UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE CIÊNCIAS ECONÔMICAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ESTUDOS ESTRATÉGICOS INTERNACIONAIS

RAFAELA DA COSTA VECHIATO

O PODER CIBERNÉTICO EM ISRAEL:
UMA ANÁLISE CRÍTICA

Porto Alegre
2023

RAFAELA DA COSTA VECHIATO

O PODER CIBERNÉTICO EM ISRAEL:
UMA ANÁLISE CRÍTICA

Dissertação de Mestrado do Programa de Pós-Graduação em Estudos Estratégicos Internacionais da Faculdade de Ciências Econômicas, Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do título de Mestre em Estudos Estratégicos Internacionais.

Orientador: Prof.ª Dr.ª Marco Aurélio Chaves Cepik

Porto Alegre
2023

CIP - Catalogação na Publicação

Vechiato, Rafaela da Costa
O poder cibernético em Israel: uma análise crítica / Rafaela da Costa Vechiato. -- 2023.
117 f.
Orientador: Marco Aurélio Chaves Cepik.

Dissertação (Mestrado) -- Universidade Federal do Rio Grande do Sul, Faculdade de Ciências Econômicas, Programa de Pós-Graduação em Estudos Estratégicos Internacionais, Porto Alegre, BR-RS, 2023.

1. Israel. 2. Poder Cibernético. 3. Capacidades Cibernéticas. 4. Doutrina Militar. I. Cepik, Marco Aurélio Chaves, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

RAFAELA DA COSTA VECHIATO

O PODER CIBERNÉTICO EM ISRAEL:
UMA ANÁLISE CRÍTICA

Dissertação de Mestrado do Programa de Pós-Graduação em Estudos Estratégicos Internacionais da Faculdade de Ciências Econômicas, Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do título de Mestre em Estudos Estratégicos Internacionais.

Orientador: Prof.º Dr.º Marco Aurélio Chaves Cepik

BANCA EXAMINADORA:

_____
Profº. Dr. Marco Aurélio Chaves Cepik – Orientador
(PPGEEI/UFRGS)

_____
Profº. Dr. Érico Esteves Duarte
(PPGEEI/UFRGS)

_____
Prof.ª Dra. Graciela De Conti Pagliari
(PPGRI/UFSC)

_____
Prof.º Dr. Fabiano Pellin Mielniczuk
(PPGEEI/UFRGS)

AGRADECIMENTOS

Estes dois anos foram muito conturbados com a pandemia e os ataques de ansiedade. Período importante para a história brasileira, sobretudo para a ciência. E eu, aqui, tentando ser cientista. Minha vida mudou drasticamente, mas agradeço, do fundo do meu coração, as pessoas que estiveram ao meu redor e me auxiliaram de alguma maneira.

Gostaria de agradecer, especialmente, ao meu orientador Prof. Dr. Marco Aurélio Chaves Cepik pelo apoio prestado, pelo trabalho realizado e pelo tempo gasto em assuntos relacionados a minha dissertação e ao meu crescimento como estudante e acadêmica. Sou grata por ter tido tal renomado orientador, um grande exemplo para mim e o maior gaúcho-mineiro de todos.

Agradeço ao Programa de Pós-Graduação em Estudos Estratégicos Internacionais (PPGEEI) e à Universidade Federal do Rio Grande do Sul (UFRGS) pela possibilidade da formação através da universidade pública, gratuita e de excelência. Por fim, meus sinceros agradecimentos à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo apoio financeiro. Agradeço, a estas instituições, por proporcionarem ciência e sabedoria em tempos conturbados.

RESUMO

O presente trabalho analisa se Israel detém ou não capacidades cibernéticas ofensivas e defensivas. Para tanto, o contexto histórico e os aspectos sociais auxiliam na compreensão da grande estratégia israelense e, por consequência, do ecossistema existente, que se relaciona e sustenta o poder cibernético em Israel. Dessa maneira, foram utilizados publicações de fontes primárias e secundárias, além de uma contextualização de uma literatura mais geral sobre os temas abordados nos capítulos. O método empregado, nesta dissertação, foi observacional do tipo qualitativo, como referentes empíricos, os documentos oficiais e a bibliografia especializada. Israel possui uma política de defesa nacional robusta, apesar de não possuir uma estratégia formal de segurança nacional. O país entende que a defesa cibernética é vital para garantir a continuidade das operações das organizações nacionais e possui uma tendência à centralização da segurança cibernética, apesar da ausência da política oficial de cooperação entre as instituições cibernéticas. Por fim, conclui-se que o poder cibernético, em Israel, está ancorado em um amplo ecossistema de capacidades industriais, científicas e de pessoal especializado, bem como na existência de unidades especializadas, civis e militares, e de uma doutrina específica de uso do poder cibernético para a sustentação do poder estatal.

Palavras-chave: Israel. Poder Cibernético. Capacidades Cibernéticas. Doutrina Militar.

ABSTRACT

The present work analyzes whether or not Israel has offensive and defensive cyber capabilities. To this end, the historical context and social aspects help to understand the Israeli grand strategy and, consequently, the existing ecosystem, which relates to and sustains cybernetic power in Israel. In this way, publications from primary and secondary sources were used, as well as a contextualization of a more general literature on the topics addressed in the chapters. The method employed, in this dissertation, was observational of the qualitative type, as empirical references, the official documents and the specialized bibliography. Israel has a robust national defense policy, despite not having a formal national security strategy. The country understands that cyber defense is vital to ensure the continuity of operations of national organizations and has a tendency to centralize cyber security, despite the absence of an official policy of cooperation between cyber institutions. Finally, it is concluded that cybernetic power in Israel is anchored in a broad ecosystem of industrial, scientific and specialized personnel capacities, as well as in the existence of specialized units, civil and military, and of a specific doctrine of use of the cybernetic power to sustain state power.

Keywords: Israel. Cyber Power. Cyber Capabilities. Military Doctrine.

LISTA DE TABELAS

Tabela 1 - Funções da NCSA de acordo com as três camadas 44

LISTA DE FIGURAS

Figura 1 - Estrutura Geral da Organização Cibernética em Israel 27
Figura 2 - Liderança Estratégica e Operacional das Instituições Cibernéticas em Israel 28
Figura 3 - Organização das instituições cibernéticas israelenses e suas funções 29
Figura 4 - As três camadas conceito de operações para a segurança cibernética israelense 41
Figura 5 - Interconexão entre regulação do mercado de cibersegurança e orientação para o setor privado 42
Figura 6 - Campanhas contra atacantes e campanhas defensivas nacionais..... 43
Figura 7 - Cronograma geral dos documentos governamentais relacionados ao ciber 46
Figura 8 - Ecossistema nacional de inovação se origina da grande estratégia 67
Figura 9 - Gastos internos brutos em P&D de Israel, Coreia, Estados Unidos e OCDE 69
Figura 10 - Comparação internacional do percentual em relação ao total de trabalhadores ativos, formado pelos funcionários no setor de alta tecnologia..... 75
Figura 11 - Dados sobre ciência, tecnologia e comunicações em Israel 80
Figura 12 - Gama de exportação de serviços israelenses em 2019 81
Figura 13 - Programas técnicos de segurança cibernética nas melhores universidades..... 83
Figura 14 - Visão geral do desempenho de Israel em poder cibernético..... 85
Figura 15 - Comparação dos 10 principais poderes cibernéticos em 2020 e 2022 91
Figura 16 - Índice nacional de poder cibernético: classificação geral 1-30 92
Figura 17 - Volume semanal de ransomware de 2021 (jul-dez) a 2022 (jan-jun) 94
Figura 18 - Distribuição geográfica de envios relacionados a ransomware..... 96
Figura 19 - Poder cibernético potencial e os fatores domésticos e internacionais 104

LISTA DE ABREVIATURAS E SIGLAS

AAA	Autentificação, autorização e auditoria
BERD	Despesas de Negócios em Pesquisa e Desenvolvimento
CERT-IL	*Israeli Cyber Event Readiness Team*
CIA	*Central Intelligence Agency*
CIP	*Critical infrastructure protection*
CNA	Ataque à rede de computadores
CND	Defesa de Rede de Computadores
CONOP	Conceito de operações
DDoS	*Distributed Denial Service*
DoS	Negação de serviço
EEI	Elementos Essenciais e Informação
FAI	*Forças Aéreas Israelenses*
FDI	Forças de Defesa Israelenses
FPT	*File Transfer Protocol*
IA	Inteligência Artificial
IABs	*Initial Access Brokers*
ICT	Tecnologias de Informação e Comunicação
IDS	*Intrusion Detection System*
INC	Infraestrutura Nacional Crítica
INCB	*Israeli National Cyber Bureau*
INCD	*Israeli National Cyber Directorate*
IPS	*Intrusion Prevention System*
ISA	*Israeli Security Agency*
ISNU	*Israeli SIGINT National Unit*

MNCs	Multinacionais de TI de Alta Tecnologia
NASDAQ	*National Association of Securities Dealers Automatic Quotation System*
NCSA	*National Cyber Security Authority*
NISA	*National Information Security Authority*
P&D	Pesquisa e Desenvolvimento
POP	*Post Office Protocol*
PRE	Planejamento de Recursos Empresariais
Q-MED	*Mediterranean Consortium Quantum*
QME	Vantagem Militar Qualitativa
RaaS	*ransomware-as-a-service*
RMA	*Revolution in Military Affairs*
SCP	*Secure Copy Protocol*
SQL	*Structured Query Language*
TI	Tecnologia da Informação
TTC	Empresas de Transferência de Tecnologia
TTPs	Táticas, Técnicas e Procedimentos
XMPP	*Extensible Messaging and Presence Protocol*

SUMÁRIO

1 INTRODUÇÃO 11
2 GOVERNANÇA 15
3 ESTRATÉGIA 30
4 DOUTRINA 49
5 CONTEXTO 67
6 CAPACIDADES 88
7 CONCLUSÃO 110
REFERÊNCIAS 112

1 INTRODUÇÃO

A doutrina de defesa nacional israelense assume como premissa que o conflito com as populações árabes dos países vizinhos, e com os palestinos em particular, não pode ser resolvido por meios exclusivamente militares. Ao mesmo tempo, a persistência da ocupação e dos conflitos torna cada vez mais difícil uma solução política. O Estado israelense, assume como premissa, a partir de sua história militar, que o desequilíbrio quantitativo poderia selar seu destino. A aceitação desta circunstância marcou a segurança como requisito essencial da existência de Israel (TAL, 2000, p. 39-40; FREILICH, 2018b, p. 22).

Com o fito de alcançar a vantagem qualitativa para compensar a inferioridade quantitativa, Israel buscou e preservou esta vantagem, a qual se tornou seu motivo estratégico fundamental. Além de se apoiar na tecnologia, Israel também enfatizou as qualidades pessoais e educacionais, concomitante à estratégia operacional criativa, de seus soldados e de sua população. Em geral, Israel frequentemente recorria e recorre, na tecnologia avançada, uma "solução rápida" que minimizaria os custos, a duração e as fatalidades da guerra (ADAMSKY, 2010, p. 113-114).

Destarte, as Forças de Defesa Israelenses (FDI) sempre buscaram estar à frente tecnologicamente de seus inimigos, a partir de 1967 que as FDI passaram a enxergar as soluções tecnológicas como uma solução nos assuntos relacionados à segurança. Desse modo, a preferência israelense por empregar meios militares ao lidar com problemas de segurança nacional foi cada vez mais acompanhada por um reflexo condicionado de buscar soluções pelo ângulo da tecnologia. A preocupação com a segurança e uma obsessão com a sobrevivência fundamentam o *ethos* da estratégia israelense. Em circunstâncias assim, o processo rápido de tomada de decisão e um pensamento cotidiano, de curto prazo e *ad hoc*, prejudicaram a formulação de um pensamento estratégico abrangente de longo prazo. Dessa maneira, improvisações militares rápidas impulsionadas pelo pensamento tático se tornaram um traço cultural da estratégia israelense (ADAMSKY, 2010, p. 114-116).

A alavancagem do uso da tecnologia cibernética em missões tomou forma no governo israelense em meados de 1990. Com o apoio dos líderes de defesa, os esforços de segurança cibernética implicaram, em 2002, uma das primeiras iniciativas políticas focadas na proteção da infraestrutura crítica. Já em 2010 a Iniciativa Cibernética Nacional foi posta em prática. A indústria de defesa sofisticada e inovadora foi estabelecida, portanto, a partir de uma mentalidade que busca, a todo custo, a segurança absoluta, o que permitiu a Israel desenvolver um

arsenal tecnológico e capacidades novas, tal como a cibernética. Essa metamorfose na interpretação da vantagem qualitativa em favor da crescente dependência da tecnologia fez com que o país desenvolvesse um ecossistema capaz de fornecer um capital humano importante e de alto grau de qualidade (ADAMSKY, 2010, p. 72-73).

Este ecossistema, fruto da tríade entre governo, indústria e academia, é composto por *startups* israelenses, empresas globais, academia e centros de segurança cibernética civis e militares e possui base nas idiossincrasias culturais, cria o cenário propício ao desenvolvimento de capital humano qualificado e inovador, bem como a ciência e a tecnologia de ponta (TABANSKY; ISRAEL, 2015, p. 15-18; ADAMSKY, 2010, p. 125-126). A crescente colaboração da tríade foi tida como a melhor abordagem com o fito de melhorar a segurança cibernética nacional e, por conseguinte, conquistar o objetivo estratégico de tornar o Estado israelense em uma das maiores potências cibernéticas globais. Este processo incluiu esforços organizacionais e legislativos ao decorrer dos anos. Aqui, o contexto histórico e o processo político chamam a atenção para um novo foco: os aspectos não técnicos na segurança cibernética (ADAMSKY, 2010, p. 72-73).

O presente trabalho avalia Israel do ponto de vista do poder cibernético e, sobretudo, constata que o país detém capacidades cibernéticas ofensivas e defensivas. Desse modo, visa-se responder como Israel conseguiu se transformar em uma das maiores potências cibernéticas atuais. Para tanto, pretende-se utilizar o contexto histórico e aspectos sociais com o fito de compreender melhor a grande estratégia israelense e, por consequência, o ecossistema existente que se relaciona e sustenta o poder cibernético em Israel. Salvo indicação em contrário, não foram empregadas as siglas e os termos técnicos na língua oficial de Israel, nem utilizada a transliteração do hebraico. Neste trabalho, foi priorizada apenas a tradução para o inglês e, quando necessário, a livre tradução para o português.

