Universidade Federal Fluminense – UFF
Instituto de Estudos Estratégicos – INEST
Programa de Pós-Graduação em Estudos Estratégicos

UMA COMPARAÇÃO DAS ESTRATÉGIAS PARA SEGURANÇA E DEFESA CIBERNÉTICAS NO BRASIL E EM ISRAEL

Niterói – RJ
Novembro/2020

Universidade Federal Fluminense – UFF
Instituto de Estudos Estratégicos – INEST
Programa de Pós-Graduação em Estudos Estratégicos

UMA COMPARAÇÃO DAS ESTRATÉGIAS PARA SEGURANÇA E DEFESA CIBERNÉTICAS NO BRASIL E EM ISRAEL

Autor: Bruno Salomão Silva de Lima

Monografia apresentada ao Instituto de Estudos Estratégicos da Universidade Federal Fluminense – INEST/UFF, como parte dos requisitos necessários à obtenção do título de Especialista em Estudos Estratégicos e Relações Internacionais.

Orientador: Prof. Dr. Vitelio Marcos Brustolin

Niterói – RJ
Novembro/2020

UNIVERSIDADE FEREAL FLUMINENSE
INSTITUTO DE ESTUDOS ESTRATÉGICOS

Ficha de Avaliação de Trabalho de Conclusão de Curso

Uma comparação das estratégias para segurança e defesa cibernéticas no Brasil e em Israel

Aluno: Bruno Salomão Silva de Lima

Semestre Letivo: 01/11/2020

Avaliadores:

_____
Vitelio Brustolin – Orientador (Avaliador 01)
Departamento de Estudos Estratégicos
e Relações Internacionais

_____
Marcio Rocha – (Avaliador 02)
Departamento de Estudos Estratégicos
e Relações Internacionais

Notas dos Avaliadores	
Avaliador 01	
Avaliador 02	
Nota Final	

RESUMO

Em um mundo cada vez mais avançado, onde a vanguarda tecnológica passa a ser o diferencial entre aqueles mais desenvolvidos, no campo de batalha moderno não poderia ser diferente e tais desenvolvimentos trazem novos desafios. Um campo específico se mostra cada vez mais relevante para todas as políticas estratégicas dos Estados, é o chamado poder cibernético, no qual alguns atores globais se destacam e, dentre estes, Israel. O objetivo do trabalho é realizar uma comparação das estratégias para segurança e defesa cibernéticas no Brasil e em Israel mostrando a aproximação desses países além do campo diplomático. Para isso, foi realizada uma pesquisa bibliográfica baseada na obra de autores pertinentes ao tema em questão, a fim de responder: Como as estratégias para segurança e defesa cibernéticas realizadas por Israel podem ser comparadas com as realizadas pelo Brasil? Como resultado foi possível perceber que o Brasil necessita de investimento no desenvolvimento de tecnologias, inovações e treinamentos, a fim de se proteger de ameaças externas, além disso, a troca de experiência e desenvolvimento de parcerias com países como Israel que tem um uma vivência maior nesse tipo de ataque facilitaria o caminho na busca de minimizar tais problemas. Concluiu-se que o Brasil ainda precisa evoluir nessa batalha a fim de se tornar menos vulnerável aos ciberataques que crescem a cada dia.

Palavras-Chave: Estratégia. Tecnologia. Segurança e Defesa Cibernética.

ABSTRACT

In an increasingly advanced world, where the technological vanguard becomes the differential among those more developed, in the modern battlefield it could not be different and such developments bring new challenges. A specific field is proving to be increasingly relevant to all strategic policies of the States, is the so-called cyber power, in which some global players stand out and, among these, Israel. The objective of the work is to carry out a comparison of the strategies for cyber security and defense in Brazil and Israel, showing the approach of these countries beyond the diplomatic field. For this, a bibliographic research was carried out based on the work of authors relevant to the topic in question, in order to answer: How can the strategies for cyber security and defense carried out by Israel be compared with those carried out by Brazil? As a result it was possible to realize that Brazil needs investment in the development of technologies, innovations and training, in order to protect itself from external threats, in addition, the exchange of experience and development of partnerships with countries like Israel that have a greater experience in this type of attack it would facilitate the way in the search to minimize such problems. It was concluded that Brazil still needs to evolve in this battle in order to become less vulnerable to cyber attacks that are growing every day.

Keywords: Strategy. Technology. Cyber Security and Defense.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

TIC - Tecnologia da Informação e Comunicação
PC - Posto de Comando
SISMC2 - Sistema Militar de Comando e Controle
END - Estratégia Nacional de Defesa do Brasil
TCP - *Transmission Control Protocol*
IP - *Internet Protocol*
ARPNet - *Advanced Research Projects Agency Network*
ComDCiber - Comando de Defesa Cibernética
GSIPR - Gabinete de Segurança Institucional
EB - Exército Brasileiro
MD - Ministério da Defesa
GSI - Gabinete de Segurança Institucional
GPS - Global Positioning System
NSA - *National Security Agency*
ITU - *International Telecomunication Union*
CRE - Comissão de Relações Exteriores e Defesa Nacional
CDCIBER - Centro De Defesa Cibernética
SRCC - Serviço de Repressão à Crimes Cibernéticos
SERPRO - Serviço Federal de Processamento de Dados
NuENaDCiber - Núcleo da Escola Nacional de Defesa Cibernética

SUMÁRIO

1 INTRODUÇÃO

Quando se fala em grandes operações militares, o que imediatamente vem à mente são grandes carros de combate, canhões poderosos, aviões avançados e longas fileiras de soldados, materializando-se como a visão das batalhas mais clássicas e que renderam diversos estudos e teorias ao longo dos últimos milênios, destacando-se dentre tantos outros, Carl Phillip Gottlieb von Clausewitz (1780 - 1831) que foi um militar do Reino da Prússia que ocupou o posto de general e é considerado um grande estrategista militar e teórico da guerra por sua obra “Da Guerra”.

Os manuscritos de Clausewitz revolucionaram o campo de batalha do século XX, e suas teorias mesmo nos dias atuais, são instrumentos de base para as maiores e mais respeitadas escolas de guerra do mundo.

A realidade das grande operações militares são muito mais complexas do que a simplista visão clássica.

Há 2.500 anos, Sun Tzu, estrategista chinês disse algo sobre a guerra que continua válido até os dias de hoje: “Se você conhece a si mesmo e também o inimigo não precisará temer o resultado de cem batalhas” (Sun Tzu, 500 a.C.).

Isso quer dizer que um líder militar que conheça exatamente a composição e a disposição das suas próprias forças, e que tenha em mãos informações detalhadas sobre a composição do dispositivo inimigo, estará sempre alguns passos à frente no campo de batalha, crescendo de importância o desenvolvimento cibernético. Isso provou ser verdadeiro na Segunda Guerra Mundial, quando os britânicos conseguiram quebrar a encriptação da máquina Enigma usada pelos alemães para o envio de ordens cifradas, e também quando os americanos quebraram código que os japoneses usavam, e raças a essa gigantesca vantagem, os aliados conseguiram por diversas vezes se antecipar aos alemães na Europa e aos japoneses no Pacífico.

Durante aquela guerra, que decorreu entre 1914/1918, o rádio ainda estava na sua infância, com aparelhos muito grandes pesados e com pouco alcance, mas serviu para mostrar que o caminho para as comunicações no campo de batalha passava por essa via. Quando a segunda guerra mundial começou em 1939, o rádio já tinha evoluído muito e abriu caminho para o aparecimento de equipamentos móveis com potências e alcances elevados.

Porém se nos anos 30 os militares precisavam estar atentos apenas a certas frequências de rádio, hoje no século XXI, em plena era da informação, os militares precisam estar atentos a diversas outros recursos, tais como: celulares, rádio comunicadores, e-mail e mensagens instantâneas, tornando-se um desafio quase sobre-humano, tendo em vista o gigantesco volume de dados que são trocados a cada segundo por esses meios, tendo em vista também o poder cada vez maior de processamento dos computadores, sendo relativamente fácil interceptar essas comunicações. Entretanto é difícil decifrar e classificar essas informações e extrair uma informação relevante que possa lançar alguma luz sobre as atividades do inimigo das infindáveis toneladas de mensagens trocadas a cada segundo. Por esse motivo muitos países investem pesado nesse tipo de tecnologia que pode transformar a realidade do campo de batalha como a história já demonstrou.

Um exemplo disso é Israel, que segundo Zhou (2020) é um país com poucos recursos naturais, em uma região de conflitos efervescentes e cercado por inimigos políticos. Em um ambiente hostil e desfavorável, criatividade e eficiência são primordiais e a inovação vem pela necessidade de sobreviver e prosperar. Esse cenário estimulou o governo de Israel a unir forças com Exército, Universidades e ecossistema empreendedor para transformar o país em uma das maiores referências em inovação, empreendedorismo e tecnologia do mundo. Mas, foi sua preocupação com a segurança que garantiu ao país mais um reconhecimento: potência em Segurança cibernética. As areias do deserto de Negev deram lugar à uma infraestrutura urbana que abriga um dos maiores centros de cibersegurança no mundo.

Reconhecida globalmente como o 2º principal polo de inovação deste segmento, Israel conforme explica Zhou (2020) foi notada por gigantes do Vale do Silício como Microsoft, Google e IBM, que além de levar filiais de seus negócios pra lá, também adquiriram empresas de cibersegurança do país.

O apoio à tecnologia é tão valorizado que o governo israelense investe cerca de 5% de seu PIB em Pesquisa e Desenvolvimento. Com mais de 5 mil startups, o país leva o codinome de Startup Nation, além de abrigar as top 10 maiores empresas de Cibersegurança do mundo. Somente em 2018, foram investidos US$1,19 bi em startups de cibersegurança no país, quase 20% dos investimentos globais no setor.

Segundo Zhou (2020) explica que a região de Tel Aviv tornou Israel referência

em inovação e empreendedorismo, abrigando a maior parte das startups e empresas de tecnologia do país e reunindo grandes eventos sobre Cyber Security, como a Cyber Week.

Há poucos quilômetros dali, está Beersheva: um dos principais conglomerados mundiais de pesquisa em cibersegurança. A pequena região, que antes era cercada apenas por deserto, se tornou sede da Universidade de Ben-Gurion que junto do exército israelense foi a primeira instituição a iniciar as pesquisas nesse setor. Empresas como Paypall, IBM e Deutsche Telekom têm escritórios na região, apoiando e incentivando o desenvolvimento do local.

Bersheeva é também sede da *CyberSpark*, que conforme relatam Clarke e Knake (2015) trata-se de uma *joint venture* do Departamento Nacional de segurança Cibernética de Israel no gabinete do Primeiro Ministro, do Município, da Universidade Ben Gurion e empresas líderes de cibersegurança, com mais de 10 edifícios dedicados exclusivamente ao desenvolvimento dessa tecnologia.

Para Clarke e Knake (2015) é uma das maiores provas de intersetorialidade e colaboração de uma nação em prol da criação de um ecossistema sustentável e determinado a evoluir. Israel está muito à frente de grandes países desenvolvidos quando o assunto é Cibersegurança, se consolidando como referência mundial no assunto.

Zhou (2020) complementa que essa evolução resultante de pesquisas, educação e tecnologia foi desenvolvida diante de tantas ameaças e forças externas que obrigaram o país a investir pesadamente em segurança. Os conflitos Israel-Palestina e Israel-Síria são exemplos claros de porque o país tem que revisar suas medidas de segurança constantemente. Para explicar o movimento de investir pesadamente em segurança cibernética. O investimento pesado em segurança realizado por Israel contando com equipes específicas para lidar com tal problema se deve ao terrorismo internacional em evolução, visto que Israel enfrenta um ambiente desafiador, especialmente do Oriente Médio, enfrentando todos os meses, inúmeros ataques cibernéticos aos sistemas de dados e sites do governo

1.1 Problema de Pesquisa

Esta pesquisa como problemas de pesquisa para o trabalho a busca por trazer luz a algumas teorias de Clausewitz sob a ótica do espaço cibernético

moderno, além dos desafios presentes para o desenvolvimento e atendimento das necessidades da Tecnologia da Informação e Comunicação (TIC) em comunhão com a Guerra Cibernética. O trabalho propõe uma comparação das estratégias para segurança e defesa cibernéticas no Brasil e em Israel e para isso busca responder a seguinte questão problema: Como as estratégias para segurança e defesa cibernéticas realizadas por Israel podem ser comparadas com as realizadas pelo Brasil?

1.2 Objetivo Geral

Realizar uma comparação das estratégias para segurança e defesa cibernéticas no Brasil e em Israel mostrando a aproximação desses países além do campo diplomático

1.3 Objetivos Específicos

- Explicar questões como poder, tecnologia e informação abordando conceitos clássicos de Guerra e Guerra Cibernética;
- Descrever questões como Cibernética, espaço cibernético, segurança, defesa e poder Cibernético e analisar as políticas de controle relacionadas à segurança da informação ou segurança cibernética;
- Descrever a Guerra Cibernética, mapeando as principais ameaças e os prejuízos ocasionados ao país;
- Mostrar a aproximação entre Brasil e Israel além do campo diplomático;
- Apresentar o avançado sistema de defesa cibernética de Israel e os desafios do Brasil no Século XXI.

1.4 Metodologia

A metodologia do trabalho se resume a uma pesquisa bibliográfica baseada em pesquisas documentais dos termos relacionados à Guerra Cibernética, integração de sistemas, segurança e agilidade no fluxo de transmissão de ordens de

comando no que tange àquilo que há de mais atual, assim como livros, artigos e teses que abordem o problema em questão.

