulo, ed. 2340, ano 48, 2015 *apud* GAMA NETO, Ricardo Borges. Guerra cibernética / guerra eletrônica – conceitos, desafios e espaços de interação. **Revista Política Hoje**, Recife, v. 26, n. 1, 2017, p. 201-217. Disponível em: <https://periodicos.ufpe.br/revistas/politicahoje/article/view/9180>. Acesso em: 1 jul. 2020.

TRINDADE, Rodrigo. Guerra. 2.0, o futuro chegou: novas tecnologias mudam a lógica dos conflitos e exigem a revisão dos tratados, mas poucos estão a fim. **Tilt**, São Paulo, 24 ago. 2019. Disponível em: <https://www.uol.com.br/tilt/reportagens-especiais/novas-tecnologias-irao-moldar-guerra-do-amanha/#page23>. Acesso em: 7 maio 2020.

VARELLA, Luisa. Guerra cibernética e os conflitos na era da informação. **Compugraf**, São Paulo, 13 jul. 2020. Disponível em: <https://www.compugraf.com.br/guerra-cibernetica>. Acesso em: 23 out. 2020.

VIEIRA, Marcos. Operação jogos olímpicos: geopolítica, engenharia de software e STUXNET. **Infinitividades**, [S. l.], 2016. Disponível em: <http://www.infinitividades.com.br/wordpress/-jogos-olimpicos-geopolitica-engenharia-de-software-e-*Stuxnet*/>. Acesso em: 5 jun. 2020.

WALKER, Marcio Saldanha. O papel da inovação tecnológica e da gestão conjunta do setor cibernético na integração das Operações de Informação no Brasil: comparação com Estados Unidos, Reino Unido, Alemanha e Rússia. **Revista da UNIFA**, Rio de Janeiro, v. 30, n. 2, p. 24 - 35, jul./dez. 2017. Disponível em: <https://www2.fab.mil.br/unifa/images/revista/pdf/v30n2/Art-92-Papel-R6.pdf>. Acesso em: 3 maio 2020.

WENDT**,** Emerson. Ciberguerra, inteligência cibernética e segurança virtual: alguns aspectos. **Revista Brasileira de Inteligência**, Brasília: Abin, n. 6, abr. 2011. Disponível em: <http://www.abin.gov.br/conteudo/uploads/2018/05/RBI6-Artigo2-CIBERGUERRA-INTELIG%C3%8ANCIA-CIBERN%C3%89TICA-E-SEGURAN%C3%87A-VIRTUAL-alguns-aspectos.pdf>. Acesso em: 28 abr. 2020.

WIENER, Norbert. **The human use of human beings: cybernetics and society**. Londres: Free Association Books, 1989 *apud* LOBATO, Luisa; KENKEL, Kai Michael. A ciberguerra é moderna! Uma investigação sobre a relação entre tecnologia e modernização na guerra. **Contexto Internacional**, Rio de Janeiro, v. 37, n. 2, maio/ago. 2015. Disponível em: <https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-85292015000200629>. Acesso em:1 out. 2020.

ZETTER, Kim. How digital detectives deciphered STUXNET, the most menacing malware in history. **Wired**, [S. l.], 7 nov. 2011 *apud* FEITOSA, Caio Vinícius Cesar. **Ataques cibernéticos:** estudo de caso STUXNET. 2017. 59 f. Projeto Final (Tecnólogo em Sistemas de Computação). – Universidade Federal Fluminense, Niterói/RJ, 2017. Disponível em: <https://app.uff.br/riuff/handle/1/5630>. Acesso em: 21 maio 2020.