No capítulo dois (governança), os aspectos da governança, comando e controle de Israel. Para tanto, apresentar-se-á um resumo do contexto histórico e da progressão das instituições israelenses responsáveis por construir, utilizar e desenvolver o poder cibernético no país. Desse modo, abordar-se-á os primeiros e os atuais esforços da política nacional de segurança cibernética; a criação, o desenvolvimento e a atualidade das instituições governamentais, bem como as suas funções; e como o contexto histórico influencia, atualmente, a capacidade cibernética israelense. Por fim, demonstrar-se-á a estrutura geral da organização de segurança cibernética.

No capítulo três (estratégia), demonstrar-se-á, a partir de documentos oficiais, a estratégia cibernética israelense. Para tanto, foi necessário abordar o contexto histórico para entender

a doutrina atual, tendo em vista que Israel possui uma estrita política de não publicar documentos relacionados a esta temática. Aliás, o país nunca realmente materializou sua doutrina em documentos oficiais, possuindo uma abordagem muito mais cultural. Tal é a importância do contexto histórico e do resgate dos princípios doutrinários de Ben Gurion. Desse modo, abordar-se-á, cronologicamente, os documentos relevantes para a criação e o desenvolvimento das capacidades cibernéticas israelenses, apresentando suas características e implicações.

No capítulo quatro (doutrina), tratar-se-á do conceito de doutrina militar e de grande estratégia, as quais serão entendidas a partir dos termos utilizados por Posen (1984). Consoante a isto, abordar-se-á como tanto o contexto histórico quanto os traços culturais convergiram a fim de moldar a doutrina israelense e garantir a sobrevivência do Estado que, inicialmente, sofria uma desvantagem quantitativa amedrontadora. Desse modo, apresentar-se-á alguns pilares da doutrina militar israelenses, bem como a evolução e alteração dos que são considerados inimigos do Estado israelense. Por fim, identificar-se-á três teorias, demonstradas por Sagan (2000), que focam em diferentes explicações plausíveis para a escolha de doutrinas militares específicas. Neste capítulo, portanto, a interpretação possui, como ponto de partida, uma visão culturalista da explicação dos fundamentos da estratégia do poder cibernético em Israel, mas procura-se demonstrar como o fundo cultural perpassa pelas características operacionais, econômicas e de governança.

Demonstrar-se-á, no capítulo cinco (contexto), o contexto tecnológico existente em Israel e como este se relaciona com o ecossistema nacional de inovação. Visa-se, portanto, confirmar a relação entre a grande estratégia israelense e seu ecossistema e como ambos são importantes no que se refere ao entendimento do poder cibernético em Israel. Assim sendo, apresentar-se-á dados sobre o sistema de P&D no país, bem como programas governamentais que incentivam a aprendizagem tecnológica e cibernética, além de como o serviço militar realiza um papel crucial na formação deste capital humano. Ademais, evidenciar-se-á a relação intrínseca entre governo e instituições privadas no desenvolvimento deste poder, bem como a relação com a educação nacional e seus respectivos projetos. Por fim, apresentar-se-á a classificação geral de Israel de acordo com critérios utilizados para medir sua capacidade cibernética.

Por fim, no capítulo seis (capacidades), tratar-se-á das capacidades ofensivas e defensivas de Israel no âmbito cibernético. Inicialmente, abordar-se-á o contexto atual de países a partir de estudos realizados por instituições, estabelecendo um diagnóstico sobre o desenvolvimento no âmbito mundial destas capacidades. Em seguida, expor-se-á quais são os ataques cibernéticos mais comuns dentre os países, como se dão e quais são suas consequências. Ademais, tratar-

se-á das definições de ataque e defesa cibernéticas, seus procedimentos e exemplos envolvendo Israel. Por fim, utilizar-se-á a definição utilizada por Bebber (2017) sobre o poder cibernético potencial e os fatores domésticos e internacionais, Israel detém as capacidades ofensivas e defensivas. Vale salientar que este capítulo é o menos desenvolvido, justamente por conta do desenvolvimento teórico incipiente da literatura. Apesar da falta do conhecimento técnico do tema, faz-se importante situar a discussão tão necessária sobre as capacidades cibernéticas.

2 GOVERNANÇA

O capítulo visa a apresentar os aspectos da governança, comando e controle de Israel. Para tanto, apresentar-se-á um resumo do contexto histórico e da progressão das instituições israelenses responsáveis por construir, utilizar e desenvolver o poder cibernético no país. Desse modo, abordar-se-á os primeiros e os atuais esforços da política nacional de segurança cibernética; a criação, o desenvolvimento e a atualidade das instituições governamentais, bem como as suas funções; e como o contexto histórico influencia, atualmente, a capacidade cibernética israelense. Por fim, demonstrar-se-á a estrutura geral da organização de segurança cibernética.

Em Israel, os envolvidos com tecnologia cibernética nos órgãos competentes dentro da comunidade de defesa compreenderam, desde cedo, que a inserção de sistemas de computadores oferece vantagens consideráveis. Tanto as FDI quanto os serviços de inteligência israelenses impulsionaram os desenvolvimentos tecnológicos em direções que abarcam questões relacionadas à criptografia e à segurança da informação. Apesar das oportunidades existentes da computação, também existem riscos. Em meados da década de 1990[1], ficou claro, para alguns líderes de defesa, a importância do ciberespaço quanto ao funcionamento da sociedade (TABANSKY; ISRAEL, 2015, p. 31; ADAMSKY, 2010, p. 98-99).

Além disso, nesta mesma década, três elementos importantes foram introduzidos ao mesmo tempo na atividade militar israelense: um conceito de arte operacional, uma metodologia única para a análise de operações militares e o reconhecimento da *Revolution in Military Affairs* (RMA), os quais tornaram-se organicamente interconectados. Isto é, ao utilizar uma nova metodologia, as FDI embarcaram na inovação organizacional e conceitual de RMA e a tratou como desenvolvimento da versão israelense de arte da guerra. Com isso, as tentativas de envolver o setor civil foram a principal fonte para as primeiras iniciativas de política civil, de modo que mudanças extremas se manifestaram para além do campo de batalha (TABANSKY; ISRAEL, 2015, p. 31; ADAMSKY, 2010, p. 98-99).

No ano de 1995, o governo israelense decidiu estabelecer um departamento específico com o fito de proteger "informações confidenciais." Entretanto, o governo não implementou a resolução em sua totalidade, criando o departamento apenas em 1999. Posteriormente, um conselho consultivo para sistemas informatizados e revisão de segurança da informação foram estipulados para debater metodicamente questões relevantes. Em conjunto com o conselho, várias

[1]Alguns acontecimentos provocaram esta percepção: a ascensão da internet e seu papel central nas comunicações e o computador da IBM Deep Blue que acabou derrotando o então campeão mundial de xadrez, Garry Kasparov, sendo uma grande demonstração de inteligência artificial que provocou altas expectativas em TI.

unidades de tecnologia da informação (TI) implementaram as recomendações separadamente. Ademais, os empreendimentos para integrar a TI do governo em um único órgão obtiveram sucesso parcial em áreas restritas (TABANSKY; ISRAEL, 2015, p. 32).

Em 1997, foi criada a unidade Tehila (Infraestrutura do Governo para a Era da Internet) com o fito de fornecer, às agências institucionais, serviços básicos para uma infraestrutura de TI segura e unificada para todo o governo. Os serviços incluem: acesso seguro à internet para serviços governamentais; hospedagem segura de sites governamentais e serviços de governo eletrônico; e infraestrutura segura para dar suporte aos projetos governamentais futuros (TABANSKY; ISRAEL, 2015, p. 33).

À época, a unidade Tehila esteve vinculada à identificação digital de *smartcard*, formulários eletrônicos, serviço de pagamento eletrônico para taxas e impostos; *software* de gerenciamento unificado de planejamento de recursos empresariais (PRE) da *Merkava*[2]; banco de dados biométrico para carteiras de identidade digitais de cidadãos, portais da *Web*, dentre outros. Além disso, atuou como provedora de serviços de aplicativos e apoiou na implementação da Lei de Liberdade de Informação[3] (TABANSKY; ISRAEL, 2015, p. 33).

Em geral, a segurança de TI foi um elemento essencial do trabalho da unidade desde o início. Inicialmente, era apenas voltada para expandir os serviços e a conectividade. Mais recentemente, houve um aumento do número e da sofisticação das tentativas de invasão, bem como a frequência e o volume de ataques *Distributed Denial Service* (DDoS)[4]. Com isso, a demanda dos cidadãos por serviços eletrônicos seguros e que preservam a privacidade também aumentou. Desde a Operação Cast Lead[5], de 2008, a infraestrutura governamental de Tehila resistiu repetidamente a ataques DDoS, tendo sido capaz de evitar graves perturbações imediatas e implicações a longo prazo. Todavia, tanto os esforços do governo quanto a segurança de

[2]Sistema de informação integrador, capaz de consolidar a gestão de todos os processos de trabalho e recursos de forma a melhorar os processos de trabalho (ISRAEL, 2006, p. 67).

[3]Esta lei de 1998 estipula que "todo cidadão ou residente israelense tem o direito de receber informações de uma autoridade pública." A lei garante o direito de receber do *National Insurance of Israel* (NII) informações sobre as atividades do escritório com relação aos assuntos sob sua responsabilidade, como informações sobre benefícios e cobrança, políticas administrativas e procedimentos operacionais, estatísticas, sobre filiais todo o país e serviços prestados ao público, consulta de documentos, dentre outros (ISRAEL, 2022b).

[4]*Distributed Denial Service:* ataque cibernético em que *hackers* forçam os dispositivos conectados à internet a enviar solicitações a um serviço ou site específico, geralmente infectados com *malware*, com a intenção de sobrecarregá-los com tráfego ou solicitações falsas. Este tipo de ataque previne que usuários não possam criar uma conexão entre o sistema e o servidor (ALWAREBYTES, 2022).

[5]De acordo com as IDF, a Operação Cast Lead tinha por objetivo atacar infraestruturas, usadas para atividades terroristas e disparos de foguetes da Faixa de Gaza contra civis israelenses. Esta operação ficou conhecida pelos mais de 1.300 palestinos mortos e pelo relatório Goldstone (Missão das Nações Unidas para apuração de fatos sobre o conflito em Gaza). Este relatório concluiu que há evidências indicando que graves violações dos direitos humanos internacionais e do direito humanitário foram cometidas por Israel durante o conflito de Gaza, e que Israel cometeu ações equivalentes a crimes de guerra e possivelmente crimes contra a humanidade (ISRAEL, 2017a; ONU, 2009).

TI nunca conseguiram alcançar o objetivo desejado, justamente porque as diversas agências do governo não estavam em conformidade devido às circunstâncias legais, orçamentárias e políticas complexas (TABANSKY; ISRAEL, 2015, p. 33).

Em suma, os primeiros esforços da política nacional de segurança cibernética foram consequência do progressivo reconhecimento pelos líderes de defesa. De 1995 a 2002, as agências governamentais realizaram atividades em áreas associadas, em vez de esforços coerentes e coletivos de segurança cibernética, isso porque a maioria das agências foi capaz de satisfazer suas necessidades independentemente do serviço da unidade Tehila. Nesse sentido, a materialização dessas políticas levou um longo tempo por três grandes causas: a introdução ainda recente das TIs; a relutância de muitos interessados em serem proativos; e a competição com outros tópicos urgentes dentro do sistema do governo israelense. Destarte, por um lado o foco israelense em ciência e tecnologia suscitou a disponibilidade de capacidades técnicas e o aumento da conscientização, por outro a eficiência e a segurança de TI estavam longe de ser exemplares na época (TABANSKY; ISRAEL, 2015, p. 34).

Em 2010, o então Primeiro-Ministro, Benjamin Netanyahu, determinou a formação de uma estratégia nacional (Iniciativa Cibernética Nacional) com o fito de posicionar o país entre os principais países líderes no ramo de segurança cibernética, bem como ser líder em inovação tecnológica e parceiro nos processos globais de formação do espaço cibernético. Netanyahu, então, ordenou a formação de uma equipe a fim de formular tal estratégia. A principal recomendação proposta pela equipe foi a necessidade de uma nova organização governamental de cibersegurança que fosse capaz de coordenar todos os esforços políticos com o fito de promover a capacidade nacional no espaço cibernético e capacitar o país para lidar com as ameaças cibernéticas (IISS, 2021, p. 70; CCDCOE, 2017).

No mesmo ano, líderes políticos israelenses concluíram que o *Shin Bet* não continuaria a ser a principal autoridade responsável por proteger os sistemas de informação. Havia, portanto, necessidade de uma solução mais focada para coordenar as atividades nacionais de defesa cibernética. Destarte, em 2011, foi criado o *Israeli National Cyber Bureau* (INCB), para consolidar a segurança cibernética civil em nível nacional, a qual destinava-se a proteger infraestruturas nacionais críticas contra os ataques cibernéticos provenientes de outros países ou grupos terroristas, a partir de uma orientação voltada para a política (IISS, 2021, p. 70; CSS, 2020, p. 7). Sob a supervisão do Primeiro-Ministro, o INCB servia como um órgão consultivo sobre a política nacional de segurança cibernética e a promoção de sua implementação em todo o governo (CCDCOE, 2017, p. 12).

A partir de então, o governo de Israel percebeu a necessidade de uma autoridade separada para lidar com a segurança cibernética e, em 2016, foi criada a *National Cyber Security Authority* (NCSA). A partir de uma orientação operacional, a NCSA tinha como objetivo defender o ciberespaço conduzindo, operando e implementando todos os esforços defensivos operacionais no ciberespaço. De modo geral, foi criada para fornecer uma resposta defensiva completa e contínua aos ataques cibernéticos, bem como lidar com ameaças e incidentes cibernéticos em tempo real. Ademais, possuía a responsabilidade de manter o CERT[6] do país, aumentar sua organização e resiliência, desenvolver uma doutrina cibernética nacional e promulgar uma lei de segurança cibernética adequada (CCDCOE, 2017, p. 12). A NCSA foi, posteriormente, fundida com o INCB, tornando-se a *Israeli National Cyber Directorate* (INCD).