1.5 Justificativa

A escolha do tema se justifica diante de um cenário globalizado que traz diversas vulnerabilidades, onde cada vez mais, as pessoas sentem a necessidade de conectar-se uma com as outras, que o mercado precisa de velocidade para suprir suas demandas e as empresas desejam flexibilidade e interligação, e só a gigantesca rede de computadores, que é a internet, é capaz de suprir essas urgências. No entanto, a rede é dotada de incertezas, e os países que desejam preservar seus interesses e proteger suas riquezas bem como áreas críticas, devem investir em segurança. No mundo todo, os ataques cibernéticos se tornam diariamente mais frequentes, em todos os tipos de cenário, tanto na paz quanto na guerra. Nesse sentido, diferentes países escolheram sua forma de desenvolver sua defesa cibernética, baseado em suas capacidades e necessidades. Cabe ao Brasil observar como países experiêntes como Israel tratam tal questão e articular seus recursos de forma consciente para desenvolver de forma eficiente um meio de se defender de tais ataques cibernéticos.

.

1.6 Estrutura do Trabalho

Este trabalho aborda o tema Brasil e Israel, aproximação diplomática e apoio na segurança cibernética, sendo o domínio tecnológico imprescindível para que uma nação se mantenha soberana no atual cenário internacional. A abordagem geral levantada, é que o domínio da capacitação e modernização da Tecnologia da Informação e Comunicação (TIC) e guerra cibernética nos mais diversos meios de utilização, contribui para sua adequada capacidade de Defesa.

Para isso, o desenvolvimento deste trabalho ocorre com o primeiro capítulo focando nas teorias do poder e Clausewitz e os diversos campos de atuação da tecnologia cibernética atualmente, posteriormente no segundo capitulo é abordado o mapeamento das ameaças da guerra cibernética no cenário mundial atual e no terceiro e último capitulo é estudada a relação de algumas das maiores potências no campo da guerra cibernética com o Brasil.

2 PODER, TECNOLOGIA E INFORMAÇÃO

2.1 Clausewitz e a teoria da submissão pela força

Utilizando Clausewitz (1989) [1832] como o de partida para a comparação entre o conceito clássico de Guerra e o conceito de Guerra Cibernética, amplamente utilizado pela literatura que trata sobre o tema. Sabemos que guerra é um tema de estudo antigo e a definição clássica de Clausewitz já é muito conhecida no meio acadêmico. Porém o conceito de Cibernética não é tão conhecido e pode ter algumas apropriações distintas quando combinado com o conceito de guerra. como

> The first, the supreme, the most far-reaching act of judgment that the statesman and commander have to make is to establish by that test the kind of war on which they are embarking, neither mistaking it for, nor trying to turn it into, something that is alien to its nature (CLAUSEWITZ, 1989 [1832] p. 88-89).[1]

Com a Era da Informação, e os constantes avanços da tecnologia da informação todo o planeta passou a se organizar em redes onde trafegam um enorme fluxo de informações, acarretando que várias atividades com potencial beligerante pudessem ter sua eficácia potencializada. Nesse contexto, a transformação de informação em inteligência torna-se um processo muito mais complicado que no passado. Clausewitz (1989) [1832] reforça o conceito de guerra citando: a guerra é, portanto, um ato de força para obrigar o nosso inimigo a fazer a nossa vontade [...] A guerra é meramente a continuação da política por outros meios (CLAUSEWITZ, 1989 [1832], p. 75).

Analisando a definição de Clausewitz (1989) [1832], que afirma que as características principais da guerra são o uso da força, o fato da guerra ser um instrumento para se chegar a um determinado fim e o fato da guerra ser um ato político. No uso da força ou no ”ato de força” em qualquer guerra, existe uma causalidade direta entre a ação e, pelo mesmo, a possibilidade de que a mesma cause lesões graves ou até a morte de pessoas. Além disso, é a declaração política de guerra que possibilita às partes compreenderem o propósito político pelo qual

[1] O primeiro ato de avaliação, o maior deles, o de maior alcance que o político e o comandante têm que fazer é estabelecer, através daquele exame, em que tipo de guerra estão se envolvendo, não se enganando com relação a ela, nem tentando transformá-la em algo que seja alheio à sua natureza. (CLAUSEWITZ, 1989 [1832] p. 88-89, tradução nossa).

determinada guerra estaria sendo travada.

Segundo Brustolin (2020) o ato de força ocorre ao obrigar o inimigo a fazer a vontade dos indívíduos que agem sob o comando de um agente físico, nesse contexto, o autor acima relata:

> Observation of the alpha reveals their command over their group. In the case of the existence of groups commanded not by an alpha, but by all the individuals, command implies the ability of the commander to convince or to force his opponents to submit to his will inside the group and to follow a single policy, forming a single command that represents “all interests of the community”. Command is, therefore: The consensual or forced submission of the will of others (BRUSTOLIN, 2020, p. 659)[2].

A declaração de guerra conforme relata o autor acima, possibilita às partes compreenderem o propósito político pelo qual determinada guerra estaria sendo travada. Contudo as atividades cibernéticas, ao invés de atos de força, são consideradas versões contemporâneas da subversão, espionagem e sabotagem que apesar de métodos de guerra, também acontecem em tempos de paz. Tais atividades apesar de serem perseguidas e punidas, tanto em tempos de guerra como nos de paz, por si só não são equivalentes aos atos de força.

Os Estados deveriam compreender como as atividades de subversão, espionagem e sabotagem se comportam quando utilizadas no espaço cibernético e o seu potencial de forçar o inimigo a se subeverter a vontade de outro, conceitos estes alinhados às teorias de Clausewitz sobre a imposição do poder e da força.

- A subversão é uma atividade de revolta contra a ordem social, política e econômica estabelecida vigente. Pode manifestar-se tanto sob a forma de uma oposição aberta e declarada, sob a forma de uma oposição sutil e prolongada. Esta é a atividade que necessita de menos habilidade técnica e que pode ser amplificada pela possibilidade de mobilização de uma grande quantidade de pessoas em curto espaço de tempo.
- A espionagem consiste na prática de obter informações de caráter sigiloso relativos a governos ou organizações, sem a autorização desses, para obtenção de vantagem militar, política, econômica, cintífica, tecnologia e/ou

[2] A observação do alfa revela seu domínio sobre o grupo. No caso da existência de grupos comandados não por um alfa, mas por todos os indivíduos, o comando implica a capacidade do comandante de convencer ou forçar seus oponentes a se submeterem à sua vontade dentro do grupo e seguir uma única política, formando um único comando que representa "todos os interesses da comunidade". O comando é, portanto: A submissão consensual ou forçada da vontade de outros (BRUSTOLIN, 2020, p. 659, tradução nossa).

social. Necessita de um nível alto de habilidade técnica, sendo a espionagem cibernética muito mais eficiente que sua contraparte tradicional.

- Sabotagem é uma ação deliberada que visa enfraquecer um governo, esforço ou organização através de obstrução, ruptura ou destruição. Aquele que se envolve em sabotagem é um sabotador. Sabotadores tipicamente tentam esconder suas identidades por causa das consequências de suas ações. É considerada aquela atividade que necessita da mais alta capacidade de inteligência, pois enfrenta dificuldades técnicas mais complexas que as da espionagem (CLAUSEWITZ, 1989 [1832]).

As ajudam a compreender que na atualidade existem atividade que são exercidas exclusivamente no espaço físico, enquanto outras com poder de devastação igualmente grande, podem ser exercidas no espaço cibernético e são igualmente capazes de subverter a outros, sem a necessidade de se utilizar a força física, apenas utilizando a capacidade técnica e inteligência cibernéticas, mesmo nos conflitos tradicionais os armamentos avançados, muitas vezes, depende da confiabilidade do levantamento de informações.

Castells (1996) enumera quatro culturas que formaram a Internet: a cultura tecnomeritocrática, a cultura hacker, a cultura comunitária virtual e a cultura empreendedora, esta sociedade só foi possível devido a revolução das tecnologias da informação que criou um espaço virtual de disputa de poder, denominado espaço cibernético. Porém, não se pode deixar que o impacto das novas tecnologias nos leve a crer, que tal revolução modificou a essência tanto da política quanto da guerra clássica de Clausewitz. A Era da Informação viabilizou o acesso a todo tipo de dados com muita velocidade, todavia é vital que essas informações se transformem em inteligência, seja nos espaços físicos ou cibernéticos. Diante disso, se faz importante uma abordagem a respeito da tecnologia e da informação nos dias de hoje.

2.2 Tecnologia e Informação na atualidade

A tecnologia vem ocupando espaços cada vez mais significativos em todos os campos da sociedade, estando as forças armadas na vanguarda tecnológica, um grande questionamento atualmente difundido é como as características do combate moderno vem se tornando cada vez mais dependentes do aspecto tecnológico. Nota-se ainda, que as ações de combate utilizadas são caracterizadas pelo controle

e emprego de armamentos que possuem alta capacidade de tecnologia agregada.

Hoje, em muitos países a tecnologia de inteligência artificial vem sendo amplamente aplicada para a resolução de problemas em vários campos da sociedade, tais como: aeconomia, medicina, infraestrutura e militar. Percebe-se que os acontecimentos ocorridos nos combates do século XXI pelo mundo mostram a necessidade do desenvolvimento de novos armamentos, novas capacidades marítimas e aéreas e de novos estudos de casos militares voltados para um “novo combate” que ora se apresenta em novos espaços no século XIX.

Segundo Nye (2010) com a migração das batalhas para ambientes urbanos onde a evolução tecnológica e meios de difusão das informações são amplamente influenciada pelos atores participantes dos conflitos (população local, mídia, opinião pública, redes sociais, etc), a revolução tecnológica se espalhou pela sociedade e hoje em dia a velocidade de propagação dos dados pode representar uma amaeça real para transformar a opinião pública hostil em questão de minutos.

A informação tornou-se uma ferramenta primordial para o êxito nas operações militares atuais, possibilitando aos tomadores de decisão influenciar no combate para obter, produzir, difundir e até manipular a busca da legitimidade das ações, além de poder ser o diferencial entre se estar à frente das ações do inimigo.

Nye (2010) relata ainda que a demanda pela velocidade de propagação de dados tornou-se popular e amplamente difundida nas mais diversas classes sociais. E essa demanda somada ao ambiente competitivo do sistema internacional que difunde e determina o constante progresso tecnológico, bem como a transformação dos serviços e produtos estatais e privados. Sob o argumento de que o Sistema Internacional é anárquico, existe a necessidade de desenvolver-se ferramentas capazes de coibir ameaças, dependendo cada vez mais de pesquisa e desenvolvimento de tecnologias da área. As vantagens atinentes ao surgimento e aperfeiçoamento da ciência computacional e robótica são indubitáveis, mas é preciso ter uma visão holística a fim de se compreender o verdadeiro impacto dessa revolução digital no mundo.

2.3 Cibernética

Segundo Marinescu (2017) cibernética é uma ciência, nascida por volta de 1942 e dirigido inicialmente por Norbert Wiener, um renomado físico, com o livro

“cibernética: ou controle e comunicação no animal e na máquina” que desenvolveu uma linguagem e técnicas que nos permitirão resolver o problema do controle e comunicação em geral. Dois anos depois Wiener escreve outro livro “Uso humano de seres humanos: cibernética e sociedade”, buscando difundir melhor os conceitos para o público não especializado. A palavra cibernética vem da palavra grega kybernetes, que significa leme, piloto, um dispositivo usado para dirigir um barco ou para apoiar a governança humana.

Wiener (2017) define cibernética como o estudo do controle e da comunicação no animal e na máquina e tal ciência se desenvolveria em torno da informação a partir da segunda metade do século XX.

A cibernética se preocupa com os conceitos essenciais para a compreensão de sistemas complexos, como aprendizagem, cognição, adaptação, emergência, comunicação e eficiência e tem aplicações em campos tão diversos como psicologia e teoria do controle, filosofia e engenharia mecânica, arquitetura e biologia evolutiva, ou ciências sociais e engenharia elétrica.

Segundo o Ministério da Defesa (2014) o termo que se refere à comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação.

> No campo da Defesa Nacional, inclui os recursos de tecnologia da informação e comunicações de cunho estratégico, tais como aqueles que compõem o Sistema Militar de Comando e Controle (SISMC2), os sistemas de armas e vigilância, e os sistemas administrativos que possam afetar as atividades operacionais (MINISTÉRIO DA DEFESA, 2014, p. 18).

De acordo com Nye (2010) a importância sobre as ameaças cibernéticas começaram a surgir no início dos anos 90, décadas após o seu surgimento como ciência. Desde então, com o crescimento da rede digital em níveis globais, o número de usuários, saltou de 1 milhão de usuários, para 1 bilhão em 15 anos. Com as atividades bélicas migrando e sistemas cada vez autonomos os riscos inerentes ao domínio virtual foram crescendo à medida que a rede se difundia e o controle dos entes estatais sobre ela diminuía. A dependência de sistemas cibernéticos complexos para apoiar atividades econômicas e militares criou novas vulnerabilidades em grandes estados que puderam ser exploradas por atores não estatais. O autor acima descreve bem a expansão deste recurso e as preocupações do Estados Unidos no início dos anos 90:

> O governo dos EUA só começou a desenvolver sérios planos nacionais de segurança cibernética na última década. Em 1992, havia apenas um milhão de usuários na Internet; dentro de quinze anos que haviam crescido para um bilhão. 14 Nos primeiros dias, os libertários proclamavam que "a informação quer ser gratuita" e retratavam a internet como o fim dos controles governamentais e a "morte à distância". Na prática, governos e jurisdições geográficas desempenham um papel importante, mas o domínio também é marcado pela difusão de poder (NYE, 2010, p. 3).

Desde o final dos anos 80, os ciberataques evoluíram várias vezes para usar inovações em tecnologia da informação como vetores para cometer crimes cibernéticos . Nos últimos anos, Nye (2010) comenta que a escala e a robustez dos ataques cibernéticos aumentaram rapidamente. No período imediato pós-Guerra Fria a infraestrutura das redes e a indústria de alta tecnologia pode se desenvolver mais vocacionada para o uso civil e esse descompasso entre o começo da ampla utilização e o início da percepção de risco por todos gerou solo fértil para o crescimento de agentes maliciosos. A transmissão de dados instantâneos, a rapidez nunca antes vista nas comunicações, as transações bancárias podendo ser realizadas a partir de qualquer lugar do globo terrestre, a administração de dados por meio digital por estados, empresas e pessoas floresceram nessa fase. Entretanto esses recursos não surgiram com base em princípios de segurança, proteção, transparência e privacidade.

Nye (2010) explida que as atividades criminosas como como roubo de dados, acesso descabido a dados confidenciais, falsificações eletrônicas, sabotagem e espionagem começaram a afetar de maneira considerável indivíduos, empresas e os seus respectivos governos. Conforme observado pelo Fórum Econômico Mundial em seu relatório de 2020, que aponta como principais riscos e tendencias os “Ataques cibernéticos em grande escala” e a “Crescente dependência cibernética”.

As ameaças cibernéticas são evidenciadas em razão da atual interdependência de sistemas e sua integração em redes de computadores, com muitos sistemas estão na world wide web e em outras redes a ela conectada que elas incidem de maneira mais significativa. Os usuários não têm a percepção que o ambiente pode ser monitorado e as punições são raras e de difícil execução dado ao volume e a capilaridade da rede mundial. Concomitantemente a essa sensação de impunidade, há a grande parcela dos meios de controle de estruturas fundamentais da sociedade serem conectados através de ciber sistemas. Nye (2010) relata que a percepção de que a infraestrutura é intrinsicamente dependente deste dominio

virtual torna-se importante para compreesão deste novo mundo. Cabe destacar ainda na visão de Nye (2010) que a cibernética é uma das áreas listadas prioritariamente pela Estratégia Nacional de Defesa do Brasil (END), ao lado da nuclear e da espacial.

2.4 Espaço Cibernético

O termo ciberespaço foi criado em 1984 por William Gibson, que usou o termo em seu livro de ficção científica, Neuromancer. O ciberespaço é o espaço virtual para a comunicação que surge da interconexão das redes de dispositivos digitais interligados no planeta, incluindo seus documentos, programas e dados, portanto não se refere apenas à infraestrutura material da comunicação digital, mas também ao universo de informações que ela abriga. Os primórdios datam do final da década de 60 relacionados a uma pequena rede de computadores e a elaboração do protocolo TCP/IP, que são códigos para a transferência de dados. Essa rede foi desenvolvida pelo Departamento de Defesa Americano e ficou sendo conhecida como “ARPANET”. Esse novo sistema foi concebido para montar uma internet basilar que tinha a capacidade de transmitir agrupamentos de informações digitais. Em 1972 os códigos para troca de dados (TCP/IP) foram criados para constituir uma Internet, o projeto até então exclusivamente começou a crescer e expandir a nível internacional até chegar próximo do que conhecemos atualmente (NYE, 2010).

O conceito de ciberespaço, ao mesmo tempo, inclui os sujeitos e instituições que participam da interconectividade e o espaço que interliga pessoas, documentos e máquinas. O ciberespaço representa a capacidade dos indivíduos de se relacionar criando redes que estão cada vez mais conectadas a um número maior de pontos, tornando-se as fontes de informação mais acessíveis, mas que se compreende não só como um ambiente de divulgação de informação, mas também de entretenimento e cultura, no qual os indivíduos podem expressar suas singularidades e, ao mesmo tempo, se relacionar criando novas e diversas pluralidades. Por fim, Nye (2010) explica que o ciberespaço é considerado um espaço de acesso livre e descentralizado, onde todos os tipos de texto, voz, imagens, vídeos, etc. são traduzidos a uma única linguagem: a informática.

Ciberespaço, na visão de Bussel (2017) é um mundo supostamente virtual criado por links entre computadores, dispositivos, servidores, roteadores e outros

componentes. Ao contrário da própria Internet, entretanto, o ciberespaço é o lugar produzido por esses links.

Na cultura popular da década de 1990, ciberespaço foi um termo usado para descrever o local em que as pessoas interagiam umas com as outras enquanto usavam a Internet. Bussel (2017) explica que o ciberespaço também se tornou um local importante para discussão social e política, com o surgimento popular no final do século 20 e no início do século 21 de fóruns de discussão baseados na web e blogs.

Desde o surgimento da Internet, no entanto, os governos nacionais e seus analistas têm mostrado a relevância tanto das regulamentações nacionais quanto dos acordos internacionais sobre o caráter do ciberespaço. Bussel (2017) explica que esses atores sem corpo no ciberespaço devem acessar esse outro reino por meio de sua forma corporal e, portanto, continuam a ser limitados pelas leis que regem sua localização física. O governo chinês mantém controles rígidos sobre quem pode acessar a Internet e qual conteúdo está disponível para eles. Os Estados Unidos desenvolveram uma estratégia para a segurança do ciberespaço a fim de prevenir e responder a ataques à infraestrutura da Internet.

O controle do ciberespaço é, portanto, importante não apenas por causa das ações dos participantes individuais, mas porque a infraestrutura do ciberespaço agora é fundamental para o funcionamento dos sistemas de segurança nacionais e internacionais, redes comerciais, serviços de emergência, comunicações básicas e outras atividades públicas e privadas. Bussel (2017) relata que como os governos nacionais veem ameaças potenciais à segurança de seus cidadãos e à estabilidade de seus regimes surgindo no ciberespaço, eles agem para controlar o acesso e o conteúdo.

O Espaço Cibernético na visão das forças armadas brasileiras, mais especificamente do ponto de vista da Defesa Nacional, é o termo é definido da seguinte forma: espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas (MINISTÉRIO DA DEFESA).

Seguindo a Estratégia Nacional de Defesa atraves do Livro Branco de Defesa Nacional tem como organização responsável pelo setor no Brasil o Comando de Defesa Cibernética (ComDCiber), organização militar conjunta, na estrutura organizacional do Comando do Exército. O espaço cibernético tornou-se uma

preocupação para o país, por colocar em risco a integridade de infraestruturas sensíveis, essenciais à operação e ao controle de diversos sistemas e órgãos diretamente relacionados à segurança nacional (MINISTÉRIO DA DEFESA, 2014).

> A proteção do espaço cibernético abrange um grande número de áreas, como capacitação, inteligência, pesquisa científica, doutrina, preparo e emprego operacional e gestão de pessoal. Compreende, também, a proteção de seus próprios ativos e a capacidade de atuação em rede. A implantação do Setor Cibernético tem como propósito conferir confidencialidade, disponibilidade, integridade e autenticidade aos dados que trafegam em suas redes, os quais são processados e armazenados. Esse projeto representa um esforço de longo prazo, que influenciará positivamente as áreas operacional e de ciência e tecnologia. Sob a coordenação do Exército, significativos avanços têm se concretizado na capacitação de pessoal especializado e no desenvolvimento de soluções de elevado nível tecnológico. (MINISTÉRIO DA DEFESA, 2008, p. 51).

Muitas incertezas ainda pairam sobre as mudunças que ocorrerão no sistema internacional sobre o tema. Todavia é consenso de que o conjunto de propriedades do espaço cibernético geram no âmbito das relações internacionais uma difusão do poder, e o mais importante é de que forma os Estado vão se adaptar ou resistir a esse novo universo, visto que a popularização está cada vez mais proeminete e, consequentemente, influenciam notavelmente neste universo sem fronteiras e com limitado ordenamento juridico para coibir ações de atores não estatais.

2.5 Segurança, defesa e poder cibernético

A direção das ações e os conceitos de segurança cibernética e defesa cibernética foram segregadas em dois órgãos distintos no Brasil e estão sendo elaborados por diferentes segmentos do Estado e a zona de ação da Segurança Cibernética compreende óticas e atuações de prevenção e repressão em nível político, enquanto as ações de defesa cibernética visam a proteção em nível de Estado mais amplo e estratégico.

Tabela 1 – Níveis de Decisão do Estado Brasileiro

Nível de Decisão	Designação	Estrutura
Político	Segurança Cibernética	Gabinete de Segurança Institucional (GSIPR)
Estratégico	Defesa Cibernética	Ministério da Defesa

Fonte: Adapatado do CDCiber/EB/MD

Na visão acadêmica atual, a Defesa Cibernética e a Segurança Cibernética ganharam notoriedade nos últimos anos, em razão das vulnerabilidades prementes e intangíveis sistemas cada vez mais integradas e em rede. Os ataques cibernéticos são uma realidade mesmos em sistemas mais robustos e poderosos, lavando os Estados a estabelecerem políticas de estratégia nacional para repelir as agressões, muitas vezes anônimas.

Uma característica interessante sobre a Defesa Cibernética a Segurança Cibernética é relatada por Brustolin (2020):

> The cyber defence is a level above cybersecurity, ensuring the execution of processes and activities, free of threats. Cyber defence also helps to improve the capabilities and uses of the security strategy (Galinec, Možnik, and Guberina 2017). Cybersecurity and cyber defence work together (or should work) (BRUSTOLIN 2020 apud GALINEC 2017 p 93).[3]

As definições muitas vezes se confundem, porém devem ser diferenciadas, uma outra definição necessária por questão de diferenciação é a de segurança cibernética.

Segundo Mandarino (2009), a expressão segurança cibernética é compreendida como requisito para a proteção e salvaguarda das informações de uma nação: “a segurança Cibernética é entendida como a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas infraestruturas críticas” (MANDARINO, 2009 p 26).

A segurança cibernética busca garantir a integridade, disponibilidade, confidencialidade e autenticidade de sistemas de informação. O Gabinete de Segurança Institucional - GSI conceitua a segurança cibernética como a arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas infraestruturas críticas (GSI 2009a p 19).

Dois conceitos importantes para a segurança cibernética envolvem os ativos

[3] A defesa cibernética, por outro lado, é “um mecanismo de defesa de redes de computadores que inclui resposta a ações e proteção de infraestrutura crítica e garantia de informações para organizações, entidades governamentais e outras redes possíveis (Galinec, Možnik, and Guberina 2017) [...] Portanto, a defesa cibernética está um nível acima da segurança cibernética, garantindo a execução de processos e atividades, livre de ameaças. A defesa cibernética também ajuda a melhorar os recursos e usos da estratégia de segurança (Galinec, Možnik, and Guberina 2017) [...] A segurança cibernética e a defesa cibernética trabalham juntas (ou deveriam trabalhar) (BRUSTOLIN 2020 apud GALINEC 2017 p 93, tradução nossa).

de informação, definidos pelo GSI (2009) como meios de armazenamento, transmissão e processamento, bem como os locais onde se encontram esses meios e as pessoas que a eles tem acesso e as infraestruturas críticas que englobam as instalações, serviços, bens e sistemas que foram interrompidos ou destruídos, provocando sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade.

É nítida a percepção e preocupação com a segurança cibernética e com a defesa cibernética dos sistemas virtuais e de infraestrutura pelos Estados. A questão principal gira em torno de como se defender de agressores anônimos, muitas vezes não estatais, e com recursos inalcançaveis no espaço cibernético. Nas palavras do General Santos em sua entrevista, há notória preocupação no recrutamento de talentos civis especializados, fato que já ocorre em diversos outros países, ainda que haja a clara dificuldade de se manter o alinhamento entre os talentos civis e os interesses nacionais.

Segundo o que consta na Doutrina Militar de Defesa Cibernética o conceito de Defesa Cibernética pode serdescrito como um conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, com a finalidade de proteger os sistemas de informação de interesse da Defesa Nacional, a fim de obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente (MINISTÉRIO DA DEFESA, 2014).

Após a compreensão sobre a cibernética e o seu espaço, bem como as vertentes e suas aplicações, é possível abordar sobre o poder derivado destes campos do conhecimento e o que seus recursos oferecem. A Doutrina Militar de Defesa Cibernética define o poder cibernético como a “capacidade de utilizar o Espaço Cibernético para criar vantagens e eventos de influência neste e nos outros domínios operacionais e em instrumentos de poder.” (MINISTÉRIO DA DEFESA, 2014, p. 19).

Diante do que foi colocado, compreende-se a necessidade de analisar os tipos de recursos decorrentes da capacidades cibernéticas capazes de mudar a natureza do poder e aumentar sua difusão. Esses recursos são interconectados, porém o seu arranjo se dá de maneira indistinta entre os variados estados-nações do ordenamento mundial. Entende-se que os estados permanecerão com os atores dominantes no cenário mundial, mas acharão o cenário muito mais movimentado e difícil de controlar, visto que as características do espaço cibernético produzem

alguns dos diferenciais de poder entre os atores e, portanto, fornecem um bom exemplo da difusão de poder que tipifica a política global neste século.

No campo militar, o poder cibernético é valoroso, e tem um lado nivelador, sendo tratado como política de estratégia nacional em diversas nações, inclusive em alguns países beligerantes há políticas voltadas para a persecução ou mesmo destruição de seus oponentes, como por exemplo as hostilidades entre Irã e Israel no Oriente Médio.

3 ANÁLISE DAS POLÍTICAS DE CONTROLE RELACIONADAS À SEGURANÇA DA INFORMAÇÃO OU SEGURANÇA CIBERNÉTICA

3.1 Guerra Cibernética, o novo campo de batalha no século XXI

A guerra cibernética exerce papel cada vez mais importante no mundo militar moderno, não é de hoje que a informação e a capacidade de conhecer as intenções do inimigo são essenciais para a vitória no campo de batalha. Segundo Melo et al (2012) durante a Segunda Guerra Mundial os aliados eram capazes de ler as ordens enviadas pelos alemães através da sua máquina enigma, um equipamento que encriptava as mensagens em milhões de combinações possíveis. Graças a esse esforço, muitos dos movimentos dos alemães no campo de batalha eram previamente conhecidos o que facilitou em muito a vitória dos aliados naquela guerra.