Percebe-se, então, que a infraestrutura crítica foi, inicialmente, a principal motivação das primeiras medidas de segurança cibernética civil israelense. No começo, ao invés dos esforços serem coordenados, estes eram focados em soluções baseadas no curto prazo, no pragmatismo *ad hoc*, o que resultou em um sistema parcialmente descentralizado. Para tanto, a *National Information Security Authority* (NISA), estabelecida em 2002, dentro do *Shin Bet*, permaneceu responsável por instruir, orientar e coordenar as atividades entre as instituições públicas e as empresas privadas tidas como críticas para a segurança cibernética de Israel. Atualmente supervisiona a implementação de várias políticas de segurança da informação e de proteção da informação. Como parte da proteção de infraestrutura crítica, a NISA é incumbida de preparar objetivos de segurança cibernética, desenvolver um plano para sua implementação e supervisionar sua implementação. Ela está sob o comando do Comitê Diretor, composto por órgãos regulamentadores, tais como ministérios governamentais, bancos, indústrias, empresas, dentre outros (CCDCOE, 2017, p. 13).

Assim, no que tange à capacidade central de inteligência cibernética, Israel possui três agências principais: *Military Intelligence Directorate (Aman)*, encarregado da maioria das questões de inteligência aérea, naval, terrestre e de sinais; *Institute for Intelligence and Special Operations (Mossad)*, responsável pelas atividades de inteligência estrangeira; e, por fim, *Israeli Security Agency (Shin Bet)*, a qual administra das operações de inteligência interna, incluindo aquelas nos territórios ocupados por Israel (IISS, 2021, p. 71).

O *Aman* é uma das diretorias mais antigas dentro das FDI, estabelecida logo que o Estado de Israel foi declarado. Sua missão primordial remete ao fornecimento de avisos e alertas

[6]*The Israeli Cyber Event Readiness Team* (CERT-IL) gerencia nacionalmente incidentes de segurança cibernética, compartilha inteligência com parceiros nacionais e internacionais, buscando desenvolver as melhores práticas de segurança cibernética e conscientizar sobre segurança cibernética (CCDCOE, 2017, p. 13).

diários de inteligência durante os períodos de paz e de guerra, tanto ao governo quanto às FDI, com o fito de proteger o Estado. Para tanto, o corpo de inteligência deve utilizar artifícios e acompanhar as atividades e o surgimento de "terroristas", além dos avanços tecnológicos ao redor do mundo. Assim, os soldados do Corpo de Inteligência recebem e processam informações de inteligência provenientes de fontes para criar uma avaliação atualizada de uma determinada situação. Tal ação requer, sobretudo, a elaboração de sistemas e ferramentas novas para o rastreamento de inteligência, de modo que os soldados possam transmitir e atualizar as informações em tempo real (ISRAEL, 2021c).

Além disso, o Corpo de Inteligência possui uma unidade de elite, a *Sayeret Matkal*, considerada como a melhor unidade de combate das FDI e uma das melhores unidades de forças especiais do mundo. Apesar de ser especializada em operações de comando e reconhecimento, tais como navegação, orientação, utilização de uma ampla gama de veículos, esta unidade não faz parte de nenhum comando regional, respondendo apenas às ordens do Chefe do Estado-Maior (ISRAEL, 2021c).

Dentre algumas outras funções da *Aman*, estão: identificar, selecionar e sintetizar informações escutadas em árabe (*listening*); traduzir informações de relatórios (*translation of information*); interpretar informações aéreas e transformá-las em mapas por meio da decriptação de imagens (*decryption of aerial images*); e, por fim, o estabelecimento de sistemas de verificação, produção de cartões eletrônicos, construção de terminais de computadores seguros (*electronics technician*) (ISRAEL, 2021c).

Dentro do *Aman*, há três principais unidades: a Unidade 8200, a Unidade 9900 e a Unidade 504. A primeira, sendo a maior unidade, trabalha com a coleta de informações do *Aman*, analisando, processando e compartilhando-as com oficiais relevantes. Ao atuar em tempos de paz e guerra e em todos os setores, a Unidade 8200 possibilita um maior e mais rápido fluxo de informações fundamentais aos quartéis-generais envolvidos no combate. Esta unidade será melhor explicada doravante (ISRAEL, 2021c).

Em relação ao *Mossad*, seu estabelecimento se deu logo após a declaração do Estado israelense, realizado a partir da percepção da necessidade de se estabelecer estruturas nacionais para os órgãos de inteligência que operavam durante o período pré-Estado. A partir disso, instituiu-se, em 1948, o serviço de informação militar chefiado pelo Quartel General, responsável pela segurança, censura e contra-inteligência. Inicialmente, diversas medidas intra e interorganizacionais com os demais órgãos de inteligência do Estado estavam em processo de formação. Estas medidas incluíam o estabelecimento do Comitê Supremo de Coordenação Inter-Serviços

em abril de 1949. Este comitê incluía o *Shin Bet*, que estava sendo formulado a partir do *Shai* (serviço de informação do *Haganah*[7]), do Departamento de Estado, do departamento de inteligência militar e da Polícia de Israel. Este serviço externo de informação estatal tornaria-se, posteriormente, o *Mossad* (ISRAEL, 2022a).

Em 1949, foi proposta a criação de um Instituto Central (*Mossad*), para a Coordenação dos Serviços de Inteligência e Segurança, com o objetivo de obter maior coordenação e direcionamento da atividade de inteligência. Após a proposta ter sido aprovada por Ben Gurion, o órgão foi estabelecido no mesmo ano. O Instituto de Coordenação controlava o Departamento de Estado e deveria coordenar a atividade dos outros dois órgãos: o *Shin Bet* e o departamento de inteligência da divisão de operações das FDI. Outrossim, a data de 1949 foi definida como a data de criação do *Mossad*, que mais tarde se tornou o Instituto de Inteligência e Operações Especiais (ISRAEL, 2022a).

Desde a sua criação, o *Mossad* está envolvido na coleta de inteligência com base nas necessidades do Estado, sendo então verificadas e elaboradas periodicamente por meio de um sistema conhecido como Elementos Essenciais e Informação (EEI). O EEI possui várias maneiras de ser utilizado, entre elas há a HUMINT[8] e a SIGINT[9]. Além disso, *Mossad* atua como ponte para estabelecer relações secretas com países que evitam contato aberto com Israel, além de dar assistência aos líderes do Estado em negociações encobertas, tais como as que antecederam os acordos de paz com Egito e Jordânia. Outrossim, possui um papel essencial no "combate ao terror" contra judeus e israelenses que residem no exterior, além de atuar na prevenção de países, que são considerados como ameaça a Israel, a obterem armas não convencionais (ISRAEL, 2022a).

A *Israeli Security Agency (ISA), Shin Bet* ou *Shabak*, por sua vez, é uma organização estatal encarregada por resguardar a segurança do Estado de Israel. Apesar de existir desde 1949, junto às organizações que viriam a ser o *Aman* e o *Mossad*, o *Shin Bet* não foi revelado até 1957. Dentre as suas obrigações, estão o combate à espionagem estrangeira, o combate à subversão política doméstica e a responsabilidade pela segurança de instituições vitais dentro do país e em embaixadas no exterior (ISRAEL, 2020c).

---

[7]Representa o embrião do exército israelense, sendo responsável pela organização militar e defesa da comunidade judaica na Palestina até a fundação do Estado (CONIB, 2022).

[8]HUMINT *(human intelligence):* termo eufemista, incorporado ao jargão internacional, que remete à espionagem, mas também à inteligência advinda de fontes humanas (CEPIK, 2003, p. 36-37).

[9]SIGINT *(signals intelligence):* originário de interpretações, decodificação, tradução e análise de mensagens por terceiros, remete à criptografia e criptologia. Há duas disciplinas complementares: COMINT (*communications intelligence;* interceptação, processamento e pré-análise de transmissões) e ELINT (*electronics intelligence;* interceptação, processamento e pré-análise de sinais eletromagnéticos não-comunicacionais) (CEPIK, 2003, p. 40-41).

Outrossim, nos anos de 1950 e 1960, a principal atribuição do *Shin Bet* era ajudar a administração militar, combater o terrorismo e a subversão política entre os judeus israelenses e combater a espionagem estrangeira. A partir dos anos 1970, estabeleceu-se um aparato de segurança mundial para proteger alvos israelenses de ameaças terroristas. Já nas décadas de 1980 e 1990, suas atividades foram caracterizadas principalmente pelo combate à atividade terrorista. Ademais, apesar dos ataques terroristas sofridos e ao assassinato do então Primeiro-Ministro, Yitzhak Rabin, o *Shin Bet* passou a aplicar e dar grande ênfase ao aprendizado constante (*debriefings*, autoavaliação intransigente e a implementação de conclusões) (ISRAEL, 2020c).

Em 2002, a organização teve o seu estatuto aprovado, de modo a conceder ao Primeiro-Ministro o poder de estabelecer regimentos nos campos regulados pela lei *2002 ISA Statute* e a estabelecer quatro aspectos centrais: o aspecto institucional (estabelecimento das suas competências e a sua subordinação ao governo); as suas funções, ou seja, missão, funções, poderes gerais que lhe são conferidos (incluindo a autoridade para conduzir interrogatórios) e poderes específicos concedidos (realizar buscas, receber dados de comunicações, realizar verificações de segurança, dentre outros); controle e supervisão, como o *status* do controlador interno, a exigência de que relatórios periódicos sejam fornecidos ao *Knesset* (parlamento israelense), tanto ao governo quanto ao Procurador-Geral, a exigência de aprovação externa de portarias, regras e instruções legais e o estabelecimento de uma entidade de recurso externa para verificações de segurança; e, por fim, seus aspectos únicos, sendo o *status* dos relatórios internos, exceções relativas à responsabilidade dos funcionários e seus procuradores, restrições aos funcionários durante e após seu período de emprego e instruções sobre confidencialidade (ISRAEL, 2020c).

Sendo assim, o *Shin Bet* é uma organização líder em inteligência e tecnologia, criando e desenvolvendo várias soluções operacionais no âmbito cibernético, *big data* e *mobile*. Este tipo de tecnologia possibilita que ferramentas sejam criadas e utilizadas para interromper ameaças de terror e espionagem. Dentro da organização, cerca de um quarto dos funcionários são orientados tecnologicamente. Aliás, a divisão de Tecnologia de Sistemas de Informação é responsável pelo desenvolvimento de sistemas inovadores e infraestruturas na área de inteligência/tecnologia operacional, de modo que os mesmos são integrados às atividades principais da organização e ajudam a cumprir suas tarefas e missões (ISRAEL, 2020a).

Esta divisão, no caso, atua no desenvolvimento de inovações em áreas como visão computacional, reconhecimento de fala, mineração de dados e processamento de linguagem, utilizando a tecnologia mais avançada atualmente disponível no mercado: SDx, virtualização, automação, dentre outros. Recursos baseados em aprendizado de máquina e algoritmos de redes neurais desenvolvidos na divisão permitem uma identificação melhor e auxiliam a lidar com a crescente variedade, quantidade e ritmo de entrada de informações (ISRAEL, 2020a).

Para tanto, é necessário uma conexão com o trabalho de campo, para que os funcionários entendam os requisitos tecnológicos à medida que surgem e oferecem soluções. Isto permite a produção de sistemas em curto prazo e soluções únicas. Os sistemas e infraestruturas desenvolvidos pela divisão são equipamentos cruciais no esforço do *Shin Bet* para obter informações em tempo real e interromper antecipadamente qualquer incidente (ISRAEL, 2020a).

No que tange à divisão de Tecnologia e Ciber, a mesma é encarregada por iniciar, desenvolver e produzir ferramentas tecnológicas avançadas para coleta de inteligência, com o fito de combater o terrorismo, espionagem e subversão doméstica contra Israel e seus interesses. Nesse sentido, para que esses objetivos sejam alcançados, a divisão une inteligência com tecnologia. Isto implica o *Shin Bet* investir fundos substanciais no desenvolvimento autônomo de capacidades tecnológicas inovadoras, enquanto se dedica concomitantemente em projetos de desenvolvimento e infraestrutura em larga escala com empresas líderes na indústria tecnológica, em Israel e no mundo (ISRAEL, 2020b).

O desenvolvimento de sistemas avançados pela divisão de Tecnologia e Ciber é possibilitado por uma combinação de conhecimento profissional em várias áreas, incluindo: (a) engenharia reversa; (b) pesquisa de vulnerabilidade; (c) desenvolvimento avançado no núcleo de sistemas operacionais em ambientes móveis, computadores e ambientes incorporados; (d) análise de comunicações; (e) codificação; (f) capacidades de engenharia de sistemas; (g) capacidades de RF *(radio frequency)* e profundo conhecimento na área de antenas para todas as frequências; (h) processamento de sinal; (i) processamento de vídeo; (j) processamento e análise em tempo real; e (k) altas capacidades mecânicas na área de maquinação (ISRAEL, 2020b).

Não obstante, o governo israelense vem realizando esforços significativos com o objetivo de unificar as diferentes agências civis de segurança cibernéticas existentes em uma única entidade: o INCD. Isto demonstra a clara tendência à centralização da segurança cibernética (CSS, 2020, p. 7). Portanto, *Mossad* e *Shin Bet* integram o âmbito cibernético israelense para fortalecer a segurança doméstica, envolvendo-se em processos de compartilhamento de informações com órgãos governamentais, ainda que separados do INCD, justamente por conta de seu mandato como serviços de inteligência (CSS, 2020, p. 7 e 15).

O INCD, portanto, é a agência nacional de segurança e tecnologia encarregada por defender o ciberespaço nacional e por estabelecer e avançar o poder cibernético de Israel. Ao atuar no nível nacional para reforçar regularmente o nível de defesa das organizações e dos cidadãos, previne e lida com ataques cibernéticos, reforçando as capacidades de resposta às emergências. Dentre as suas funções, estão a promoção de soluções cibernéticas inovadoras e soluções tecnológicas direcionadas ao futuro, formulação de estratégias e políticas nos âmbitos nacional e internacional, bem como o desenvolvimento da mão de obra cibernética. O INCD trabalha com o fito de manter um ciberespaço protegido e facilitar o crescimento e a base de poder de Israel (ISRAEL, 2020d).