O contrário também provou ser extremamente vantajoso, ou seja, fazer o inimigo pensar uma coisa quando o que se planejava era outra coisa completamente diferente. Melo et al (2012) explicam que se antigamente era necessário espiões para executarem missões perigosas que incluía a invasão de instalações inimigas, nos tempos atuais, com informações valiosas e sensíveis armazenadas e ligadas à internet, qualquer jovem com os equipamentos e meios adequados, é capaz de ter acesso a essas informações.

Como é óbvio, há diversos métodos e formas de proteger informações militares valiosas, alguns mais eficientes do que outros, mas de forma geral a partir do momento em que um servidor está ligado de alguma forma a internet, o risco de ser invadido e infectado é real.

O termo Guerra cibernética na visão de Melo et al (2012) é relativamente novo, podendo ser definido também como ações tomadas por uma nação com objetivo de invadir os computadores de outra nação, com o propósito de roubar informações, destruir sistemas, ou causar o mau funcionamento de instalações. Trata-se de uma atividade tão importante que todas as principais potências militares do mundo já criaram unidades e agências especiais dedicadas a este campo.

Como já explicado anteriormente, a guerra cibernética envolve basicamente dois tipos de atividade a espionagem e a sabotagem, que pode envolver desde a destruição de projetos planos e documentos, até ações diretas contra infraestruturas

controladas por computadores, tais como: sistema de distribuição de eletricidade, usinas nucleares, sistemas de transporte, estações de tratamento de água, dentre outros.

Através da Guerra cibernética segundo Melo et al (2012) países relativamente pequenos podem se destacar e alcançar vantagens sobre as grandes potências militares, motivo pelo qual países como Israel, Irã e a Coreia do Norte, supostamente, investem muito neste tipo de atividade, porém, países como a China, a Rússia e os Estados Unidos são os que mais se dedicam a guerra cibernética. Não se sabe exatamente quantos recursos cada país dedica especificamente para essa área, mas acredita-se que sejam valores bem elevados e que aumentam de ano para ano com a crescente demanda mundial.

Os autores acima ainda explicam que a espionagem é a face mais visível da guerra cibernética, com países investindo pesado na interceptação de mensagens alheias, com destaque para as escutas telefônicas que os norte-americanos fizeram de líderes estrangeiros, como por exemplo a Chanceler Alemã Angela Merkel, e a própria ex-presidente brasileira Dilma Rousseff, que tiveram seus telefones supostamente grampeados durante alguns anos.

Os chineses também não ficam atrás na guerra cibernética, o país possui milhares de espiões que trabalham como engenheiros em grandes empresas de informática dos Estados Unidos e na Europa. Através desta intrincada rede os chineses conseguem ter acesso a informações que de outra forma seria praticamente impossível. A Índia, que se semelhança da China e forma milhares de novos engenheiros altamente qualificados todos os anos, também tem investido pesado nesse campo (MELO ET AL, 2012).

É prática comum de muitos governos oferecerem oportunidades de emprego a hackers apanhados cometendo crimes cibernéticos, já que são indivíduos com clara aptidão para esse tipo de ativo, diante disso percebe-se que o mundo cibernético será sem dúvida um campo de batalha cada vez mais importante no futuro, e a guerra cibernética ditará o resultado de muitas batalhas travadas entre países.

3.2 Mapeamento de algumas das principais ameaças

Segundo Vieira (2020) a medida que as nações buscam se modernizar e com

a implementação cada vez maior de infraestruturas críticas e integradas na grande rede, ocorre a dependência crescente das tecnologias da informação e comunicações, evidenciando as fragilidades dos Estados em lidar com esta realidade.

Tais vulnerabilidades, entretanto, resultam em investimentos de defesa e políticas de Estado para se contrapor aos riscos, e em indeterminações do domínio cibernético, além de explicar a vontade dos Estados de se prepararem para um possível conflito. Vieira (2020) relata que a contante de insegurança é uma das características mais proeminentes de estudos das relações internacionais no domínio cibernético. Tal domínio garante ao usuário, devidamente habilitado, realizar ataques em anonimato ou fraudando sua identificação.

Buscando controlar este ambiente virtual foram sendo estabelecidas políticas de controle relacionadas à segurança da informação ou segurança cibernética. As políticas de segurança são adotadas por empresas públicas ou privadas com a finalidade de proteger seus ambientes tecnológicos e todas as informações neles contidas. Muita atenção também é dada às políticas públicas relacionadas à segurança da informação, que são tratadas pelos órgãos governamentais, de forma a proteger os cidadãos e o estado (VIEIRA, 2020).

Isso tem por consequência o fato de que cada vez mais estados incrementem suas capacidade cibernética de forma a assossiar uma força cibernética para sua defesa e segurança nacional, assim como para ter a qualificação necessária para conseguir dados sigilosos e informações municiando assim o seu sistema de inteligência, a sua indústria e o seu polo de desenvolvimento científico.

Segundo Vieira (2020) devido a velocidade instantânea de um ataque cyber e do impedimento de se identificar o ofensor, ocorre uma disparidade, pois os atacantes têm grande vantagem perante os defensores nesse domínio, com isso, o cenário entre as nações se nivelam, tornando o desenvolvimento do poder cibernético estratégico para os atores de menor relevância.

Existe ainda o ganho com a reengenharia através da captura de informações de projetos modernos em nações mais desenvolvidas, tais práticas podem ter sido realizadas de forma institucional por parte de nações em desenvolvimento (VIEIRA, 2020).

Sabendo disso, por mais que seja possível elencar diversas razões para se investir no domínio da tecnologia cibernética, sendo por defesa e segurança ou pelo

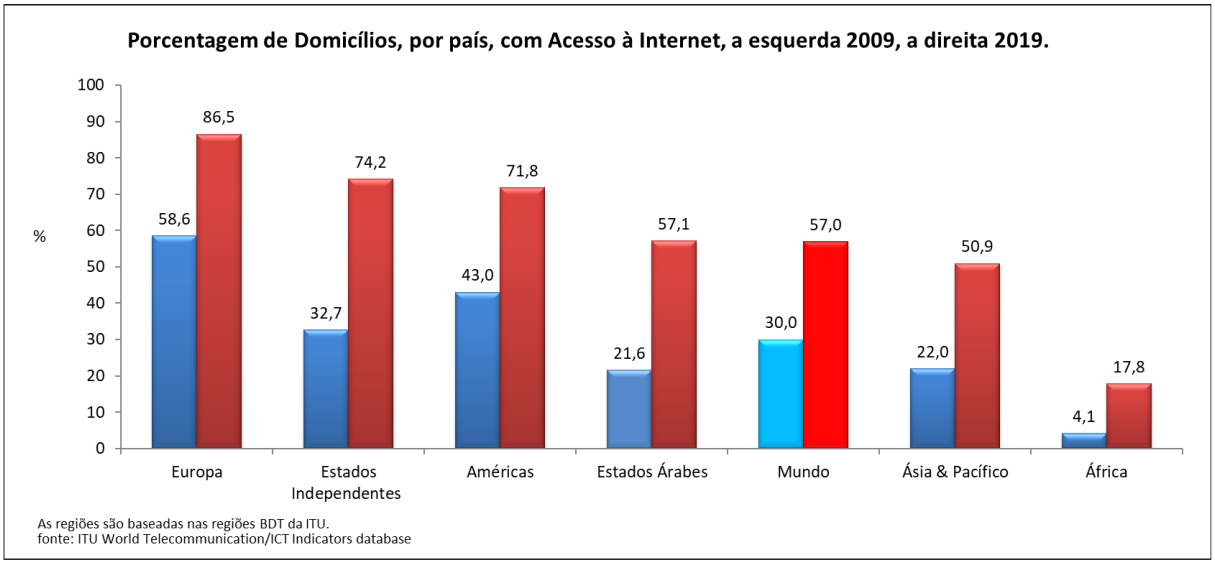
conjunto de possibilidades, a forma de recrutamento e a habilitação de pessoal qualificado é recurso chave do poder cibernético de um país, evidenciando que quando se desenvolvem tais recursos, ampliam-se sobremaneira as suas capacidades. Como ocorre, por exemplo, com a Unidade 8200, de Israel, melhor explicada em próxima sessão desse estudo, e que realiza este trabalho de recrutamento e qualificação, colocando aquela nação entre as mais desenvolvidas neste quesito, demonstrando assim que a forma como acontecem é muito mais relevante do que a quantidade de recursos financeiros aplicados.

3.3 Ataques Cibernéticos

Como explanado anteriormente, os ataques cibernéticos são um risco real, seja em níveis públicos, governamentais ou em sistemas privados. Tais ataques vem aumentando ao longo dos últimos anos e mostram-se cada vez mais ameaçadores. De forma a materializar tais ameaças, a União Internacional de Telecomunicações (UIT), uma agência das Nações Unidas (ONU), criada em 1957 e cobrindo todos os 193, estima que mais de 3 bilhões de pessoas são usuários diretos da Internet no mundo (*INTERNATIONAL TELECOMMUNICATION UNION - ITU, 2018*).

O quadro 1 (abaixo) descreve sucintamente o aumento considerável da porcentagem de usuários na internet em 10 anos.

Quadro 1 - Porcentagem de usuários na Internet em 2009 e 2019.



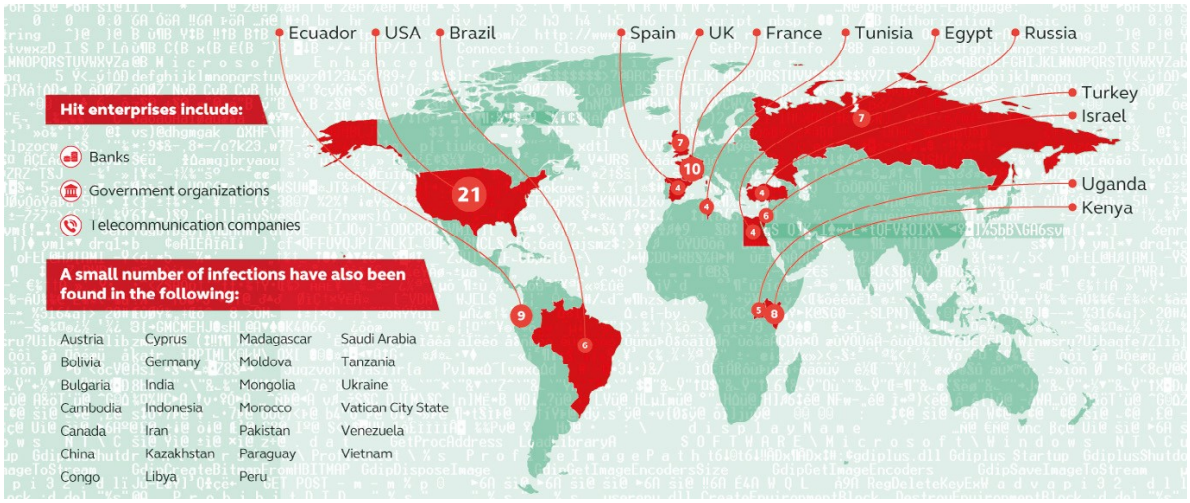
Fonte: União Internacional das Telecomunicações (2019).

Além dos usuários diretos da Internet, existem aqueles que são indiretamente afetados pela Internet. Tais como empresas dos ramos financeiro, energético, navegação com GPS por exemplo, onde seus sistemas vitais muitas vezes estão intrinsicamente interlegados na grande rede, ou seja, a dependência global do espaço cibernético é fundamental para o equilíbrio das atividades, mesmo as atividades atividades mais secretas, como as militares confiam em redes de dados seguros para realizar suas missões e executar suas tarefas (*INTERNATIONAL TELECOMMUNICATION UNION - ITU, 2018*).

A importância dessa temática fica constatada diante de casos como os de 2013 com a divulgação do roubo de informações realizado pela *NSA* – Agência Nacional de Segurança dos Estados Unidos (*National Security Agency*) que comprovou a fragilidade do Brasil e de outros países quanto à guarda das informações e o poder político que tais informações podem ter. Tais preocupações se materializaram em fatos concretos, quando no ano de 2017 mais de 100 países foram atingidos por ataques cibernéticos e no Brasil diversas empresas e órgãos públicos registraram ataques, gerando prejuízos em suas atividades (*INTERNATIONAL TELECOMMUNICATION UNION - ITU, 2018*)

Os ciberataques mundiais em 2017 nas agências e empresas governamentais são exibidos na Ilustração 1 (abaixo).

Ilustração 1 - Alvos mundiais de ataques cibernéticos



Fonte: AO Kaspersky Lab apud Brustolin (2017)

Na ocasião do levantamento destes dados, ocorreu o maior ataque cibernético global já registrado com o lançamento de um vírus de *ransomware* chamado "*WannaCry*" que se espalhou de maneira rápida e avassaladora. Esse tipo

de vírus é conhecido por fazer uma espécie de "sequestro" dos arquivos das máquinas infectadas e exigir o pagamento de um valor fixo para "libertar" o equipamento. Ao todo, estima-se que mais de 230 mil sistemas foram infectados, até que um "antídoto" descobriu o problema e controlou o caso. Também houve a divulgação de que diversas grandes empresas e governos sofreram ataques com vazamento de dados - como o caso da *Equifax*, nos EUA.

Atualmente os *smartphones* são vistos como potenciais ameaças, haja visto o que agentes cibernéticos podem fazer com dispositivos desprotegidos, por exemplo: a rede de bots Mirai, que atacou pela primeira vez em 2016, e o *IoT Reaper*, em 2017. Esse malware surgiu em diversas variantes para atacar dispositivos conectados, como roteadores, gravadores de vídeo em rede e câmeras IP. Eles expandiram seu alcance quebrando senhas e explorando vulnerabilidades conhecidas para criar redes mundiais de robôs. Segundo dados da *Kaspersky Lab*, as ameaças mais comuns para os próximos anos serão:

- Inteligência artificial;
- Evasões diferentes para malware diferente;
- Ameaças sinérgicas vão se multiplicar, exigindo respostas combinadas;
- Criminosos cibernéticos utilizarão campanhas de extorsão e desinformação em mídias sociais para desafiar as marcas das organizações;
- Os ataques de vazamento de dados visarão a nuvem;
- Assistentes digitais controlados por voz, o próximo vetor no ataques contra dispositivos IoT; e
- Os criminosos cibernéticos aumentarão os ataques contra plataformas de identidade e os dispositivos periféricos serão sitiados.

3.4 Prejuízos ocasionados ao país devido a ataques cibernéticos

O Brasil ocupa a 70º colocação no índice de segurança cibernética da União Internacional de Telecomunicações (*ITU*) que coordena esforços nesta área, enquanto Israel ocupa a 39º colocação (porém no estudo, Israel está no grupo de países que não participaram do processo do “Índice Global de Cibersegurança de 2018”, não submetendo respostas ao questionário e nem validaram os dados coletados pela equipe do “Índice Global de Cibersegurança”), maculando assim sua

real posição em relações aos demais países participantes do estudo. (*INTERNATIONAL TELECOMMUNICATION UNION - ITU, 2018*)

Silva (2018) explica que a situação de fragilidade apontada no *ranking* faz com que o Brasil seja um dos países que sofrem maiores prejuízos no mundo com ataques cibernéticos e um dos que mais tem sofrido perdas econômicas advindas de tais ataques, segundo dados mais recentes da ITU, numa medição de 12 meses entre 2017 e 2018.

Em relação aos prejuízos ocasionados por ataques cibernéticos, em setembro de 2019, o Coronel Arthur Sabbat, Diretor do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional (GSI) da Presidência da República, detalhou em uma audiência na Comissão de Relações Exteriores e Defesa Nacional (CRE) que especialistas avaliam que o mercado de segurança cibernética alcançará US$ 151 bilhões em 2020, no mundo todo. Um indicativo claro da prioridade que já vem sendo dada mundialmente a esta questão.

No Brasil a segurança dessa área não se encontra no nível desejado. No ano passado, 70 milhões de brasileiros foram vítimas de ilícitos cibernéticos. É nesse montante que as perdas chegam a US$ 20 bilhões".

O agravante no caso do Brasil é o fato de 100% dos órgãos federais e estaduais utilizarem a Internet. A rede mundial também está presente em 80% das casas do país, chegando a 116 milhões de usuários. O índice de utilização da internet entre as empresas também é quase pleno: 98%, segundo dados do relatório da União Internacional de Telecomunicações (ITU) de 2018. (*INTERNATIONAL TELECOMMUNICATION UNION - ITU, 2018*)

4 BRASIL E ISRAEL, APROXIMAÇÕES ALÉM DO CAMPO DIPLOMÁTICO

Segundo Ferdika (2019) o foco nos laços econômicos na América Latina é uma espécie de partida para Israel. Ao longo das décadas de 1970 e 1980, Israel construiu suas relações com estados regionais, incluindo Guatemala, Nicarágua, Honduras, Argentina e Colômbia, com apoio militar e apoio a vários grupos armados. Seus laços com o Brasil e países vizinhos hoje são mais amplos em comparação. No entanto, o equipamento militar ainda tem um papel a cumprir nas parcerias.

No caso do Brasil, a transferência e o desenvolvimento de tecnologia são prioritários. O Brasil inicia contatos e conversas com Israel em março de 2018 para adquirir e trocar tecnologias científicas e de defesa, um acordo que iria ao mesmo tempo satisfazer o desejo de Israel de exportar bens e serviços militares, sua área de especialização e a necessidade do Brasil de adquirir tecnologia mais avançada. Os dois também chegaram a acordos nascentes sobre tecnologia de defesa, como mísseis, radares e câmeras de vigilância de alta tecnologia. Ferdika (2019) relata que a exploração espacial e satélites são outros pontos de interesse mútuo. O Brasil pode se beneficiar do know-how de Israel no assunto, enquanto Israel tira proveito dos locais de lançamento estratégicos do Brasil perto do equador.

Por tudo, o que uma cooperação renovada tem a oferecer a Brasil e Israel nas esferas econômica e tática, do ponto de vista político, os ganhos são modestos. Para Ferdika (2019) o alinhamento com Israel ajudará o Brasil a se conformar com os Estados Unidos, ao mesmo tempo que promover a Israel mais apoio diplomático - uma vantagem para um país cercado por inimigos e sujeito a investigações, se não censura, no cenário internacional. A crescente parceria entre Israel e Brasil é pragmática, baseada em necessidades complementares. Essas necessidades militares ou ambientais estão conduzindo os dois países juntos, o Brasil em sua busca para desenvolver sua economia e assumir maior influência nos assuntos globais, e Israel em seu esforço para encontrar novos mercados juntos no exterior para impulsionar sua economia.

Sabe-se que a aproximação de Brasil e Israel traz perdas e ganhos, no entanto, não é escopo deste trabalho entrar nestes detalhes. Nesse contexto, Passarinho (2019) confirma que a forte aproximação com Israel tem impacto econômico, mas também um custo político-diplomático.

4.1 O avançado sistema de defesa cibernética de Israel

Existe uma grande diferença entre Brasil e Israel em relação aos métodos para lidar com a questão da guerra cibernética. Tais fatos podem ser evidenciados quando dizem respeito ao recrutamento de talentos e a importância despejada por cada país nesta ramo da tecnologia. Beha (2017) explica que Israel possui a unidade 8200, uma Força especializada na coleta de sinais de inteligência e na vigilância das redes de computadores, e que é vista como a primeira linha de defesa na guerra cibernética.

Para Beha (2017) esta difícil missão entregue a Unidade 8200 é dedicada a coletar e decifrar informações do inimigo, e é diretamente subordinada a AMAN (sigla para Inteligência Militar Israelense) um departamento criado em 1950 com a missão de estar sempre atento a qualquer informação que venha do adversário. Informações dão conta de que a unidade 8.200 é tão avançada como a NSA (Agência de Segurança Nacional dos Estados Unidos), sendo por isso encarada como uma das mais bem equipadas do mundo para tratar assuntos relacionados a guerra cibernética, tanto em termos de equipamentos como em termos de pessoal.

Trata-se da maior unidade das forças de defesa de Israel, com seus membros dedicados a extrair e decifrar o máximo de informações possíveis de sinais de rádio, televisão, jornais e, principalmente, da internet e dos seus inúmeros meios: desde blogs e fóruns, até mensagens instantâneas trocadas por meio de aplicativos. Beha (2017) ainda explica que este tipo de atividade exige com frequência técnicas avançadas de hacking e, principalmente, de técnicas de Data Mining, ciência dedicada a peneirar toneladas de informação, extraindo dessas montanhas de dados um trecho de informação importante num determinado contexto.

A unidade 8.200 também é responsável por criar vírus com a missão de infectar computadores de instalações de adversários, Essa unidade, também possui grupos dedicados a monitorar as atividades da internet, buscando padrões de tráfego considerados hostis, antecipando-se assim a ataques contra redes Isrelenses.

Nos tempos da chamada guerra cibernética, a unidade 8200 conforme relata Beha (2017) representa, simultaneamente, a primeira e a última linha de defesa de Israel, composta de membros jovens aficionados por computadores e por novas tecnologias, mas que protegem as instituições e instalações Israelenses de ataques

cibernéticos que podem ser potencialmente devastadores.

4.2 Os Desafios Cibernéticos do Brasil no Século XXI e o Apoio na Segurança Cibernética

Diniz et al (2014) relatam que numa guerra cibernética, muitos interesses são despertados a respeito do nível de proteção do governo brasileiro e das forças armadas, por isso algumas iniciativas e medidas vem sendo tomadas no Brasil, como a iniciativa da instalação de um escritório de negócios em Jerusalém, destinado aos assuntos de ciências, tecnologia e inovação, além de comércio e economia que poderia ser utilizada para tomada de parceirias no campo cibernético. Desde 2009, que a defesa cibernética tornou-se uma prioridade na estratégia Nacional de Defesa do Brasil, naquele ano foram estipulados três setores de importância estratégica para o país, tais como: o espacial, o nuclear e o cibernético.

Desde 2003 que o programa espacial brasileiro avança de forma muito lenta, principalmente após o acidente com o veículo lançador de satélites V3, que em agosto daquele ano, explodiu na base de lançamento de Alcântara no Maranhão, resultando na destruição do foguete e na morte de 21 técnicos civis. No que tange ao setor nuclear, foi inicialmente aquele que mais evoluiu, principalmente após o início da parceria com a França para construção do submarino nuclear brasileiro, no entanto nos últimos anos também esse programa tem diminuído muito ritmo devido à crise financeira e a escândalos de corrupção.

Em 2012, foi criado o Centro de defesa cibernética, que conforme explica Diniz et al (2014) integra o chamado Sistema Militar de Defesa Cibernética, que tem por objetivo proteger dos sistemas brasileiros informações, sejam eles civis ou militares e inibir possíveis ataques através de uma monitorização constante das redes, esse centro atua também em parceria com o Serviço de Repressão à Crimes Cibernéticos da Polícia Federal, e também com Agência Nacional de telecomunicações - ANATEL, que tem técnicos especializados em segurança de redes informáticas, o Serviço Federal de Processamento de Dados (SERPRO), também é consultado por tsl serviço atuando como parceiro em algumas ações.

Essas são em resumo as principais organizações dedicadas à guerra cibernética no Brasil, o investimento ainda baixo, principalmente se comparado com o que é investido pelas grandes potências, mas o Brasil já está dando seus primeiros

passos. Nos últimos anos esses atuaram em conjunto para defesa cibernética de grandes eventos no Brasil, com destaque para o Rio+20 em 2012, a Copa das Confederações em 2013, a Jornada Mundial da Juventude também em 2013, a Copa do Mundo em 2014 e as Olimpíadas em 2016. Nesses eventos não se registraram grandes ataques as redes informáticas de instituições brasileiras, graças principalmente a atuação desses órgãos.

Em 2014, foi criado o núcleo do Comando De Defesa Cibernética, inserido na estrutura regimental do Comando do Exército Brasileiro e formado por militares os três ramos das forças armadas (DINIZ et al, 2014).

Em 2015 foi criado o Núcleo da Escola Nacional de Defesa Cibernética em parceria com a Universidade de Brasília, cujo objetivo seria capacitar engenheiros e profissionais do setor para o combate a ataques cibernéticos, mas devido a falta de recursos a escola ainda não deu início as suas atividades (SECRETARIA DE ECONOMIA E FINANÇAS – SEF, 2019).

Apesar do país estar ainda muito atrás de outras potências mundiais, é inegável que muito trabalho tem sido realizado nos últimos anos, no entanto, como parece ser a norma, falta algum empenho e principalmente uma fonte estável de recursos no longo prazo.

Segundo Diniz et al (2014) no Brasil os projetos muitas vezes começam bem, e com grandes promessas de recursos, mas depois de algum tempo esses recursos não se materializam e os projetos acabam não evoluindo como inicialmente previsto, e na área cibernética no Brasil parece que está acontecendo o mesmo.

O governo e as forças armadas identificaram os riscos e criaram órgãos e agências que, se bem financiadas e equipadas, são capazes de garantir a segurança do país contra ataques cibernéticos estrangeiros, falta agora é um comprometimento mais sério nessa área, sob a forma principalmente de uma linha de recursos e de financiamento de longo prazo.

Pode-se concluir que o Brasil não está completamente preparado para a guerra cibernética, as forças armadas e o governo têm todos os órgãos e agências necessárias para realização de uma ampla segurança das redes, contudo aparentemente, faltam ainda recursos. A ameaça cibernética é real, e pode colocar em risco a segurança nacional de qualquer país do mundo e o Brasil não é exceção.

Segundo Passarinho (2019) em visita do atual presidente do Brasil a Israel foram firmados convênios nas áreas de ciência e tecnologia; defesa; segurança

Pública; aviação Civil; cyber segurança; e saúde. O Brasil lembrou que Jerusalém é parte inseparável da identidade do povo judeu há mais de três milênios e se tornou o coração político do moderno e próspero Estado de Israel.

Os dois governos concordaram em cooperar em diversos setores, como petróleo e gás, termeletricidade e energias renováveis. No campo da energia e mineração, eles reconheceram o papel transformador da inovação, robótica e cibersegurança. Como dois importantes produtores de gás natural, os dois países trocarão as melhores práticas no desenho de mercados domésticos de gás natural.

Durante essa visita, o presidente do país assinou um Acordo de Cooperação em Ciência e Tecnologia com Isael que permitirá o lançamento de novas iniciativas na área de ciência e tecnologia direcionadas a segurança cibernética.

Por fim, Passarinho (2019) relata que o Brasil pode ganhar pelo fato de se aproximar de Israel é que sendo Israel um polo tecnológico,o Brasil poderia, potencialmente, se beneficiar com parcerias que incluam transferência de conhecimento científico, irigação para o setor agrícola, dessalinização de água em áreas de seca e em especial a segurança cibernética para uso no combate ao crime organizado, parcerias essas que estão na mira do governo brasileiro.