Em geral, os objetivos do INCD são: planejamento estratégico de políticas a fim de melhorar a força cibernética contra riscos, apoiando infraestruturas críticas e impondo regulamentações; implementação e regulamentação a nível nacional da estratégia cibernética nacional (i.e. melhorar a robustez, a resiliência e a defesa, incluindo CERT-IL e CIP[10]); desenhar e formular estratégia e política cibernética nacional em Israel, bem como internacionalmente; facilitar a cooperação internacional, bem como a formulação de um marco legal para atividades cibernéticas (doméstica e internacional); estabelecer e reforçar a base cibernética de ciência e tecnologia ao desenvolver capital humano de alta qualidade; preparar e permitir que o setor privado israelense e o público em geral se protejam de ameaças cibernéticas; gerir integralmente as campanhas de defesa nacional (em tempos de paz); melhorar a resiliência em colaboração com a Polícia de Israel e o Ministério da Justiça; apoiar *Shin Bet*, IDF, *Mossad*, Polícia de Israel e Ministério da Justiça no fortalecimento da defesa cibernética civil (CSS, 2020, p. 14; ISRAEL, 2020d).

O INCD fornece serviços de tratamento de incidentes e orientação para empresas do setor civil, tanto empresas privadas quanto gestores de infraestrutura críticas nacionais. Há, aliás, o sistema denominado de *Showcase*, implementado em 2019, o qual conecta estas empresas ao INCD, permitindo que acessem em tempo real o nível de risco cibernético a que estão expostas. Isto permite que o INCD incorpore capacidades e conhecimento dos envolvidos e desenvolva medidas para classificar os riscos cibernéticos a serem enfrentados (IISS, 2021, p. 73).

[10]CIP *(critical infrastructure protection)* se refere às ações realizadas para proteger infraestruturas críticas, tais como pessoas, entidades físicas e sistemas cibernéticos indispensáveis para a segurança pública, nacional e estabilidade econômica. Os métodos utilizados pela CIP detêm ou mitigam ataques realizados por hackers, terroristas, eventos naturais (furacões ou inundações) ou por acidentes de materiais perigosos envolvendo substâncias nucleares, biológicas ou químicas (USA, 2001).

Para tanto, a agência divulga, periodicamente, diretrizes e recomendações para empresas e cidadãos se protegerem dos riscos cibernéticos. Ademais, ela possui a Equipe de Resposta a Emergências Cibernéticas, a qual mantém um mecanismo de comunicação 24 horas entre o INCD e as empresas privadas e governamentais (IISS, 2021, p. 73). Outrossim, tanto os poderes regulatórios quanto a base legal para as atividades do INCD foram estabelecidos pelo Projeto de Lei da Direção Nacional de Cibersegurança e Cibernética[11] de 2018, responsável por todos os aspectos da defesa cibernética na esfera civil, desde a formulação de políticas e construção de poder tecnológico até a defesa operacional no ciberespaço (ISRAEL, 2020; IISS, 2021, p. 70 e 73).

Nesse sentido, garante uma adaptabilidade organizacional na região em que Israel se encontra. Em tempos de paz, ela é responsável pela gestão da defesa cibernética nacional. Já em tempos de emergência, as FDI coordenam campanhas cibernéticas tanto ofensivas quanto defensivas. Há uma relação de cooperação entre o exército, academia, governo e sociedade com o mundo cibernético. Atualmente, existem várias plataformas de cooperação que permitem a difusão de conhecimentos entre estes setores (CSS, 2020, p. 18; IISS, 2021, p. 72).

Em resumo, há dois organismos principais dentro das FDI que possuem responsabilidades cibernéticas, sendo eles: a Unidade 8200, maior unidade do *Aman*, encarregada das capacidades cibernéticas ofensivas das FDI; e o C4I20 e o Diretório de Defesa Cibernética, responsáveis por prestar apoio tecnológico avançado às operações terrestres, marítimas e aéreas das FDI, incluindo missões de ciberdefesa (IISS, 2021, p. 71; CSS, 2020, p. 15).

A Unidade 8200, também conhecida como *Central Collection Unit of the Intelligence Corps* ou *Israeli SIGINT National Unit (ISNU)*, fornece importância à flexibilidade operacional: suas restrições legais são relativamente frouxas, possui uma cultura organizacional que aceita e incentiva ações ofensivas inéditas, operando com recursos financeiros substanciais, além de deter capacidades operacionais relativamente fortes. Destarte, a Unidade 8200 assumiu o ataque ofensivo cibernético conhecido como *Flame*, além de supostamente ter desenvolvido *Duqu* e *Stuxnet*. Essas operações são exemplos dos seus objetivos: sabotagem de instalações industriais, espionagem e apoio às forças militares. Posto isto, tanto o *Mossad* quanto o *Shin Bet* cooperam com ela (CSS, 2020, p. 15-16).

[11]Este projeto de lei não avançou no processo legislativo devido aos impasses políticos e às fortes objeções levantadas nas áreas profissionais de segurança cibernética bem como em autoridades governamentais, justamente por causa de suas preocupações com o amplo escopo de autoridade, além de possíveis ações invasivas e a potencial violação de privacidade em nome da segurança nacional. Em 2021, foi apresentado um novo projeto, sendo este uma abreviação da versão de 2018, porém enquadrado como legislação temporária com prazo de dois anos. Este ainda está em análise (CSS, 2020, p. 14; HOUSEN-COURIEL; MIMRAN; SHANY, 2021).

Não menos importante, esta unidade tem papel fundamental em influenciar a indústria tecnológica de Israel. Dentro da Unidade 8200, há uma seção de tecnologia (Unidade 81) que se concentra em pesquisa e desenvolvimento para seu próprio pessoal. Este tipo de cooperação entre os setores privado e militar israelenses fornece uma vantagem tecnológica para ambos os envolvidos, isto é, novas tecnologias cibernéticas são testadas em campos de batalha, o que garante a sua eficácia e antes de serem promovidas no mercado global. Isto demonstra uma característica peculiar da interação da Unidade 8200 com as FDI (IISS, 2021, p. 72).

Já em relação ao Diretório C4I, também conhecido como *C4I Corps* ou *Teleprocessing Corps*, tem por objetivo proteger a infraestrutura de comunicação e os sistemas de teleprocessamento do IDF, sendo subordinada à *Computer Services Directorate (Atak).* Atualmente, ela atua a partir de uma abordagem de "defesa ativa", a qual implica uma série de ataques de dissuasão e prevenção. Esta atuação remete aos princípios doutrinários de 1953 de Ben Gurion no que diz respeito à defesa do Estado, ou seja, vitória rápida e decisiva, dissuasão, superioridade qualitativa e capacidades de alerta precoce. Esta diretoria possui um centro que, por sua vez, integra a divisão de informática e as forças de inteligência militar, apesar de sofrer algumas limitações financeiras (CSS, 2020, p. 16).

Nesse sentido, tem-se que os principais órgãos de defesa cibernética das FDI são a Unidade 8200 (operações ofensivas) e a Diretório C4I (operações defensivas e de segurança de infraestrutura), ainda que *Shin Bet, Mossad,* a Polícia de Israel e o Ministério da Justiça também estejam envolvidos. Todos colaboram e são coordenados pelo INCD (CSS, 2020, p. 5). É interessante notar que o desenvolvimento das capacidades de ciber-inteligência estão centradas principalmente na Unidade 8200 (IISS, 2021, p. 71).

A Polícia de Israel, por sua vez, objetiva lidar com o crime cibernético e servir como um ponto central para o desenvolvimento de perícia digital e evidências (CCDCOE, 2017, p. 13). Nesta instituição, há poucas pessoas trabalhando dentro da unidade de crimes cibernéticos (LAHAV 433), sendo considerado o ator mais fraco da comunidade de segurança israelense, isto é, não possui capacidade de impactar significativamente no desenvolvimento de políticas (CSS, 2020, p. 15). *Lahav 433* é uma organização-chave da Polícia de Israel contra crimes cibernéticos. Criada em 2008, esta organização está dividida em três áreas principais de atuação: investigações, inteligência e tecnologia. Além de contar com uma assessoria jurídica especializada em tecnologia, ela trabalha em conjunto com a Unidade 105, estabelecida para prevenir a violência contra menores na Internet (DOMBE, 2020).

O Ministério da Justiça israelense também possui um papel relevante no que tange à capacidade cibernética. Dentre os cargos existentes dentro deste ministério, há o escritório do Procurador-Geral *(State Attorney)*, o qual possui uma unidade cibernética *(Cyber Unit)*, estabelecida em 2015. A criação desta unidade surgiu a partir do trabalho realizado em conjunto com o *National Cyber Bureau* (NCB) do gabinete do Primeiro-Ministro, adotado pelo Procurador-Geral e pelo Procurador do Estado. De acordo com o Ministério, os crimes cibernéticos passaram a apresentar uma forte tendência de crescimento, tanto no aspecto qualitativo quanto quantitativo, o que forçou o Ministério Público a reconhecer a necessidade de coordenar esforços no enfrentamento ao crime e ao terrorismo no âmbito cibernético (ISRAEL, 2021b).

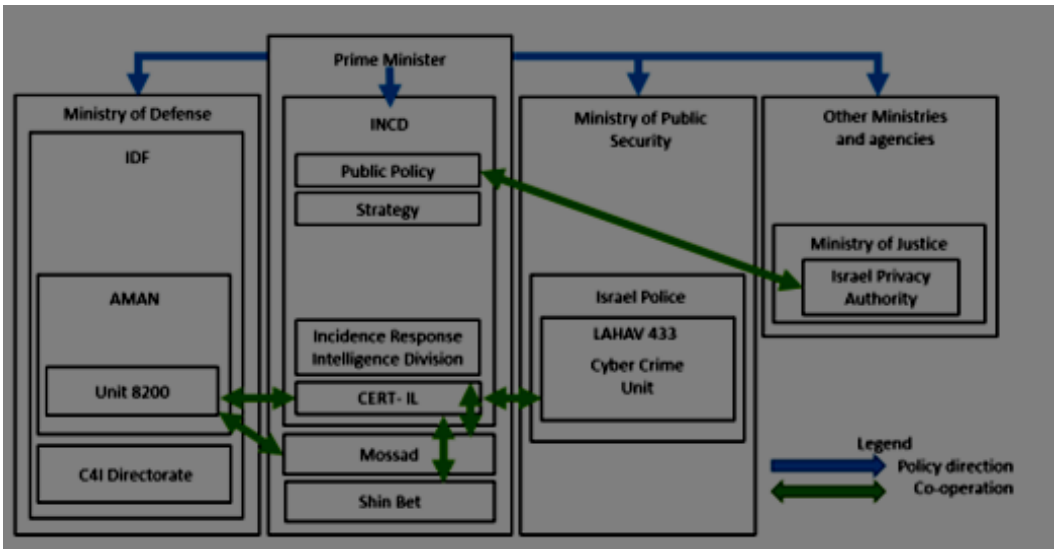
Destarte, a *Cyber Unit* atua em três áreas: (a) divisão da sede do Ministério Público na área de cibernética e o SIGINT, englobando questões de infrações informáticas, provas digitais, escutas telefônicas e dados de comunicações[12]; (b) condução de arquivos criminais no campo de crimes de informática e informação que estão sob investigação pela *Lahav 433*, da Polícia de Israel e pela Autoridade de Lei, Informação e Tecnologia de Israel no Ministério da Justiça; e (c) execução alternativa para a prevenção e frustração de danos de atos proibidos no ciberespaço, compreendendo atos de remoção de conteúdo ofensivo, filtragem de resultados de buscas, coibição de internautas de atos proibidos e medidas protetivas e preventivas no ciberespaço como instrumentos legais (ISRAEL, 2021b).

Em relação às parcerias, a Unidade Cibernética do Gabinete do Procurador do Estado trabalha rotineiramente com a Polícia de Israel, os órgãos de segurança e defesa, o NCB, a Lei Israelense, Informação e Tecnologia Autoridade no Ministério da Justiça, o Gabinete de Assessoria Jurídica e Assuntos Legislativos do Ministério da Justiça, os comitês do *Knesset*, os provedores de serviços de Internet, colegas e partes paralelas em todo o mundo, as organizações internacionais que lidam com a área de cibernética e as ONGs que operam nas áreas de proteção contra danos no ciberespaço (ISRAEL, 2021b).

A figura 1 apresenta como a organização do Ministério da Justiça está dividida. Observa-se que o Gabinete do Procurador-Geral faz parte da Autoridade Executiva do Estado israelense e atua como uma unidade separada, porém dentro do Ministério da Justiça (ISRAEL, 2019). Dentre os departamentos existentes, encontra-se a *Cyber Unit*.

[12]Esta unidade direciona e assiste profissionalmente os advogados e órgãos de fiscalização dessas áreas em todos os temas relacionados ao trabalho do Ministério Público (ISRAEL, 2021b).

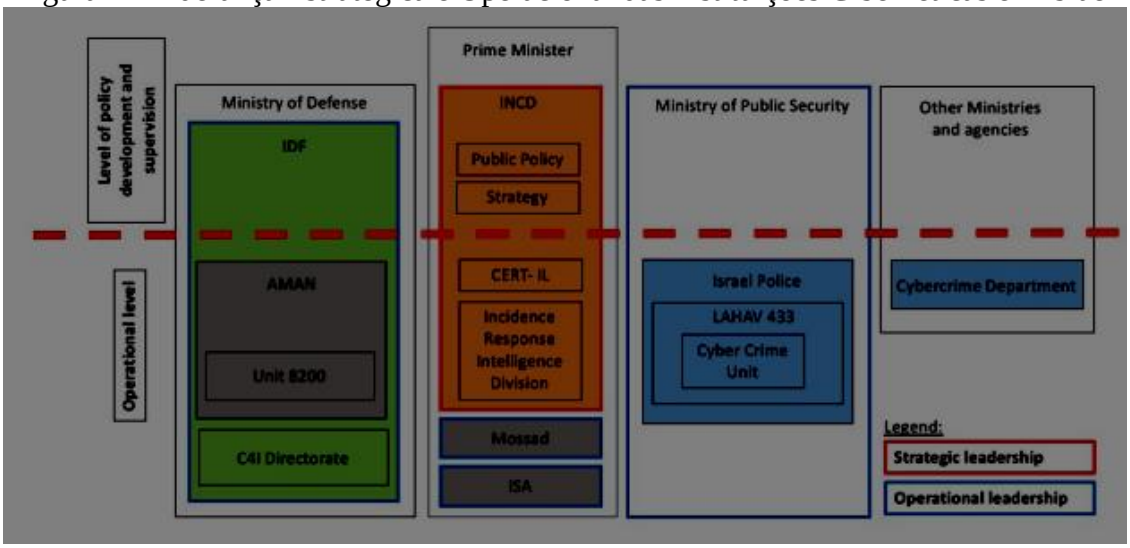
Figura 1 - Estrutura Geral da Organização Cibernética em Israel



Fonte: CSS, 2020, p. 14

A figura apresenta uma caracterização da estrutura geral da organização de segurança cibernética em nível nacional. Entretanto, por conta da própria classificação dos documentos e das ações de cada órgão, bem como a lei cibernética ainda não estar em vigor, as informações fornecidas pela figura não são baseadas em declarações oficiais. A ausência dessa política oficial de cooperação fornece relativa flexibilidade para os atores: caso tenham de lidar com algum problema e, caso algum órgão não queira cooperar, o ator em questão possui margem de manobra para cooperar com certa liberdade com diferentes instituições (CSS, 2020, p. 14). A figura abaixo mostra a mesma organização de informações, porém enfatizando a liderança estratégica e operacional das instituições.