Quadro 2 – Principais pontos relacionados à Defesa Cibernética do Brasil e de Israel

	BRASIL	**ISRAEL**
DEFESA CIBERNÉTICA	Conjunto de ações ofensivas, defensivas e exploratórias com a finalidade de proteger os sistemas de informação de interesse da Defesa, obter dados para produzir inteligência e comprometer o inimigo; Fortalecimento das ações de governança cibernética; Incentivo à criação de soluções inovadoras em segurança cibernética; Ampliação de parcerias relacionadas à segurança cibernética, entre setor público, privado, academia e sociedade; Aumento do o nível de maturidade da sociedade em segurança cibernética.	Desenvolvimento, a instalação de tecnologias avançadas de infraestrutura de comunicação, que incluem além de cabos fixos, a construção de fibra ótica em nível avançado; Arquitetura de rede e de sistema, criptografia, amostras de *malware*, comandos militares e indicadores de defensores cibernéticos; IDF *Cyber Defender Training* Coursell, que consiste em um amplo programa de treinamento militar para segurança cibernética.

Fonte: Departamento de Segurança da Informação – DSI (2018)

De acordo com a Declaração Conjunta por ocasião da Visita Oficial a Israel

do Presidente da República Federativa do Brasil, em 2019, os líderes dos dois países afirmaram que a parceria entre Brasil e Israel está alicerçada sobre valores comuns da liberdade, da democracia, da economia de mercado, da justiça e da paz, e sua determinação comum de buscar a prosperidade para seus povos. Nesse contexto, Israel reiterou seu forte apoio à adesão do Brasil à Organização para Cooperação e Desenvolvimento Econômico (OCDE) (BRASIL, 2019).

Os dois líderes saudaram a assinatura do Acordo de Cooperação em Ciência e Tecnologia, que permitirá planejamento mais adequado, monitoramento e avaliação das atividades bilaterais, assim como o lançamento de novas iniciativas no campo da ciência e tecnologia. Eles expressaram satisfação com os esforços de aproximação dos ecossistemas de inovação brasileiro e israelense. Nesse contexto, celebraram o lançamento de duas chamadas conjuntas da FINEP e da EMBRAPII com a Autoridade Israelense de Inovação, assim como a primeira edição do programa “Scaleup in Brazil” com startups israelenses (BRASIL, 2019).

Os líderes observaram que os intercâmbios entre Brasil e Israel nos campos da ciência, tecnologia e inovação ilustram as sinergias existentes em diversas áreas, que podem e devem ser mais exploradas para estimular investimentos recíprocos, que estão aquém do nível e da complexidade das economias dos dois países. Tais líderes tomaram nota com satisfação da celebração de um acordo de serviços aéreos entre Brasil e Israel. O acordo procura aumentar a conectividade entre os dois países, garantindo ampla liberdade operacional às companhias aéreas, o que ajudará a fortalecer os laços entre as suas sociedades (BRASIL, 219).

Os mesmos se comprometeram a aprofundar a cooperação bilateral em segurança pública e no combate a todas as formas de crime organizado. A esse respeito, expressaram satisfação com as possibilidades oferecidas pela assinatura de um acordo bilateral sobre segurança pública e um memorando de entendimento sobre segurança cibernética. Por fim, os governantes relataram os benefícios mútuos decorrentes da cooperação em assuntos relacionados à defesa e expressaram seu compromisso de se engajarem em um diálogo construtivo nesse campo. Congratularam-se com a assinatura do Acordo de Cooperação em Matéria de Defesa, que fornece arcabolço legal para iniciativas militares conjuntas e abre caminho para laços mais estreitos neste campo (BRASIL, 219).

Segundo o memorando de entendimento o Presidente da Repíblica do Brasil submeteu à apreciação do Congresso Nacional, por meio da Mensagem nº 556 de

2019, o acordo (vide anexo desse trabalho) que tem por objetivo desenvolver, facilitar e maximizar a cooperação entre as instituições científicas e tecnológicas do Brasil e de Israel, com base nas prioridades nacionais no campo de ciência e tecnologia e nos princípios da igualdade, reciprocidade e benefício mútuo, de acordo com as leis nacionais (BRASIL, 2020).

O texto do Acordo conta com apenas 11 dispositivos, com temas pertinentes e divididos em artigos que citam, dentre os principais é possível citar:

Artigo 1º - Define e delineia os objetivos de desenvolvimento, facilitação e maximização da cooperação entre as instituições científicas e tecnológicas nas áreas da ciência e da tecnologia, observados os princípios da igualdade, reciprocidade e benefício mútuo.

Artigo 2º - Define a condução de pesquisas científicas e tecnológicas conjuntas; o desenvolvimento de programas e projetos; e o fornecimento e troca de equipamentos para pesquisa; a implementação de mecanismos de apoio e facilitação de atividades no campo da C&T, a realização de mesas-redondas, seminários, simpósios, workshops e conferências sobre questões de cooperação em C&T; a organização de programas científicos e tecnológicos conjuntos, projetos, workshops, exposições e cursos de treinamento, visitas e intercâmbio de cientistas, pesquisadores, especialistas técnicos e estudantes no ensino superior.

Artigo 3º - As Partes estabelecem a instituição de um “Comitê Diretor” para a Cooperação em C&T, que se reunirá regularmente, e cujos membros serão designados pelas partes, a fim de planejar, monitorar e avaliar as atividades bilaterais; propor atividades de cooperação e estabelecimento de um programa de trabalho; indicar as áreas prioritárias de interesse mútuo em que se busca a cooperação em C&T; trocar e compartilhar informações entre instituições das Partes que manifestarem interesse em realizar projetos no âmbito do Acordo; incentivar a participação do setor privado, da sociedade civil e da academia em atividades bilaterais de C&T.

Artigo 4º - Estabelece regras gerais quanto à repartição dos custos referentes às atividades de cooperação realizadas no âmbito do Acordo.

Artigo 5º - Visa facilitar a entrada, a permanência e a saída de seu território de pessoas, materiais, dados e equipamentos utilizados ou relacionados com as atividades de cooperação, sendo concedidas, em relação a esses, determinadas isenções de impostos e de direitos aduaneiros (BRASIL, 2020).

5. CONCLUSÃO

O desenvolvimento tecnológico proporcionado também pelo crecimento da internet principalmente a partir dos anos 1990, tornou muitas das infraestruturas críticas existentes vulneráveis a ameças cibernéticas, devido a dependencia computacional e a integração das redes, tais ameaças que possuem capacidade de executar ataques através desse novo domínio e podem afetar a segurança e defesa nacional de um Estado, uma vez que possuem a capacidade de parar e neutralizar o funcionamento dessas estruturas essências para a sociedade.

Em um cenário global cada vez mais complexo, onde experimentamos uma expansão do número de usuários e entidades que demandam por conectividade, torna-se mais dificil o controle deste sistemas sem fronteiras. Toda a demanda tecnológica exigida pela sociedade moderna, muito mais dinâmica, exigem recursos computacionais mais velozes e capazes de atender a tais demanadas, com os benefícios vieram muitos riscos, pois a preservação das informações de um Estado contra sabotagem ou espionagem é um elemento considerado vital para a soberania de um país, demandando enormes investimentos para se contraporem a estes riscos que são altamente dinâmicos em uma área em constante revolução.

Neste ponto, acordos e declarações de cooperação entre nações amigas sobre o tema de defesa cibernética poderiam ser estratégico para ambos, já que a troca de experiência traria benefícios compartilhados. As colaborações de troca de conhecimento e intercâmbio de agentes de defesa cibernética, a semelhança do que ocorre na relação entre Colômbia e Coreia do Sul que apresentam uma cooperação um pouco mais robusta ainda que pontual, poderia ser interessante para o Brasil e para Israel.

Israel é muito avançado tecnologicamente e entende que o caminho para a estruturação passa obrigatoriamente pelo desenvolvimento de sua defesa cibernética com base em pesquisa, desenvolvimento e recrutamento de talendos precocemente, sendo com isso um país referência nesta área e com a recente aproximação diplomática entre as nações, o Brasil poderia propor parcerias que alavancassem o desenvolvimento tecnológico de sua defesa cibernética.

O domínio da tecnologia cibernética é fundamental para qualquer país, e a sociedade pode exercer papel relevante quando se tem a consciência de sua importância. No contexto exposto por este trabalho, fica claro que o ambiente de

incerteza e insegurança tem se tornado cada vez mais constante nas relações entre as nações, encorajando-os a despatar a necessidade de autopreservação no que compete a guerra cibernética.

Israel é um país onde essas trocas de experiência e parcerias poderam ser realizadas, visto que tal país possui um sistema de defesa digital bastante sofisticado e as empresas voltadas para o ramo tecnológico e de inovações nas áreas cibernéticas que se destacam mundo afora também são israelenses.

É importante que os fornecedores de soluções de cibersegurança auxiliaem na defesa de empresas no Brasil, visto que**,** ter uma cultura corporativa de que segurança cibernética é essencial. Porém, essa cultura ainda não se difundiu o suficiente. O sistema financeiro, por exemplo, já é bem protegido, mas é preciso disseminar a mentalidade junto às pequenas e médias empresas.

A tecnologia, pode ajudar a detectar ameaças, uma vez que a mesma pode ser feita à distância, sem violar a soberania de um estado. Por outro lado, a necessidade de maior cooperação e informação internacional é essencial.

Em termos de defesa, os estados que desejam reforçar suas capacidades podem se concentrar no melhor uso da tecnologia. Defender o reino cibernético exige que tecnologias existentes sejam melhoradas e novas sejam criadas. O mecanismo de defesa também deve ser apropriado para a situação. Nos estágios iniciais de um ataque, antes que qualquer dano real tenha sido feito ou sistemas penetrados, esforços para interromper ou redirecionar o ataque podem ser adequados. Se o sistema tiver sido penetrado, ou dano feito, o mecanismo de defesa deve procurar conter o ataque, bem como evitar que o invasor saiba que o intrusão foi descoberta e interrompida com sucesso.

Proteger redes nos setores governamental e privado exigem nova legislação e regulamentos. Novas agências governamentais porem precisam ser criados para ajudar a elaborar requisitos específicos e para garantir que mecanismos de defesa são implementados.

O Comando Cibernético de Israel é um exemplo de organização centralizada e responsável para supervisionar a criação e implementação de estratégias de defesa cibernética, incluindo esforços para trabalhar com o setor privado.

Governos e empresas privadas e acadêmicas devem colaborar para desenvolver novas ferramentas e estratégias técnicas defensivas e melhorar as existentes. Os governos podem oferecer incentivos monetários a entidades privadas,

apropriados, para ajudar a construir defesas robustas.

Medidas surpreendentemente simples podem ser bastante eficazes ao combate aos ataques ciberenéticos, assim como as utilizadas em Israel como exigir que funcionários do governo agências e entidades privadas conectadas a redes governamentais usem senhas fortes que são alteradas regularmente, bem como treinamento obrigatório para identificar e evitar ciberameaças.

Os defensores também devem considerar a cadeia de abastecimento usada para projetar e fabricar seus equipamentos, como: *hardware, firmware* e *software* que estão atualmente sendo criados e construídos em todo o mundo, o que torna difícil garantir que um o produto seja definitivamente seguro. Isto porque, as empresas e nações em que esse equipamento é projetado e fabricado pode incluir códigos ocultos que permitem aos dispositivos eventualmente ser hackeado.

Os governos devem considerar trabalhar em conjunto com empresas e nações estrangeiras para desenvolver um sistema de acreditação que garanta que os processos de design e fabricação sejam transparentes. Tal plano apresenta perigos, no entanto, principalmente porque, pode tornar mais difícil proteger a propriedade intelectual, aumentar o preço do equipamento e adicionar uma despesa adicional e até mesmo reduzir o ritmo de inovação.

A criação de leis globais, normas e acordos internacionais pode ser útil no reforço da defesa cibernética e quanto mais os países se desempenharem em desenvolver um papel ativo na criação dessas leis e normas, quanto mais envolvido o país estiver, maior será sua capacidade de proteger seus interesses e moldar o sistema futuro.

Tentar construir leis e normas é um empreendimento barato que poderia potencialmente melhorar a segurança cibernética para nações ao redor do mundo. Se bem-sucedidos, eles seriam um meio de reforçar não apenas defesa, mas também detecção, dissuasão e derrota.

É difícil dizer quando um ataque ocorreu, entretanto, para aumentar sua capacidade de derrotar os invasores no reino cibernético, é preciso se espelhar em grandes países como Israel que como já dito apresenta um enorme poder de defesa, sendo capazes de isolar as nações atacantes e adotar ferramentas de confronto, como sanções econômicas ou diplomáticas, no esforço de convencê-los de que a ação ofensiva contínua é muito cara.

As perspectivas de derrotar um inimigo no reino cibernético podem ser

aumentadas se os países assim como Israel, se concentrarem sobre maneiras de destruir as capacidades cibernéticas do oponente com um conhecimento e treinamento extenso, além de equipamentos necessários e sifisticados de ataque.

Além de punições legais mais severas, os países podem tomar medidas para mitigar a ameaça de indivíduos, isolando hackers individuais, interrompendo sua internet conexões ou compartilhamento informações sobre o tais hackers, a fim de limitar sua capacidade de planejar ou lançar um ataque.

Para aumentar a resiliência no domínio cibernético, o Brasil deve buscar uma diversidade de equipamentos, ou seja, hardware e softwares que não devem ser fornecidos por uma fonte ou empresa. Quando há uma diversificação de equipamentos é possível que o país consiga isolar melhor o problema. Para ajudar a construir resiliência para as redes mais críticas, o país pode projetar arquitetura cibernética que oferece vários caminhos para sistemas de controle.

Os ataques cibernéticos não são fundamentalmente diferentes de outras ameaças e podem ser abordados aplicando os princípios clássicos da estratégia militar. Esses princípios podem não fornecer um resposta completa, tanto quanto eles não fazem quando aplicados a outras ameaças convencionais, e modificações certamente serão necessárias para os desafios colocados pelas ciberameaças.

Desta maneira, a chave para a adaptação neste cenário global que se apresenta é o investimento no desenvolvimento de tecnologias capazes de se precaver a ameaças externas, trocar de experiência e firmar parcerias com países como Israel que como já dito, possui um domínio mais avançado da tecnologia e portanto, está mais capacitado a minimizar esses tipos de ataque, facilitando assim, o caminho daqueles que, assim como o Brasil, precisam evoluir nesta que é o novo campo de batalha do século XXI .

REFERÊNCIAS

BEHA, Richard**. Israel tem a melhor (e mais misteriosa) máquina de startups do mundo**. 2017. Disponível em: orbes.com.br/negocios/2017/01/israel-tem-a-melhor-e-mais-misteriosa-maquina-de-startups-do-mundo/. Acesso em 20.ago.2020

BRASIL. MINISTÉRIO DA DEFESA. **Estratégia Nacional de Defesa**. 2a . Ed. Brasília: Ministério da defesa, 2008.

_____.**Declaração Conjunta por ocasião da Visita Oficial a Israel de o Presidente da República Federativa do Brasil, em 2019**. Disponível em: Itamaraty.gov.br/pt-BR/notas-a-imprensa/20235-visita-oficial-a-israel-de-sua-excelencia-o-presidente-da-republica-federativa-do-brasil-jair-bolsonaro. Acesso em: 21.set.2020

_____.**E-cyber.** 2018. Disponível em: http://dsic.planalto.gov.br/links-destaques/e-ciber. Acesso em 21.set.2020

_____.Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília, 2013b.

_____.Ministério da Defesa. **MD30-M-01**: Doutrina Militar de Defesa Cibernética. Brasília, 2014.

_____. Ministério da Defesa. **Minuta de nota de coordena S D M Defesa**. Exército Brasileiro, Estado-Maior do Exército, Brasília, 2010. BRASIL. Força Aerea Brasileira. Grupo de Trabalho do Projeto Carponis-1 realiza 1ª Reunião de 2019. Disponível em:<http://www.fab.mil.br/noticias/mostra/33490/ESPA%C3%87O%20-%20Grupo%20de%20Trabalho%20do%20Projeto%20Carponis-1%20realiza%201%C2%AA%20reuni%C3%A3o%20de%202019>.Acesso em: 30 Jul. 2020.

_____.**Brasil e Israel firmam cinco acordos e um memorando de entendimento.** 2020. Disponível em: https://www.correiodopovo.com.br/not%C3%ADcias/mundo/brasil-e-israel-firmam-cinco-acordos-e-um-memorando-de-entendimento-1.329961. Acesso em: 2 set. 2020.

_____.**Marinha.** Corpo de Fuzileiros Navais. CGCFN-01: Manual de Fundamentos de Fuzielros Navais. Rio de Janeiro, 2013a.

_____.**Ministério da Ciência, Tecnologia, Inovações e Comunicações**. Programa Nacional de Banda de Larga. Disponível em: <https://www.mctic.gov.br/mctic/opencms/textogeral/banda_larga.html>.Acesso em: 15 Jul. 2020.

_____.GSI – GABINETE DE SEGURANÇA INSTITUCIONAL. Portaria 45, de 8 de setembro de 2009. Publicada no DOU em 09/09/2009. Brasília: DOU, 2009a. BRASIL. Livro Branco de Defesa Nacional. Brasília: Presidência da República, 2012.

CANONGIA, Claudia; MANDARINO JUNIOR, Raphael. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parcerias Estratégicas**, v. 14, n. 29, p. 21-46, 2010.

CLARKE, Richard; KNAKE, Robert.**Guerra Cibernética**: A próxima ameaça à segurança e o que fazer a respeito. BRASPORT; 1ª Edição ,2015

CLAUSEWITZ. Carl von. ***On War*.** Translation of: *Vom Kriege*. [1832] First Princeton. Paperback printing, 1989

DINIZ Gustavo, MUGGAH, Robert, Glenny, Misha. **Deconstructing Cyber Security in Brazil: Threats and Responses**. Institute Garapé Publication Strategic. December, 2014.

DUTRA, André Melo Carvalhais. **Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto**. IX Simpósio de Guerra Eletrônica, 2007.

FERDIKA, Allison. **Brazil Finds More Than a Friend in Israel.** Disponível em: https://www.realclearworld.com/articles/2019/01/06/brazil_finds_more_than_a_friend_in_israel_112942.html Acesso em 25.ago.2020.

GEERS, **Kenneth. Strategic cyber security**. Kenneth Geers, 2011.
GSI – GABINETE DE SEGURANÇA INSTITUCIONAL. Portaria 34, de 5 de agosto de 2009. Publicada no DOU em 06/08/2009. Brasília: DOU, 2009b.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). **Global Cybersecurity** Index 2017. Genebra: 2018. ISBN: 978-92-61-25071-3. Disponível em: . Acesso em: 27 set. 2018.

LEONARDI, Ivan. Novo satélite brasileiro terá 70 cm de resolução espacial. Disponível em: http://geoeduc.com/blog/novo-satelitebrasileiro-tera-70-cm-de-resolucao-espacial/>. Acesso em: 20 Ago. 2020.

MARINESCU, Dan C., **Cybernetics: Complex Systems and Clouds**. 2017. Disponível em: https://www.sciencedirect.com/topics/computer-science/cybernetics

MELO, Abner Alves de; BARBOSA, George Gustavo da Costa; CRUZ,Jorge Vagner Vieira da; SOUZA, Edson Barbosa de; FERREIRA, Larissa Lima; KLAUS, Liliane Correa de Oliveira; PASSOS, José Carlos dos; COSTA, Luiz Rosado; BEXIGA, Victor Sardinha; BARROS E SILVA, Nilo Sérgio de Lima. Guerra Cibernética: responsabilidade do exército, dever de todos **Revista Interdisciplinar de Ciências Aplicadas à Atividade Militar** – Ano 2 Número 1 – 1° semestre de 2012

NYE, Joseph S. **O futuro do poder.** São Paulo: Benvirá, v. 333, 2012.

NYE , Joseph S. **Cyber power.** HARVARD UNIV CAMBRIDGE MA BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS, 2010.

OLIVEIRA NETTO, Alvim Antônio de. **Metodologia da pesquisa científica: guia prático para apresentação de trabalhos acadêmicos.** Florianópolis: Visual Books, 2006. 160 p.

PASSARINHO Natália. **Embaixada em Jerusalém**: o que o Brasil pode ganhar e perder se aproximando de Israel.2019. Disponível em: https://www.bbc.com/portuguese/brasil-46815018. Acesso em: 25 Ago. 2020

PINTO, Monica. **Exclusivo**: cinco perguntas sobre o Sistema de Proteção da Amazônia – SIPAM. 2007. Disponível em: <https://noticias. ambientebrasil.com.br/exclusivas/2007/03/13/29996-exclusivo-cincoperguntas-sobre-o-sistema-de-protecao-da-amazonia-sipam.html>. Acesso em 25 Ago. 2020.

PORTELA, Lucas Soares. **Geopolítica do espaço cibernético e o poder: o exercício da soberania por meio do controle**. Revista Brasileira de Estudos de Defesa, v. 5, n. 1, 2019.

PROJETO SisGAAZ. 2019. Disponivel em: <https://www.defesa. gov.br/component/content/ar ticle/156-infograficos/14789-projetosisgaaz?Itemid=101>. Acesso em: 26 ago 2020.

SANTOS, José Carlos dos. **Podemos recrutar "hackers".** Revista Época. 2011. Disponível em: http://revistaepoca.globo.com/Revista/Epoca/0,,EMI249428-15223,00GENERAL+JOSE+CARLOS+DOS+SANTOS+PODEMOS+RECRUTAR+HACKERS.html. Acesso em 05 mai. 2020.

SILVA, Washington Rodrigues da. **Análise econômica dos impactos de ataques cibernéticos**. Dissertação Mestrado. Universidade de Brasília, 2018. 107 p.

SISFRON. 2019 Disponível em: <http://www.dct.eb.mil.br/index.php/termo-de-fomento-a-ser-firmado-entre-o-exercito-brasileiroe-a-fundacao-parque-tecnologico-de-itaipu-br/35-programas-eparceiros/97-sisfron>. Acesso em: 28 Ago. 2020.

TZU, Sun; PIN, Sun. **A Arte da Guerra**. Edição Completa. Tradução a partir do Inglês de Ana Aguiar Cotrim. 1ª ed. São Paulo: Martins Fontes, 2002, 336p.

UNITED STATES. **DEPARTMENT OF DEFENSE**. Department of Defense Strategy for Operating in Cyberspace. DIANE Publishing, 2012.

UNIVERSE TODAY. Disponível em: <https://www.universetoday.com/85322/what-is-low-earth-orbit/>. Acesso em: 29 Ago. 2020.

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

WIENER, Norbert. **Cibernética**: ou controle e comunicação no aminal e na máquina.Ed Perspecitiva 1ªed, 2017, 248p.

WIENER, Norbert. **The Human use of Human Beings**. Londres, Free Association Books, 1989.

WIENER, Norbert**. Cibernética ou controle e comunicação no animal e na máquina**. Tradução de Gita K. Ghinzberg. São Paulo: Polígono e Universidade de São Paulo, 1970.

ZHOU, Zunyou. **China's Draft Cybersecurity Law**. China Brief 15, no. 24. 2015. https://jamestown.org/program/chinas-draft-cybersecurity-law/. Acesso em: 2 set. 2020.

ANEXO:

MENSAGEM
No 556, de 2019.
(Do Poder Executivo)

Submete à consideração do Congresso Nacional o texto do do Estado de Israel, assinado em 31 de março de 2019

Autor: PODER EXECUTIVO

Relator: Deputado AROLDO MARTINS

I – RELATÓRIO:

O Excelentíssimo Senhor Presidente da República submete à apreciação do Congresso Nacional, por meio da Mensagem nº 556 de 2019, o Acordo para A referida mensagem presidencial encontra-se instruída com exposição de motivos de lavra dos Senhores Ministros de Estado das Relações Exteriores e da Ciência e Tecnologia. O objetivo do presente Acordo é desenvolver, facilitar e maximizar a cooperação entre as instituições científicas e tecnológicas de ambos os países, com base nas prioridades nacionais no campo de ciência e tecnologia e nos princípios da igualdade, reciprocidade e benefício mútuo, de acordo com as leis nacionais. O texto do Acordo conta com apenas 11 dispositivos, os quais disciplinam os temas pertinentes a seu objeto da seguinte forma:

O Artigo 1º define e delineia os objetivos da avença, ou seja, o desenvolvimento, facilitação e maximização da cooperação entre as instituições científicas e tecnológicas nas áreas da ciência e da tecnologia, observados os princípios da igualdade, reciprocidade e benefício mútuo, e em 2 concordância com a legislação nacional de cada uma das Partes Contratantes.

O Artigo 2 estabelece as modalidades da cooperação a ser desenvolvida e define, entre elas: a) a condução de pesquisas científicas e tecnológicas conjuntas; b) o desenvolvimento de programas e projetos; e o fornecimento e troca de equipamentos para pesquisa; c) a implementação de mecanismos de apoio e facilitação de atividades no campo da C&T, d) a realização de mesas-redondas, seminários, simpósios, workshops e conferências sobre questões de cooperação em C&T; e) a organização de programas científicos e tecnológicos conjuntos, projetos, workshops, exposições e cursos de treinamento, visitas e intercâmbio de cientistas, pesquisadores, especialistas técnicos e estudantes no ensino superior.

Por meio do Artigo 3 as Partes estabelecem a instituição de um "Comitê Diretor" para a Cooperação em C&T, que se reunirá regularmente, e cujos membros serão designados pelas Partes. Conforme esse dispositivo, inscrevem-se no âmbito das competências previstas para o "Comitê Diretor": planejar, monitorar e avaliar as atividades bilaterais; propor atividades de cooperação e estabelecimento de um programa de trabalho; indicar as áreas prioritárias de interesse mútuo em que se busca a cooperação em C&T; trocar e compartilhar informações entre instituições das Partes que manifestarem interesse em realizar projetos no âmbito do Acordo; incentivar a participação do setor privado, da sociedade civil e da academia em atividades bilaterais de C&T.

O Artigo 4 estabelece regras gerais quanto à repartição dos custos referentes às atividades de cooperação realizadas no âmbito do Acordo.

O Artigo 5 contém disciplina tocante ao tema do trânsito internacional do pessoal e dos equipamentos empregados nas atividades contempladas pelo Acordo. Nesse sentido, é fixado o compromisso das Partes quanto a facilitar a entrada, a permanência e a saída de seu território de pessoas, materiais, dados e equipamentos utilizados ou relacionados com as atividades de cooperação, sendo concedidas, em relação a esses, determinadas isenções de impostos e de direitos aduaneiros.

O Artigo 6 da avença em apreço regulamenta as questões 3 referentes à proteção dos direitos de propriedade intelectual emergente e relacionada aos resultados obtidos em decorrência das atividades desenvolvidas sob a égide do Acordo.

O Artigo 7 dispõe sobre a troca de informações obtidas por meio do Acordo e, também, sobre o controle de divulgação de informações em relação a terceiros. Dispõe também sobre o anúncio, publicação e exploração comercial dos resultados científicos e tecnológicos derivados das atividades de cooperação realizadas.

Os artigos 8 a 11 contemplam normativa de natureza jurídica adjetiva, relacionada à aplicação do Acordo. São dispositivos que abordam e disciplinam os seguintes temas: modo de entrada em vigor do Acordo; prazo de vigência; condições de denúncia e respectivos efeitos; possibilidade de apresentação e aprovação de emendas ao texto; procedimento para solução de controvérsias; e, por último, a definição da abrangência das normas do Acordo, sendo nesta quadra consignado, por meio de menção expressa, que qualquer atividade executada por uma das Partes Contratantes, em cumprimento do Acordo, estará sujeita às leis e regulamentos nacionais. É o relatório.