Figura 2 - Liderança Estratégica e Operacional das Instituições Cibernéticas em Israel

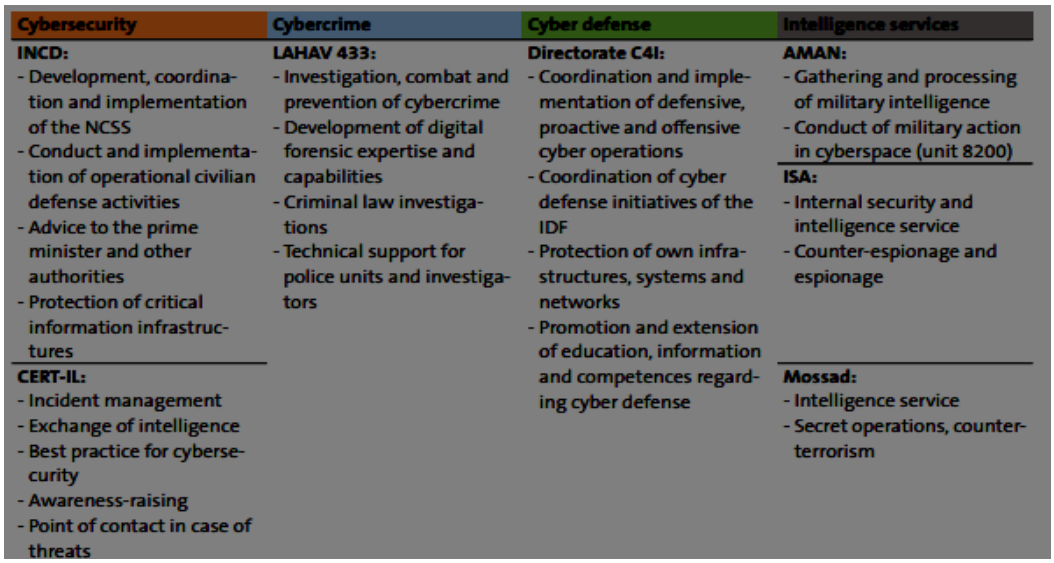


Fonte: CSS, 2019, p. 26

A estrutura organizacional de Israel tem como vantagem um ecossistema de segurança cibernética estreito e conectado o suficiente para que as informações sejam trocadas de forma rápida e eficiente (CSS, 2020, p. 16). Desde o estabelecimento da diretoria cibernética em 2018, Israel possui um alto grau de centralização institucional de aspectos de segurança cibernética defensiva sob o comando das FDI e do INCD (CSS, 2019, p. 10). Em geral, esta centralização traz vantagens e melhorias.

Posto isto, a posição do INCD aponta a importância e a prioridade da segurança cibernética e da defesa para Israel, sendo uma das maiores prioridades políticas e securitárias nacionais – tanto para o lado militar quanto para o civil. Porém, tendo em vista que o INCD é a liderança estratégica do desenvolvimento da estrutura de segurança cibernética, há a tendência de sofrer influências externas, especialmente por *Shin Bet* (CSS, 2020, p. 16-17). A imagem abaixo apresenta quatro divisões relacionadas ao ciber (segurança, crime, defesa e inteligência) e resume onde cada organização se encontra, incluindo suas funções.

Figura 3 - Organização das instituições cibernéticas israelenses e suas funções



Cybersecurity	Cybercrime	Cyber defense	Intelligence services
INCD: - Development, coordination and implementation of the NCSS - Conduct and implementation of operational civilian defense activities - Advice to the prime minister and other authorities - Protection of critical information infrastructures	**LAHAV 433:** - Investigation, combat and prevention of cybercrime - Development of digital forensic expertise and capabilities - Criminal law investigations - Technical support for police units and investigators	**Directorate C4I:** - Coordination and implementation of defensive, proactive and offensive cyber operations - Coordination of cyber defense initiatives of the IDF - Protection of own infrastructures, systems and networks - Promotion and extension of education, information and competences regarding cyber defense	**AMAN:** - Gathering and processing of military intelligence - Conduct of military action in cyberspace (unit 8200) **ISA:** - Internal security and intelligence service - Counter-espionage and espionage
CERT-IL: - Incident management - Exchange of intelligence - Best practice for cybersecurity - Awareness-raising - Point of contact in case of threats			**Mossad:** - Intelligence service - Secret operations, counter-terrorism

Fonte: CSS, 2019, p. 27

Em suma, Israel percebeu que o desenvolvimento tecnológico o ajudaria a superar sua inferioridade quantitativa. Com isso, passou a criar instituições responsáveis por alavancar e desenvolver a tecnologia, a organização e o ecossistema necessário. O poder cibernético foi percebido como importante relativamente cedo, o que possibilitou que Israel se tornasse um dos líderes atualmente. Em geral, sem o progressivo reconhecimento pelos líderes de defesa e pela formação da Iniciativa Cibernética Nacional, não haveria uma organização governamental de cibersegurança que fosse capaz de coordenar todos os esforços políticos com o fito de promover a capacidade nacional no espaço cibernético e capacitar o país para lidar com as ameaças cibernéticas. Há, portanto, uma tendência à centralização da segurança cibernética em Israel, apesar da ausência da política oficial de cooperação entre as instituições cibernéticas. Para melhor compreender estas instituições, o próximo capítulo abordará, cronologicamente, os documentos relevantes para a criação e o desenvolvimento das instituições e, por conseguinte, das capacidades cibernéticas de Israel.

3 ESTRATÉGIA

Este capítulo atesta, a partir de documentos oficiais, a estratégia e a doutrina cibernéticas israelenses. Para tanto, foi necessário abordar o contexto histórico para entender a doutrina atual, tendo em vista que Israel possui uma estrita política de não publicar documentos relacionados a esta temática. Aliás, o país nunca realmente materializou sua doutrina em documentos oficiais, possuindo uma abordagem muito mais cultural. Tal é a importância do contexto histórico e do resgate dos princípios doutrinários de Ben Gurion. Desse modo, abordar-se-á, cronologicamente, os documentos relevantes para a criação e o desenvolvimento das capacidades cibernéticas israelenses, apresentando suas características e implicações.

Israel possui uma política de defesa nacional robusta. Apesar de sua desvantagem quantitativa em relação aos seus "inimigos" árabes desde a sua criação, o país conseguiu sucessivas vitórias nas guerras travadas no século anterior, demonstrando ser capaz de superar a inferioridade. Entretanto, Israel não possui uma estratégia formal de segurança nacional. Aliás, é comum que o país não publique quaisquer documentos ou declarações relacionadas a este assunto, seja por escolha ou por restrições. Apesar disso, de acordo com Adamsky (2010, p. 98), os obstáculos políticos e burocráticos invalidaram as tentativas de se formular uma estratégia de segurança nacional atualizada. Em razão do conservadorismo intelectual e da falta de estrutura organizacional, as FDI foram incapazes de reunir conceitos de forma coesa e traduzir as ideias teóricas abstratas em reformas militares concretas. Isto posto, Israel, em vez de depender de processos de planejamento formalizados e burocráticos, implementa esforços de segurança de uma forma mais *ad hoc* (CSS, 2020, p. 9; ADAMSKY, 2010, p. 98).

Impelido por esta mentalidade *ad hoc*, as FDI não codificaram conceitos de segurança e doutrina militar de forma escrita, sob o argumento de que a liderança política forneceria orientação clara para elaborar a estratégia mais relevante em qualquer situação. Ademais, a relutância em anunciar visões de longo prazo, que podem parecer dolorosas e intoleráveis internamente e diminuir o espaço para manobras políticas, foi um dos fatores centrais para uma orientação de curto prazo. Em geral, a tomada de decisões da segurança nacional israelense gerenciou uma grande estratégia no cotidiano (ADAMSKY, 2010, p. 116).

Logo após a criação do Estado de Israel, Ben Gurion entregou, ao gabinete, o relatório que continha os princípios doutrinários que viriam a ser utilizados por Israel em sua política de segurança. Essa grande estratégia, conhecida como *Tfisat HaBitachon*, foi e vem sendo adaptada dinamicamente pelo *establishment* político e de defesa israelense. Contemplada há quase 70 anos, estes princípios doutrinários são o mais próximo que Israel já chegou de uma estratégia

formal de segurança nacional. Apesar de não ter sido elucidada de forma escrita, bem como ter sido formulada em um ambiente estratégico pouco semelhante ao atual, esta “doutrina” de defesa possui um grande impacto no pensamento estratégico do país até hoje (CSS, 2020, p. 9; FREILICH, 2018a, p. 413).

Na época, o país israelense enxergava o conflito árabe-israelense como longo, amargo e, até mesmo, existencial. Desde o início, acreditava-se que este conflito duraria décadas, talvez até séculos, de modo a não ter um fim tão próximo. Ademais, também enxergavam que a tensão existente entre Israel e os países árabes vizinhos não poderia ser alterada, ou que pelo menos Israel não tivesse margem para alterá-lo. Nesse sentido, ataques convencionais dos Estados árabes eram considerados a principal ameaçada até a década de 1980, além do terrorismo (FREILICH, 2018a, p. 413).

Uma das principais preocupações era o território estreito de Israel, de modo que suas fronteiras eram potencialmente indefensáveis e que o país poderia ser invadido rapidamente pelo norte (pela Síria), centro (pela Jordânia) e sul (pelo Egito). Além disso, esta preocupação era ainda mais agravada pela falta de obstáculos naturais e pela topografia adversa, isto é, a Síria possuía presença militar dominante nas Colinas de Golã, enquanto que a atual Cisjordânia (antiga Jordânia) tinha uma saliência profunda que se estendia até o centro de Israel. Outrossim, a maior parte de sua população (consideravelmente menor que a dos países árabes), bem como a maioria das instituições governamentais, instalações militares e infraestrutura nacional estavam concentrados na estreita planície costeira, os quais eram ameaçados pelo alcance da artilharia da Cisjordânia (FREILICH, 2018a, p. 413-414).

Dessa maneira, Israel carecia tanto de profundidade estratégica quanto tática: os países árabes detinham grandes exércitos permanentes enquanto que Israel possuía assimetria populacional e era dependente sobretudo de um exército reservista. Ademais, os árabes eram capazes de recorrer a recursos econômicos muito maiores, o que lhes permitia sustentar suas forças armadas. Eles também contavam com o apoio do Mundo Árabe e muçulmano, além de outros países e também da então União Soviética que, por sua vez, poderia ter interposto a seu favor. Isto faria com que Israel cessasse suas hostilidades antes mesmo de ter alcançado seus objetivos (FREILICH, 2018a, p. 414). É neste momento que Israel percebe a serventia do tempo.

No final de 1948, tinha-se a ideia de que, mesmo depois que os combates cessassem e a paz prevalecesse, Israel ainda precisaria estar preparado consistente e eficientemente para a defesa a qualquer momento. Concomitantemente, compreendia-se que o país israelense era economicamente incapaz de sustentar um grande exército regular, ainda mais passando por um

intenso processo de imigração, desenvolvendo assentamentos, construindo infraestrutura básica e garantindo seu crescimento econômico. Nesse sentido, o objetivo de Ben-Gurion era combinar a operacionalização e o crescimento da economia com o desenvolvimento de uma capacidade de defesa militar (TABANSKY; ISRAEL, 2015, p. 10).

Esta doutrina era essencialmente defensiva, mas operacionalmente ofensiva, com o fito de garantir a sobrevivência de Israel e derrotar rapidamente quaisquer adversários. A dissuasão desenvolvida por Israel foi organizada com o objetivo de demonstrar aos seus inimigos que tentativas de destruí-lo seriam fúteis, o que levaria às vitórias sucessivas e a aceitação de Israel (FREILICH, 2018a, p. 415).

De certo modo, a cultura de guerra israelense foi afetada pela preferência por guerras curtas em solo inimigo, de modo que a estratégia defensiva, o *status quo* e as táticas ofensivas tornaram-se as normas regulatórias da cultura estratégica israelense. De acordo com a mentalidade que se tinha na época, somente uma guerra agressiva destinada a penetrar rapidamente na retaguarda do inimigo possibilitaria conquistar uma vitória decisiva em pouco tempo. Ademais, tinha-se que a iniciativa operacional ofensiva provocava máxima eficiência de suas forças menores, mas melhor treinadas, equipadas e motivadas. Assim, a tática ofensiva examinou o efeito sinérgico do apoio aéreo aproximado, da blindagem pesada e da inteligência, cristalizando-os durante as duas primeiras décadas da existência do Estado em uma doutrina operacional não escrita (ADAMSKY, 2010, p. 112).

Isto posto, a Blitzkrieg não somente serviu como inspiração intelectual como também se tornou uma opção instintiva e uma forma quase única de guerra. A negligência das operações defensivas em favor do romantismo ofensivo neutralizou a noção de defesa móvel no pensamento operacional israelense, produziu estratagemas e diminuiu a capacidade de travar guerras prolongadas de atrito. O *ethos* da ofensiva *à outrance*[13] impôs uma abordagem simplista e mecânica ao pensamento militar israelense (ADAMSKY, 2010, p. 112-113).

Em suma, os princípios propostos por Ben Gurion em 1948 para que Israel mantenha "preparação consistente e eficiente para defesa a qualquer momento", mesmo após o fim da guerra e dos conflitos, ainda são relevantes em relação às estratégias de cibersegurança e a defesa cibernética atual (CSS, 2020, p. 9). Tais princípios podem ser resumidos da seguinte maneira:

a) Defesa do Estado, seus habitantes, sua infraestrutura e seus interesses;
b) Dissuasão de potenciais ataques;

[13]Expressão que significa "com exagero", "sem misericórdia ou piedade."

c) Formação de alianças com grandes potências para aumentar a dissuasão, fortalecer a "Muralha de Ferro" e conter os países vizinhos por um ataque total;
d) Desenvolvimento de capacidades sofisticadas de alerta precoce para compensar a falta de profundidade estratégica e inferioridade numérica;
e) Alcançar a superioridade tecnológica e adquirir uma vantagem qualitativa para compensar a falta de recursos críticos e equilibrar a inferioridade numérica;
f) Assegurar uma vitória rápida e decisiva em caso de confronto (CSS, 2020, p. 9; TABANSKY; ISRAEL, 2015, p. 11).