II - VOTO DO RELATOR As relações internacionais entre o Brasil e Israel remontam à própria fundação do Estado de Israel. O diplomata brasileiro Oswaldo Aranha presidiu a Assembleia Geral das Nações Unidas em 1947, que tomou a histórica decisão da partilha que levou à criação de Israel, em 1948.

O ato constituiu-se em importante marco nas relações do Brasil com o nascente Estado judeu, pois simbolizou verdadeiro compromisso moral do Brasil, que foi um dos primeiros países a reconhecer o Estado de Israel em 1949. Em 1951 foi criada a Legação do Brasil em Tel Aviv, elevada, em 1958, à categoria de Embaixada. Também em 1951, Israel inaugurou sua Embaixada no Brasil, no Rio de Janeiro.

Além das relações internacionais formais, entre Estados, as relações entre Brasil e Israel também se pautam em fortes vínculos humanos e culturais, tendo em vista a multissecular presença judaica no Brasil. O primeiro fluxo migratório de judeus ocorreu em Recife, no século XVII e trouxe pessoas oriundas da Península Ibérica, que fugiam da inquisição religiosa. Foram os chamados cristãos-novos.

Durante esse período, emigraram para o Recife milhares de judeus sefarditas, de origem portuguesa, refugiados nos Países Baixos, que vieram para a então colônia holandesa atraídos pela liberdade de culto religioso.

Foi assim fundada a Kahal Zur Israel (Congregação Rochedo de Israel), a primeira sinagoga das Américas, que funcionou em Pernambuco durante o período de dominação holandesa, de 1630 a 1657. Posteriormente, seguiram-se novas ondas migratórias, nos séculos XIX e XX, seguindo-se fluxo periódico e constante, sendo protagonizadas sobretudo por judeus asquenazes, provenientes do leste europeu. Atualmente, estima-se que a comunidade israelita no Brasil totalize entre 97 e 150 mil membros.

É a décima maior do mundo e a segunda maior da América Latina, sendo superada apenas pela população judaica argentina. Além disso, a coletividade israelita no Brasil convive de modo pacífico com a comunidade árabe e seus descendentes presente no País. Por outro lado, a comunidade brasileira em Israel alcança, o número de 9 mil membros. Sob o ponto de vista das relações internacionais, as relações Brasil-Israel se inscrevem no contexto da política externa brasileira para o Oriente Médio.

Tal política passou, desde o início deste século, a adquirir o caráter de prioridade na política externa brasileira. Nesse período, vem ocorrendo gradativa e constante a aproximação do Brasil com Israel. Marco resultante de tal movimento é constituído pela celebração do Acordo de Livre Comércio entre Israel e o Mercosul, em 18/12/2007, constituindo-se Israel no primeiro parceiro extra regional a firmar tal instrumento com o bloco.

Trata-se de importante parceria que baseada na firma de acordo comercial que prevê a abertura de mercados e que cobre, além do comércio de bens, a instituição de 5 regras de origem, salvaguardas, cooperação em normas técnicas, sanitárias e fitossanitárias, cooperação tecnológica e técnica, e cooperação aduaneira.

Na realidade, Brasil e Israel compartilham longa história de cooperação nas áreas científicas e tecnológicas, no setor agrícola, assim como nas áreas da defesa e em temas militares. Desde os anos 1960, Israel contribui para o desenvolvimento da agricultura do semiárido, por meio da implantação e difusão de técnicas de irrigação em regiões do Nordeste brasileiro. Além da cooperação interestatal, registra-se intenso diálogo entre instituições privadas ou não governamentais brasileiras e israelenses, modalidades cooperação que serão ratificadas e ampliadas pelo acordo em apreço.

A partir do governo do Presidente Jair Bolsonaro as relações entre o Brasil e Israel ganharam novo e forte impulso. O Primeiro-ministro de Israel, Benjamin Netanyahu esteve em visita ao Brasil no início deste ano, para comparecer à posse do Presidente Jair Bolsonaro.

Durante a visita o Premier israelense convidou o Presidente Bolsonaro a visitar Israel. Aceito o convite, a visita do Presidente do Brasil a Israel ocorreu ainda em março de 2019. Na ocasião, o Primeiro-ministro de Israel vaticinou que a cooperação entre os dois í á z “ fí emprego, na segurança, na agricultura, recursos hídricos, na indústria, enfim, em todos os domínios d h ” convite do Primeiro-Ministro de Israel, Benjamin Netanyahu, o Presidente Jair Bolsonaro cumpriu visita oficial a Israel de 31 de março a 3 de abril de 2019, abrindo um novo capítulo na história das relações entre os dois países. Na ocasião foi emitido documento oficial bilateral, denominado “D j ocasião da Visita Oficial a Israel de Sua Excelência o Presidente da República Federativa do Brasil, Jair Bolsonaro – ”, a qual expressa os principais pontos de convergência e as diretivas que haverão de pautar o relacionamento entre os dois países.

Nos termos dessa Declaração Conjunta cabe destacar os seguintes pontos: - o compromisso

recíproco quanto a alçar as relações bilaterais a um novo patamar, elevando o nível de prioridade e consolidando os sólidos vínculos históricos existentes entre os dois países. Nesse contexto, foram 6 celebrados diversos atos internacionais, entre os quais o Acordo sob análise, que visam a ampliar e aprofundar a cooperação bilateral, inclusive atualizando instrumentos anteriores, nos campos da ciência e tecnologia; defesa; segurança pública; aviação civil; segurança cibernética e saúde; -a reafirmação de que a parceria entre Brasil e Israel está alicerçada sobre valores comuns da liberdade, da democracia, da economia de mercado, da justiça e da paz, e sua determinação comum de buscar a prosperidade para seus povos.

Nesse contexto, Israel reiterou seu forte apoio à adesão do Brasil à Organização para Cooperação e Desenvolvimento Econômico (OCDE); - a reafirmação, por parte de Israel, do apreço quanto ao papel fundamental desempenhado pelo Brasil durante a Assembleia Geral das Nações Unidas que aprovou a Resolução 181, em 1947, sob a presidência do ex-Ministro das Relações Exteriores do Brasil, Oswaldo Aranha, abrindo caminho para a recriação do Estado de Israel na terra ancestral do povo judeu, em 14 de maio de 1948; - o reconhecimento, por parte do Brasil, de que Jerusalém, é parte inseparável da identidade do povo judeu por mais de três milênios e se tornou o coração político do moderno e pujante Estado de Israel. Nesse espírito, e 72 anos depois de participar do primeiro capítulo da recriação do Estado de Israel, o Brasil decidiu estabelecer um escritório de negócios em Jerusalém para a promoção do comércio, investimento, tecnologia e inovação, a ser coordenado pelo Ministério das Relações Exteriores.

A mencionada visita gerou diversos frutos, em termos de celebração de atos internacionais bilaterais - dentre os quais, o acordo em epígrafe, os quais podem ser agrupados em sete grandes áreas de interesse, a saber: Ciência, Tecnologia e Inovação, Energia, Promoção comercial e investimentos, Aviação Civil, Segurança pública e segurança cibernética, Defesa e também sobre a situação da Venezuela.

Com relação ao tema da C&T e inovação, os dois líderes consignaram na Declaração sua saudação à firma do presente Acordo de Cooperação em Ciência e Tecnologia que, segundo eles, permitirá 7 planejamento mais adequado, monitoramento e avaliação das atividades bilaterais, assim como o lançamento de novas iniciativas no campo da ciência e tecnologia. Os dois Chefes de Estado expressaram, ainda, satisfação com os esforços de aproximação dos ecossistemas de inovação brasileiro e israelense. Nesse contexto, celebraram o lançamento de duas chamadas conjuntas da FINEP e da EMBRAPII com a Autoridade Israelense de Inovação, assim como “Scaleup in Brazil” O tema da C&T e inovação é considerado da mais alta prioridade para Israel.

O desenvolvimento dessa área tem se mostrado vital na construção e preservação do Estado Israel, em diversas áreas, sobretudo se consideradas questões envolvendo o território, em que o desenvolvimento da agricultura e da irrigação foram fundamentais, assim como as tecnologias na área militar e da defesa e, ainda, o desenvolvimento nas áreas da informática e de tecnologias da informação.

Em vista disso, Israel investe maciçamente na educação de jovens. Cerca de 48% dos israelenses com mais de 15 anos possuem mais de 12 anos de estudos. Como um país tão pequeno, mas com alto nível educacional, Israel surpreende por apresentar alguns aspectos interessantes em relação às ciências, tais como: - é um dos países que mais investe em Pesquisa e Desenvolvimento em relação ao seu Produto Interno Bruto; - está entre os países

com maior número de autores publicados nos campos das ciências naturais, engenharia, agricultura e medicina; - onze (11) cidadãos israelenses foram laureados com o Prêmio Nobel nas áreas de física, química, economia e paz, sendo que mais de 19% dos prêmios Nobel foram concedidos a cidadãos de ascendência judaica.

De outra parte, um dos principais componentes que diferenciam Israel de outros países são os investimentos na área de ciências, principalmente em biotecnologia. Em 2016, o total de investimentos em empresas de ciências da vida em Israel foi de 823 milhões de dólares, sendo 8 que os investimentos anuais no setor se apresentam contínuos, o que garante uma segurança para as empresas continuarem investindo em pesquisa e desenvolvimento a longo prazo. Além disso, nesse mesmo ano, foram investidos 717 milhões de dólares por investidores estrangeiros e 106 milhões por israelenses em companhias de ciências da vida.

Na área de defesa e no campo das tecnologias militares é praticamente desnecessário e redundante mencionar que Israel é nação que figura como expoente mundial de máxima expressão. Ao longo de décadas de tensões e conflitos regionais, as forças armadas israelenses desenvolveram amplo aparato tecnológico de apoio ao arsenal militar ajudaram, bem como promoveram a formação de mão-de-obra altamente especializada. Outra característica interessante no ambiente da C&T de Israel é a proliferação de startups que, embora possam ser considerados negócios de elevado risco e incerteza, produzem por vezes resultados surpreendentes e inovadores.

O número de startups cresceu de maneira exponencial em Israel, tornando o país líder em quantidade desse tipo de empresa por número de habitantes. Na maioria estas empresas são resultado de um tripé de sucesso, um modelo que tem gerado muito sucesso em Israel para incentivar pesquisa e inovação nas universidades gerado pela cooperação baseado no tripé Universidade – Empresa – Sociedade.

Os israelenses conseguiram organizar um esquema no qual: (1) a sociedade mostra os problemas e fornece o investimento, (2) as universidades pesquisam para resolver esse problema e (3) as empresas, muitas delas sob a forma de startups, auxiliam na transformação da pesquisa em inovação, o que acaba por gerar avanços e ganhos, para os empreendedores, para sociedade e para o país, com o aumento da produtividade global e do volume total de conhecimento científico agregado.

O presente "Acordo para Cooperação em Ciência e Tecnologia entre o Governo da República Federativa do Brasil e o Governo do Estado de Israel" constitui importante expressão da vontade dos dois países em aprofundar ainda mais suas relações bilaterais. 9 O instrumento internacional visa promover a cooperação entre instituições científicas e tecnológicas de ambos os países, servindo-se para tal de diversas estratégias, tais como, viabilizar a realização de diversas atividades conjuntas, em pesquisa básica e aplicada, na área de C&T, incluindo o lançamento de chamadas para projetos.

O Acordo prevê também a constituição “Comitê Diretor” õ á j indicação de áreas prioritárias da cooperação, monitoramento e avaliação das atividades bilaterais de C&T. Conforme destacado supra, em seus dispositivos normativos, o acordo define seu objetivo e regulamenta a cooperação, modalidades, implementação, financiamento, entrada de pessoal e equipamento, propriedade intelectual, troca de informações de pesquisa e, de modo complementar, contempla questões procedimentais relacionadas à sua aplicação, como entrada em vigor, duração, denúncia, formulação de emendas, solução de controvérsias e

abrangência de sua aplicabilidade.

Além disso, o ato internacional atualiza, na parte referente à cooperação científica e tecnológica, o "Acordo Básico de Cooperação Técnica entre os Governos dos Estados Unidos do Brasil e o Governo de Israel", firmado em 1962. Por outro lado, o ato proporciona, igualmente, instrumento jurídico mais sólido e robusto, que conferirá melhor fundamento quanto ao acesso a recursos orçamentários para a cooperação do que o "Protocolo de Intenções firmado entre o MCTIC brasileiro e o MCT israelense, em 2018.

Ao mesmo tempo, o acordo possibilita, igualmente, que outros órgãos da Administração Pública ligados à C&T se beneficiem da estrutura estabelecida pelo documento. Como se pode concluir, a partir dos elementos apresentados no relatório e dos argumentos descritos supra neste parecer, o instrumento internacional em epígrafe consagra estrutura normativa hábil, coerente e que condiz com o objetivo e as finalidades para as quais foi concebida, ou seja o desenvolvimento de atividades de cooperação internacional bilateral no campo da C&T, entre os Brasil e Israel.

O ato internacional não apenas contempla dispositivos comuns às avenças do gênero, como confere tratamento 10 pormenorizado e específico a determinadas questões, com vistas a garantir maior eficácia à implementação da cooperação bilateral nas áreas da ciência, da tecnologia e da inovação entre os dois países. Ante as razões expostas, VOTO pela aprovação do Federativa do Brasil e o Governo do Estado de Israel, assinado em Jeru , nos termos do projeto de decreto legislativo que apresentamos em anexo.

Sala da Comissão, em.....de.....de 2019.

Deputado AROLDO MARTINS Relator