Estas premissas básicas nunca foram reexaminadas, nem após a guerra de 1967, quando Israel adquiriu profundidade operacional e sofisticação tecnológica, tampouco após o tratado de paz de 1979 com o Egito, o qual reforçou essas tendências. Esse culto da ofensiva estava em harmonia com traços da personalidade estratégica israelense como mentalidade de insegurança (*siege mentality)*, dinamismo, iniciativa, improvisação e criatividade operacional (ADAMSKY, 2010, p. 113).

As circunstâncias estratégicas de Israel foram transformadas a partir da Guerra de Seis Dias, de 1967, quando o mundo árabe, então comprometido com a destruição de Israel, percebeu sua derrota e a inevitável realidade de que o país não seria derrotado tão facilmente. Além disso, depois da Guerra de Yom Kippur, de 1973, os países reconheceram que não poderiam recuperar os territórios perdidos em 1967 estritamente pela guerra. A nova profundidade estratégica conquistada garantiu a Israel certa seguridade (FREILICH, 2018a, p. 416).

Nas duas décadas seguintes, os laços entre Israel e Estados Unidos evoluíram dramaticamente, tornando-se um relacionamento institucionalizado e estratégico que perdura até hoje. Esta parceria transformou as capacidades militares e a segurança geral de Israel. Desde a década de 1980, os Estados Unidos se comprometeram formalmente a preservar a vantagem militar qualitativa (QME) de Israel sobre qualquer combinação de exércitos árabes hostis. A paz com o Egito transformou ainda mais as circunstâncias estratégicas de Israel: o Estado árabe mais poderoso na época estava, agora, fora do conflito. Isto significou que os outros países não tinham mais a opção militar convencional contra Israel (FREILICH, 2018a, p. 416).

Até hoje, Israel ainda enfrenta assimetrias cruciais com os árabes em relação à população, ao território, aos recursos e à capacidade de formar coalizões. Entretanto, o mundo árabe não foi capaz de agir coordenadamente para atingir seu objetivo contra Israel. Nesse sentido, é

possível que Israel tenha alcançado a paridade convencional e até a superioridade contra qualquer adversário provável. Muitas das ameaças que Israel enfrenta hoje não se originam mais dos pontos fortes dos árabes, mas de suas fraquezas (FREILICH, 2018, p. 417).

Outrossim, a natureza da guerra e, por consequência, as ameaças militares que Israel enfrenta, mudaram drasticamente. A ameaça de uma guerra convencional ou limitada em larga escala com um Estado árabe é menos provável atualmente, havendo uma perspectiva quase nula de (re)conquista do território israelense, e o perigo de uma coalizão de guerra árabe é quase inexistente. Atualmente, as principais ameaças que Israel enfrenta advém de guerras irregulares e assimétricas, incluindo guerra cibernética e mísseis balísticos. Isto é, com a importante exceção do Irã, a ameaça hoje é de atores não estatais (FREILICH, 2018b, p. 62).

Como uma nação que depende fortemente de tecnologia avançada, Israel é vulnerável a ataques cibernéticos. De fato, Israel enfrenta constantes ataques cibernéticos. Consequentemente, o âmbito cibernético rapidamente passou a ocupar um lugar significativo no pensamento de defesa israelense nos últimos anos (FREILICH, 2018a, p. 422).

Em 2015, foi publicada, pelas FDI, a primeira doutrina de defesa pública que, por sua vez, incluía a perspectiva das FDI sobre o uso de capacidades cibernéticas. Em essência, este documento reconhece o desenvolvimento de capacidades cibernéticas dos considerados inimigos. Além disso, adota o domínio cibernético como um dos quatro domínios relevantes para a defesa do país, além da terra, do mar e do ar. Dessa maneira, a estratégia publicada considera estas capacidades como suporte integrado para a defesa e para o ataque convencionais em todos os níveis de combate, seja no âmbito estratégico, operacional ou tático. Isto posto, fica claro que as FDI passaram a considerar a defesa e o ataque cibernéticos como indispensáveis na utilização de inteligência, na defesa coletiva, nas operações de influência e na obtenção de legitimidade e respostas legais para o funcionamento das suas instituições e do Estado (CSS, 2020, p. 9).

Israel, até antes de 2017, nunca havia elaborado uma estratégia nacional holista e oficial de segurança cibernética. Entretanto, várias resoluções governamentais tentaram ordenar o cenário de segurança cibernética de Israel.

O Ministry of Defense Directorate for Defense Research & Development *(Maf'at),* após anos de experiência em defesa, acumulou conhecimento sobre a infraestrutura civil e as vulnerabilidades cibernéticas acumuladas. Ao comunicar suas preocupações de segurança cibernética às outras esferas do governo, este então encarregou o *National Security Council* (NSC), composto por altos funcionários do governo, representantes do Banco de Israel e agências de defesa,

de conceber estratégias com o fito de lidar com os riscos em ascensão. O resultado foi a Resolução Especial B/84, de 2002, sobre "a responsabilidade de proteger os sistemas informatizados no Estado de Israel", o qual definiu as finalidades e os meios da política de segurança cibernética israelense (TABANSKY; ISRAEL, 2015, p. 35-36).

Como qualquer documento formal, esta resolução traz fundamentos conceituais, tendo em vista que a Internet e a Web frequentemente se confundem com o espaço cibernético. Sendo assim, os sistemas de informação foram delineados como interconectados com o espaço físico, isto é, o que hoje é chamado de "ciberespaço" não era visto como um ambiente virtual, ou como uma área independente de operação. Tendo isto em vista, o sistema de *informação* se diferencia de um sistema de *controle*: enquanto o primeiro realiza atividades automatizadas de recepção de entrada, armazenamento, processamento e transmissão de informações, o segundo é um sistema integrado por computador que controla e supervisiona a frequência e regulação de atividades mensuráveis, realizadas por meios mecanizados dentro do próprio sistema de informação (grifo meu). Dessa maneira, a Resolução B/84 define a incumbência pela proteção dos sistemas informatizados que, por sua vez, são compartilhados pelo usuário (organização supervisionada) que opera a infraestrutura crítica, tal como pelos reguladores estaduais. Isto significa que o governo intervém em alguns temas de segurança e proteção, incluindo TI (tecnologia da informação) (TABANSKY; ISRAEL, 2015, p. 36).

Ademais, a resolução estabelece dois reguladores complementares, destinados a criar a capacidade organizacional contínua necessária para Israel se adaptar às mudanças impulsionadas pelo uso do ciberespaço: "o comitê de direção superior para a proteção de sistemas informatizados no Estado de Israel" e "a unidade nacional para a proteção de sistemas informatizados vitais" (TABANSKY; ISRAEL, 2015, p. 36). Outrossim, a Resolução B/84 trouxe um dos primeiros conceitos de política de CIP e incumbiu a NISA e o comitê diretivo de políticas com a implementação do CIP. O problema que acabou sendo gerado foi que, como a NISA fazia parte do *Shin Bet*, este possuía vasta autoridade e acesso considerável a informações e poder discricionário sobre questões de segurança. Ademais, o custo das medidas impostas teve de ser coberto pelas organizações supervisionadas. No geral, a consequência foi que a agência de inteligência parecia sufocar a inovação e o crescimento econômico (CSS, 2020, p. 10).

Em 2010, Netanyahu solicitou ao NSC uma revisão sobre a segurança cibernética e a política de Israel voltada a este tema. Aparentemente, o NSC não implementou essa tarefa. O primeiro-ministro então se aproximou do professor major-general aposentado, Isaac Ben-Israel,

que, na época, era o presidente do Conselho Nacional de Pesquisa e Desenvolvimento do Ministério da Ciência, para assumir a revisão. Ele aceitou o pedido e a Iniciativa Cibernética Nacional foi lançada em 2010. Desse modo, o ramo cibernético se tornou um objetivo nacional explícito com o lançamento desta iniciativa (TABANSKY; ISRAEL, 2015, p. 43).

A força-tarefa empregada nesta iniciativa foi encarregada pelo primeiro-ministro de propor medidas com o objetivo de promover a liderança israelense em segurança cibernética em nível global. Suas doze recomendações finais foram incorporadas à Resolução Governamental 3611, em 2011, intitulada *Advancing National Cyberspace Capabilities.* A Resolução também estabeleceu o INCB como o primeiro órgão consultivo para a segurança cibernética (CCDCOE, 2017, p. 8). Outrossim, a Resolução adotou as recomendações da força-tarefa:

> *To work towards advancing national capabilities in cyberspace and improving management of current and future challenges in cyberspace. To improve the defense of national infrastructures which are essential for maintaining a stable and productive life in the State of Israel and to strengthen those infrastructures, as much as possible, against cyber attack, by advancing Israel's status as a center for the development of information technologies; while encouraging cooperation among academia, industry and the private sector, government ministries and special bodies*[14] (ISRAEL, 2011, p. 1).

Além disso, o documento traz definições importantes sobre o ciberespaço, a cibersegurança e o espaço civil dentro do ciberespaço. O primeiro é definido como o domínio físico e não físico, criado ou composto por parte ou todos os seguintes componentes: sistemas mecanizados e informatizados, redes de computadores e comunicações, programas, informações computadorizadas, conteúdo veiculado por computador, tráfego e supervisão dados e aqueles que usam esses dados. O segundo, como políticas, arranjos de segurança, ações, diretrizes, protocolos de gestão de risco e ferramentas tecnológicas designadas para proteger o ciberespaço e permitir que ações sejam tomadas. Por fim, o espaço civil é tido como o ciberespaço que inclui todos os órgãos governamentais e privados do Estado de Israel, excluindo órgãos especiais (ISRAEL, 2011, p. 1).

Outrossim, o principal aspecto operacional da Resolução 3611 foi estabelecer, no gabinete do Primeiro-Ministro, o INCB (*Bureau)* e suas funções, bem como promover a capacidade nacional no ciberespaço e melhorar a disposição de Israel para lidar com os desafios atuais e

[14]Trabalhar para o avanço das capacidades nacionais no ciberespaço e melhorar a gestão dos desafios atuais e futuros no ciberespaço. Melhorar a defesa das infraestruturas nacionais que são essenciais para manter uma vida estável e produtiva no Estado de Israel e fortalecer essas infraestruturas, tanto quanto possível, contra ataques cibernéticos, promovendo o status de Israel como um centro para o desenvolvimento de tecnologias de informação ; ao mesmo tempo em que incentiva a cooperação entre academia, indústria e setor privado, ministérios governamentais e órgãos especiais. (ISRAEL, 2011, p. 1, tradução nossa).

futuros no ciberespaço. Sendo assim, o INCB ficou responsável por melhorar a segurança cibernética, avançar a posição de Israel como centro de desenvolvimento de tecnologia cibernética, incentivando a cooperação entre academia, indústria e setor privado, escritórios do governo e a comunidade de defesa (ISRAEL, 2011; TABANSKY; ISRAEL, 2015, p. 50). De modo geral, *"[t]he Bureau functions as an advising body for the Prime Minister, the government and its committees, which recommends national policy in the cyber field and promotes its implementation, in accordance with all law and Government Resolutions*[15]*"* (ISRAEL, 2011, p. 3).

Dividido em dois adendos, a Resolução 3611 estabelece princípios para avançar as capacidades cibernéticas defensivas em Israel e desenvolver a pesquisa e o desenvolvimento no ciberespaço e na supercomputação (adendo A), além de regulamentar a responsabilidade de lidar com o campo cibernético (adendo B). O primeiro adendo é voltado para as especificações do primeiro órgão consultivo para a segurança cibernética, isto é, estabelece a missão, as metas e os objetivos (que juntos somam 27), além da estrutura organizacional, localização, orçamento e administração do INCB. O adendo B remete ao regulamentando das responsabilidades para lidar com o campo cibernético, estabelecendo procedimentos burocráticos em relação às instituições envolvidas (ISRAEL, 2011, p. 3-9).

Posteriormente, outras resoluções governamentais foram promulgadas. Em especial, destaca-se as Resoluções 2443 e 2444, ambas de 2015. Estas resoluções foram particularmente importantes pois elaboraram as prioridades nacionais e expandiram a capacidade institucional de segurança cibernética. O governo israelense, ao aceitar as recomendações da força-tarefa de 2014, também sob os auspícios do professor Isaac Ben-Israel, decidiu estabelecer uma nova autoridade para melhorar a segurança cibernética no setor civil por meio da Resolução 2443, intitulada *Advancing National Regulation and Governmental Leadership in Cyber Security*. A nova autoridade nacional, a NCSA, obteve autoridade legal necessária para defender a esfera civil de ameaças cibernéticas. Esta foi criada para atuar ao lado do INCB que, por sua vez, continuava a manter Israel como líder internacional no âmbito cibernético (TABANSKY; ISRAEL, 2015, p. 58; CCDCOE, 2017, p. 11).

De modo geral, a Resolução 2443 determina o procedimento de integração de novos regulamentos de segurança cibernética dentro do alcance dos existentes ministérios governamentais e outros reguladores, cada qual responsável pelas capacidades regulatórias adicionais

[15]"O Bureau funciona como um órgão consultivo do Primeiro-Ministro, do governo e das suas comissões, que recomenda a política nacional no domínio cibernético e promove a sua implementação, de acordo com toda a lei e Resoluções do Governo" (ISRAEL, 2011, p. 3, tradução nossa).

de seu próprio setor. Isto é, o Ministério dos Transportes ficaria encarregado de regular a segurança cibernética no setor de transporte, por exemplo (CCDCOE, 2017, p. 12). Por objetivos, adota:

> *To advance national regulation in cyber security, and to work for governmental leadership in cyber security as part of the implementation of national regulation and to serve as an example for the public and the economy. This regulation will not apply to the defense community or to its activities through government offices as part of its missions*[16] (ISRAEL, 2015a, p. 1).

Ademais, também estabeleceu a autoridade para regulamentar o mercado de profissionais, serviços e produtos de segurança cibernética por meio do INCB (CCDCOE, 2017, p. 12). Nesse sentido, em suas definições, compreende-se mercado de serviços de segurança cibernética como empresas, fabricantes, fornecedores, instituições de treinamento e certificação e profissionais que fornecem *know-how*, produtos e serviços em segurança cibernética às organizações. Por setor, entende-se todas as organizações que trabalham no âmbito profissional de uma repartição pública e no âmbito da sua autoridade reguladora (ISRAEL, 2015a, p. 1).

Em suma, a Resolução 2443 tem por objetivo fornecer estruturas legais para as atividades da comunidade de inteligência (ou seja, equilibrar liberdade básica, privacidade e direitos civis) e apoiar empresas que carecem de recursos humanos e financeiros. Outrossim, esta resolução e, portanto, a NCSA, consistem sobretudo de novos elementos, tais como CERT-IL e seus CERTs setoriais. Estes CERTs são o cerne de Israel no que se refere ao gerenciamento e tratamento de incidentes de segurança cibernética, os quais aumentam a resiliência nacional contra ameaças cibernéticas (CCDCOE, 2017, p. 10; TABANSKY; ISRAEL, 2015, p. 58).

A subsequente Resolução 2444, denominada *Advancing the National Preparedness for Cyber Defense*, delineou o desenvolvimento da regulamentação, da padronização, do licenciamento, da auditoria, do treinamento, da instrução, das relações-públicas e da cooperação internacional. Ademais, encarregou a NCSA de desenvolver uma doutrina cibernética nacional. Em geral, a resolução determina que *"[...] protecting the proper and safe functioning of cyberspace is an essential national security interest for the State and an essential governmental interest for national security*[17]*"* (ISRAEL, 2015b, p. 1). Nesse sentido, a resolução define a segurança cibernética como o conjunto de ações para a prevenção, a mitigação, a investigação e o tratamento

[16]Promover a regulamentação nacional em segurança cibernética e trabalhar pela liderança governamental em segurança cibernética como parte da implementação da regulamentação nacional e servir de exemplo para o público e a economia. Este regulamento não se aplica à comunidade de defesa ou às suas atividades por meio de órgãos governamentais como parte de suas missões (ISRAEL, 2015a, p. 1, tradução nossa).

[17]"[…] proteger o funcionamento adequado e seguro do ciberespaço é um interesse essencial de segurança nacional para o Estado e um interesse governamental essencial para a segurança nacional" (ISRAEL, 2015a, p. 1, tradução nossa).

de ameaças e incidentes cibernéticos e a redução de seus efeitos e dos danos causados por eles antes, durante e após sua ocorrência (ISRAEL, 2015a, p. 1).

A Iniciativa Cibernética Nacional e as Resoluções implementadas demonstram que Israel, há décadas, se preocupa com as questões de segurança e ameaças cibernéticas. Entretanto, estas informações aqui citadas fazem parte de uma pequena parcela daquelas disponibilizadas ao público. Israel mantém a sua consistente posição em fornecer poucos detalhes sobre as considerações de segurança cibernética nacional e as políticas na esfera militar. Não obstante, houve uma ruptura deste padrão em 2015, quando o Chefe do Estado-Maior, Gadi Eizenkot, publicou *The IDF Strategy*.

De acordo com Finkel (2020, p. 4), o documento foi divulgado por Eizenkot com a intenção de aumentar a transparência entre as FDI, o escalão político e o público, além de tentar encorajar o esqueleto político a se familiarizar com as ideias expressas nele. Esta atitude pode ser entendida como uma espécie de resposta à ausência de documentos oficiais sobre segurança nacional, tendo em vista que apenas quatro documentos deste tipo foram divulgados. Apesar de sua publicação ter sido um fato histórico, outros documentos semelhantes já tinham circulado internamente. Nesse sentido, a divulgação do documento foi um esforço bem-sucedido das FDI para estimular o debate público sobre assuntos de defesa (FREILICH, 2018b, p. 200-201).

Este documento é um resumo não classificado da abordagem militar geral das FDI, sendo um documento militar, não uma declaração geral de estratégia nacional, o qual inclui, entre outras, a perspectiva de Eizenkot sobre o uso de capacidades cibernéticas (CSS, 2020, p. 9; CCDCOE, 2017. p. 9). É interessante notar que o plano *Gideon* foi parte de uma revisão mais ampla do pensamento estratégico das FDI incorporado na *IDF Strategy* de 2015. Este era um plano operacional e orçamentário de 2016 a 2020, o qual se concentrava na implementação de reformas estruturais dentro das FDI e no aprimoramento da eficiência e nas mudanças na alocação de recursos. O objetivo geral era reduzir o tamanho das FDI, porém tornando-as melhores treinadas e equipadas, com um alto nível de prontidão. Entretanto, este plano incluía a criação de novos comandos cibernéticos e de batalhões (FREILICH, 2018b, p. 200). Ademais, o plano *Gideon* é responsável pelo novo Memorando de Entendimento (MOU) entre os EUA e Israel, assinado em 2016. Sob o novo MOU, a ajuda militar dos EUA a Israel durante 2019-2028 será de US$ 3,3 bilhões por ano (PINCHAS; TISHLER, 2019, p. 357).

Isto posto, o documento abarca diversas referências à posição das FDI sobre segurança cibernética, englobando o entendimento de que o espaço cibernético é considerado um domínio militar, além de priorizar a construção sucessiva da capacidade cibernética ofensiva e defensiva

nos âmbitos estratégico, operacional e tático. Isto significa que as capacidades cibernéticas são apresentadas como alicerce para a defesa e ataque convencionais em todos os níveis. Ademais, o documento traz a consciência de ameaças no ciberespaço e, a nível organizacional, o início de um método para estabelecer a estrutura de comando cibernético dentro das FDI (CSS, 2020, p. 9; CCDCOE, 2017. p. 9).

Em geral, *IDF Strategy* constata que a defesa cibernética é vital para garantir a continuidade das operações das organizações nacionais em momentos de guerra ou de emergência, a utilização de inteligência, defesa coletiva, operações de influência e obtenção de legitimidade e respostas legais e o desempenho eficiente das FDI (CSS, 2020, p. 9; CCDCOE, 2017. p. 9). Mais especificamente, a estratégia descrita no documento identifica o desenvolvimento das capacidades cibernéticas dos que são considerados inimigos. Esta estratégia realça a dissuasão estratégica e tática via guerra cibernética (CSS, 2020, p. 9). Isto significa que as operações de proteção, coleta e ataque serão realizadas no domínio cibernético, de modo que Israel deve aumentar sua prontidão nessa área. Por fim, constata-se que o braço cibernético das FDI deve ser estabelecido para desenvolver as capacidades cibernéticas, possibilitando que as FDI possam ser capazes de funcionar mesmo sob ataque cibernético (UNIDIR, 2022).

Outrossim, foi a partir do documento *Israel National Cyber Security In Brief* que o INCD elaborou o primeiro *white paper* de segurança nacional israelense desde a declaração dos princípios estratégicos de Ben Gurion em 1953. Este é um pequeno documento que resumiu alguns *insights* de *white papers* confidenciais e publicados apenas internamente desde 2012. Esta estratégia, a qual proporciona uma estrutura política abrangente, é o resultado de quase uma década de desenvolvimento (CSS, 2020, p. 9; ADAMSKY, 2017, p. 116).

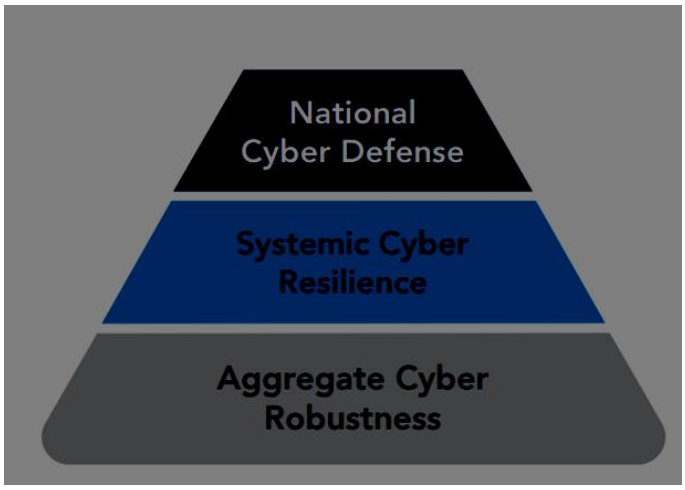
Os objetivos gerais do INCD, como o objetivo de defender a força econômica e social de Israel, descritos no documento, não se relacionam muito com a estratégia de 2015 de Eizenkot. Particularmente, retrata como Israel planeja melhorar sua robustez cibernética, sua resiliência sistêmica, sua defesa cibernética nacional civil, além de minuciar o estabelecimento e as tarefas da NCSA. Por fim, aborda a capacitação e a cooperação internacional (CSS, 2020, p. 9).

Isto posto, o primeiro capítulo, *Concept of Operations* (CONOP), delineia o próprio conjunto de atividades voltadas à defesa cibernética. A estratégia de segurança cibernética de Israel é baseada em um conceito de operações para a segurança cibernética nacional. Esta estrutura conceitual foi criada e é utilizada para todos os esforços e funções do Estado no contexto da segurança cibernética nacional. Ademais, inclui tanto ações diretas do Estado para enfrentar ameaças cibernéticas quanto esforços indiretos destinados a incentivar e apoiar atividades de

segurança no setor privado e, desse modo, colaborar com ele (ADAMSKY, 2017, p. 117; ISRAEL, 2017b, p. 9).

Em geral, o CONOP israelense consiste em uma estrutura de três camadas: robustez cibernética agregada, resiliência cibernética sistêmica e defesa cibernética nacional. De acordo com o documento, a abordagem, de três camadas, deriva da natureza única da ameaça cibernética e do papel central das organizações privadas na obtenção da segurança cibernética nacional. Outrossim, cada camada difere entre si em seus objetivos, no papel do Estado e nas relações entre o Estado e as instituições privadas (ISRAEL, 2017b, p. 9). A imagem abaixo demonstra a hierarquização de cada camada.

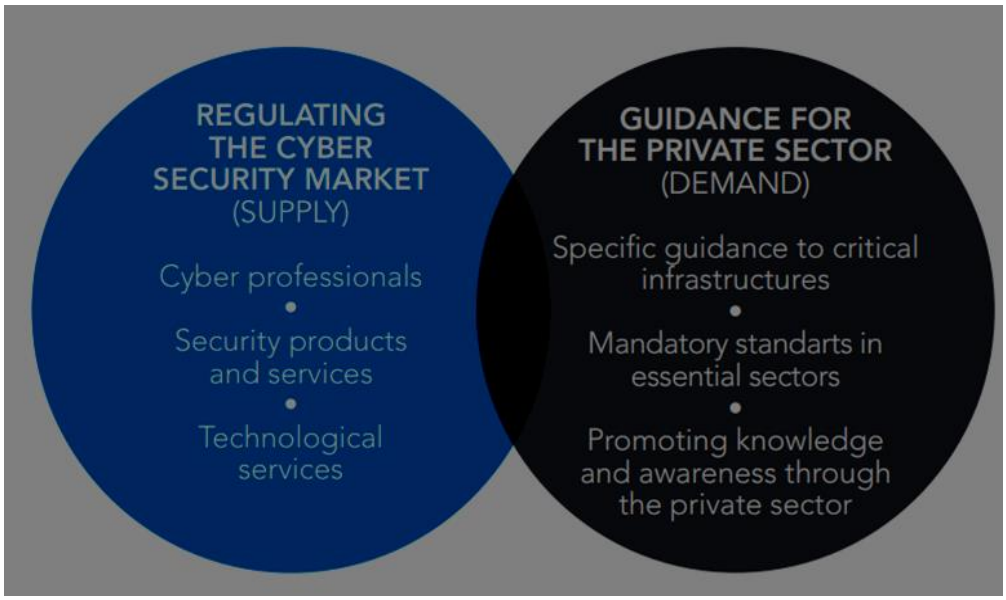
Figura 4 - As três camadas conceito de operações para a segurança cibernética israelense



Fonte: ISRAEL, 2017b, p. 9

A primeira camada de robustez cibernética se refere à capacidade de organização dos processos que continuam operando apesar das ameaças cibernéticas diárias, repelindo e prevenindo a maioria dos ataques. Tendo em vista que é a camada básica de segurança cibernética, o país israelense estabeleceu uma meta de aumentar o nível geral de robustez cibernética com o fito de prevenir os danos e reduzir os riscos. Dessa maneira, para além dos esforços já empregados pela Resolução 2443, outros esforços foram adicionados para definir o nível de segurança cibernética do governo para, enfim, empreender soluções e procedimentos tecnológicos burocráticos específicos para aumentar a robustez geral do mercado (ISRAEL, 2017b, p. 10). Por fim, apesar desta camada aparentar não possuir relações com qualquer ato específico, ela é importante, pois garante condições ideais para atividades orientadas às ameaças, ficando sob auspício da segunda camada: resiliência (ADAMSKY, 2017. p. 117).

Figura 5 - Interconexão entre regulação do mercado de cibersegurança e orientação para o setor privado



Fonte: Israel, 2017b, p. 10

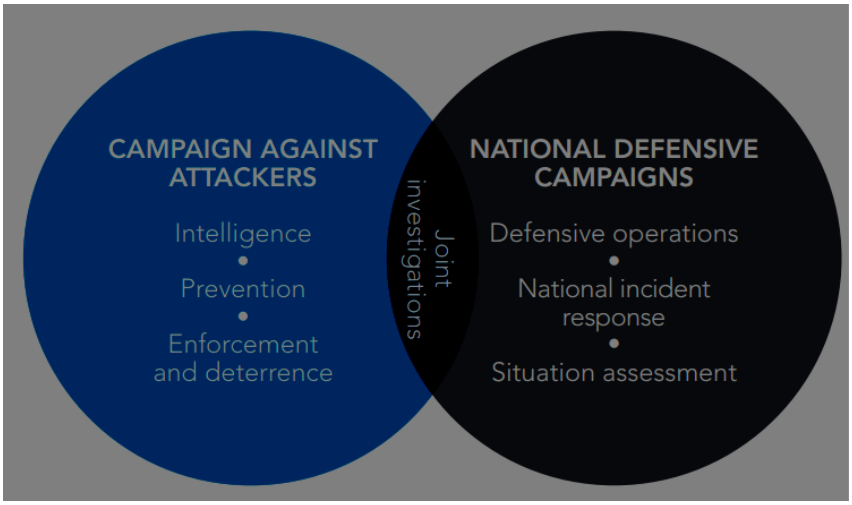
A imagem acima representa a interconexão entre regulação do mercado de cibersegurança (oferta) e orientação para o setor privado (demanda). Em relação à regulação do mercado, há, como oferta, profissionais cibernéticos, produtos e serviços de segurança e serviços tecnológicos, enquanto que na orientação para o setor privado, há, como demanda, orientação específica para infraestrutura crítica, normas obrigatórias em setores essenciais e promoção do conhecimento e conscientização por meio do setor privado. Esta interconexão entre ambos ajuda o governo a estabelecer a robustez necessária para, então, repelir e prevenir a maioria dos ataques cibernéticos por meio dos procedimentos tecnológicos burocráticos específicos. Estes procedimentos incluem atividades educacionais e de treinamento que, por sua vez, aumentam a conscientização e reduzem a probabilidade de um ataque bem-sucedido ou de danos substanciais (ADAMSKY, 2017. p. 117).

A camada Resiliência remete à capacidade sistemática de combater ataques cibernéticos antes, durante e após a ocorrência, de impedir que se espalhem e de reduzir os danos ﬠacumulativos ao país. Ou seja, é a capacidade de uma organização de se recuperar de ameaças e do Estado de evitar o potencial efeito nacional cumulativo desses ataques. A primeira diferença existente entre a primeira e a segunda camada é que a primeira está focada na redução dos ataques *a priori*, independentemente de qualquer evento em específico. Já a Resiliência pode ser obtida pelos processos, os quais incentivam o compartilhamento de informações e, portanto,

geram e divulgam informações valiosas que auxiliam as organizações durante os ataques cibernéticos. O envolvimento do Estado, separada ou conjuntamente com a organização afetada, cresce nessa camada. Todo este esforço é liderado pela NCSA, com apoio do CERT-IL à frente. Aqui, o CERT-IL trabalha avidamente com o setor privado tanto diretamente quanto por meio de centros cibernéticos setoriais que operam dentro do CERT (ADAMSKY, 2017, p. 117-118; ISRAEL, 2017b, p. 11).

Por fim, a camada de defesa representa as campanhas nacionais, tanto de natureza ofensiva quanto defensiva, vis-à-vis ameaças cibernéticas de alto nível. Essas campanhas ofensivas, de acordo com o documento, são necessárias contra ameaças graves de atacantes específicos e ricos em recursos que representam sério perigo para a nação. Esta ação implica um esforço nacional proativo (cibernético e cinético) por órgãos de aplicação da lei e segurança nacional contra iniciadores estatais e não estatais do ataque. Já as campanhas defensivas incorporam esforços com o objetivo de conter tais ataques e suas ramificações, acompanhado de esforços ativos para enfrentar as fontes das ameaças. Nesta camada, as contramedidas devem ser adaptadas ao invasor específico e à lógica estratégica geral dos fins, meios e formas de um ataque (ADAMSKY, 2017, p. 118; ISRAEL, 2017b, p. 12). As duas outras camadas, por sua vez, possuem uma natureza puramente defensiva, as quais possuem a dissuasão por negação [18] (ADAMSKY, 2017, p. 118; ISRAEL, 2017b, p. 13).

Figura 6 - Campanhas contra atacantes e campanhas defensivas nacionais



Fonte: Israel, 2017b, p. 12

[18] A dissuasão por negação é a dissuasão pelo medo do fracasso, a qual se concentra na defesa territorial e nas ameaças para derrotar a força de um invasor no campo de batalha (DALL'AGNOL; DUARTE, 2022, p. 104).

Em suma, esta abordagem de três camadas oferece uma solução geral, considerando as diferenças no nível de risco, a natureza da ameaça e o grau de clareza da ameaça ou ataque. Em relação às camadas, a camada de robustez é simplesmente a responsabilidade da organização e o Estado atua desempenhando um papel mais focado no incentivo e capacitação, enquanto que a Resiliência é uma associação entre Estado e organização, de modo a deixar a Defesa sob autoridade exclusiva do Estado. Apesar desta última possuir esse nome, ela é muito mais ofensiva por natureza, justamente por se concentrar no invasor e nos meios de ataque, o que permite a dissuasão por punição (ADAMSKY, 2017, p. 118; ISRAEL, 2017b, p. 13). A imagem acima representa esta associação. Há, portanto, um empreendimento conjunto entre as campanhas contra quem ataca, as quais incluem inteligência, prevenção e aplicação e dissuasão, com as campanhas defensivas nacionais, sendo estas operações defensivas, resposta nacional a incidentes e avaliação da situação.

O segundo capítulo, *The National Cyber Security Authority*, descreve a estrutura e a configuração do INCD. Como ela já foi abordada, novas informações serão breves. Esta organização é tida como a principal agência operacional voltada somente a assuntos relacionados à segurança cibernética. Ela serve como um centro de conhecimento nacional, um regulador cibernético primário e um centro operacional para gerenciar os ataques cibernéticos. Ademais, é a mais alta autoridade nacional para o planejamento estratégico de políticas cibernéticas, para a regulamentação de sua execução operacional em todo o governo e para a construção de capacidades cibernéticas a curto, médio e longo prazo. Para tanto, realiza campanhas defensivas integradas com agências de segurança nacional e policiais, reunindo, sob o mesmo teto, os órgãos que lideram os três vetores do CONOP – robustez, resiliência e defesa (ADAMSKY, 2017, p. 120; ISRAEL, 2017b, p. 15). A tabela abaixo demonstra as funções da NCSA nas três camadas.

Tabela 1 - Funções da NCSA de acordo com as três camadas

Robustez Agregada	Resiliência Sistêmica	Defesa Nacional
Regulamento de infraestrutura crítica	Compartilhamento de informações em todo o país	Gerenciar campanhas defensivas dentro do setor civil
Orientação de segurança (principalmente por meio de reguladores setoriais)	Assistência a organizações sob ataque	Coordenação entre agências
Centro nacional de conhecimento	Identificação e investigação de ataques	Avaliação da situação nacional

Regulação do mercado de segurança cibernética	Apoio aos Centros de Operações de Segurança (SOCs) setoriais	

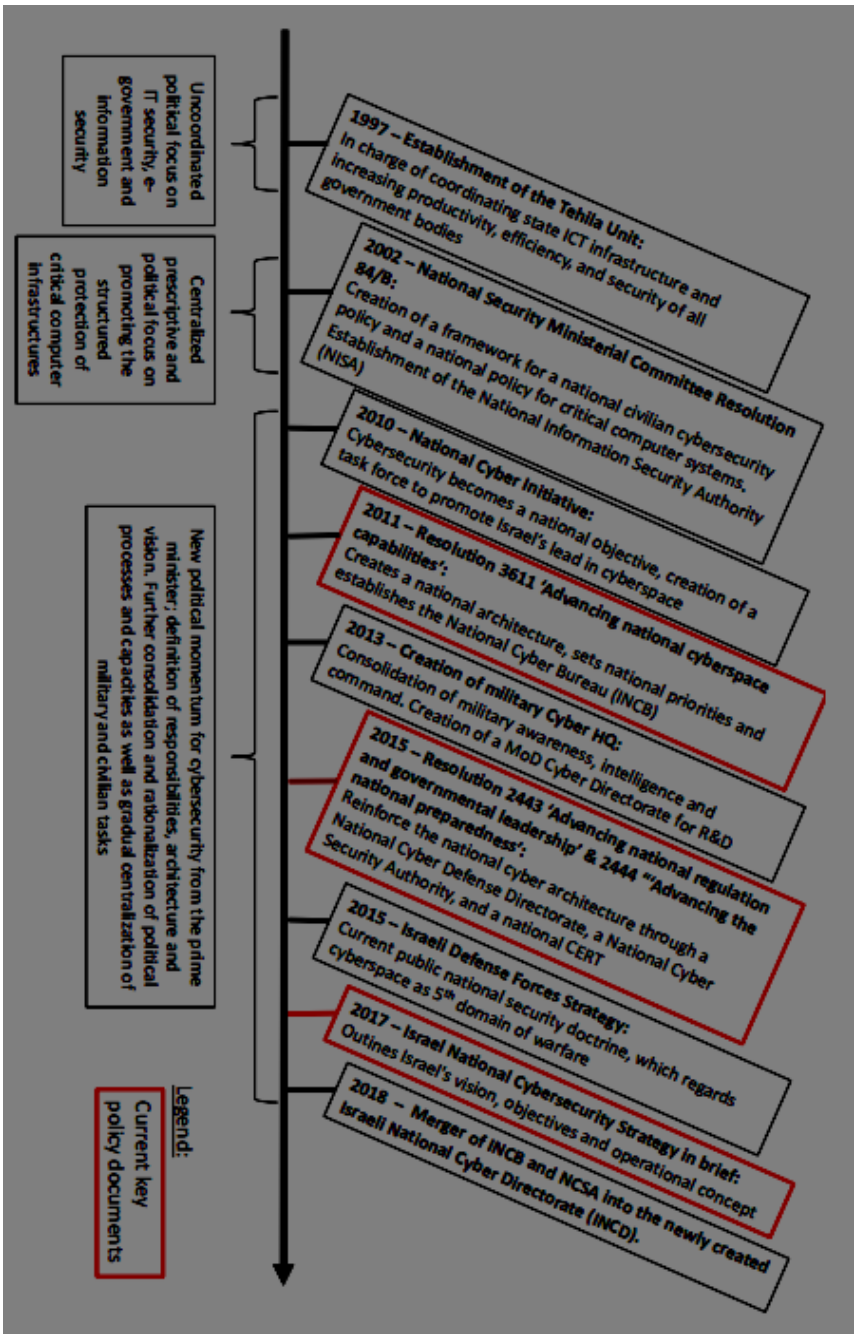
Fonte: ISRAEL, 2017b, p. 15, tradução nossa.

O terceiro capítulo, *Capacity Building*, compõe esforços designados a promover o ecossistema cibernético de Israel. Tendo em vista que a segurança cibernética é extremamente dependente da inovação para lidar com a abordagem dinâmica dos ataques cibernéticos, e que Israel tem sido líder nesta categoria e no conhecimento científico-tecnológico no âmbito da segurança cibernética, o país investe pesadamente em sua cultura de inovação e em seu capital humano único, de modo que emprega esforços de segurança nacional com o fito de criar um ambiente perfeito para a inovação cibernética (ADAMSKY, 2017, p. 118; ISRAEL, 2017b, p. 17).

Isto posto, há dois esforços principais: pesquisa, desenvolvimento e implementação de capacidades e tecnologias de segurança em nível nacional, incluindo plataformas de compartilhamento de informações seguras e eficientes, soluções que apoiam os esforços do Estado para expor, investigar e conter ataques cibernéticos, bem como processos cibernéticos robustos e serviços de segurança centralizados; e fortalecimento da base nacional de ciência e tecnologia em cibernética, promovendo a inovação industrial, apoiando a pesquisa acadêmica (incluindo o estabelecimento de seis centros de pesquisa nas principais universidades de Israel), aprimorando o capital humano da nação no campo cibernético e promovendo um ecossistema para o enriquecimento mútuo. Este inclui o projeto exclusivo *CyberSpark* – um ecossistema de segurança cibernética concentrado composto por *startups* israelenses, empresas globais, academia e centros de segurança cibernética civis e militares – todos a uma curta distância uns dos outros (ISRAEL, 2017b, p. 17). O capítulo reflete projetos formulados por *policy makers* de políticas cibernéticas israelenses durante os últimos anos para garantir que Israel assegure sua posição como uma das principais potências cibernéticas do mundo (ADAMSKY, 2017, p. 118).

Enfim, com o objetivo de agilizar o trabalho, em 2017, foi estabelecida a Resolução 3270, o qual fundiu a NCSA e o INCB, criando o INCD para ser responsável por todos os aspectos da defesa cibernética na esfera civil, desde a formulação de políticas e construção de poder tecnológico até a defesa cibernética operacional, como já detalhado no capítulo anterior (TABANSKY, 2020, p. 53).

Figura 7 - Cronograma geral dos documentos governamentais relacionados ao ciber



Fonte: CSS, 2019, p. 26.

A figura 7 acima expõe, cronologicamente, os documentos considerados importantes no que se refere ao desenvolvimento do poder cibernético em Israel. Os que estão em vermelho são os documentos-chave que ainda são utilizados e foram tratados durante o decorrer deste capítulo.

Em suma, Israel possui uma política de defesa nacional relativamente robusta, apesar de não possuir uma estratégia formal de segurança nacional. Em geral, as forças armadas israelenses possuem uma mentalidade *ad hoc* e nunca codificaram conceitos de segurança e doutrina militar de forma escrita antes do *IDF Strategy*. Aliás, este comportamento faz jus à utilização dos antigos princípios propostos por Ben Gurion nos primeiros anos de Israel. Nesta época, a cultura de guerra israelense foi afetada pela preferência por guerras curtas em solo inimigo, de modo que a estratégia defensiva, o status quo e as táticas ofensivas tornaram-se as normas regulatórias da cultura estratégica israelense. Entretanto, e por conta da alteração dos considerados inimigos, estas táticas não podem mais ser utilizadas por completo.

Atualmente, as principais ameaças que Israel enfrenta advém de guerras irregulares e assimétricas, incluindo guerra cibernética e mísseis balísticos. Isto é, com exceção do Irã, a ameaça hoje é de atores não estatais. Apesar disso, a tecnologia sempre pareceu, a Israel, vital. Como uma nação que depende fortemente de tecnologia avançada, Israel é vulnerável a ataques cibernéticos e entende que a defesa cibernética é vital para garantir a continuidade das operações das organizações nacionais. Para melhor compreender esta evolução e a importância da tecnologia, o próximo capítulo abordará a doutrina militar israelense.

4 DOUTRINA

Neste capítulo, tratar-se-á do conceito de doutrina militar e de grande estratégia, as quais serão entendidas a partir dos termos utilizados por Posen (1984). Consoante a isto, abordar-se-á como o contexto histórico e os traços culturais convergiram a fim de moldar a doutrina israelense e garantir a sobrevivência do Estado que, inicialmente, sofria uma desvantagem quantitativa. Desse modo, apresentar-se-ão alguns pilares da doutrina militar israelenses, bem como a evolução e alteração dos que são considerados inimigos do Estado israelense. Por fim, identificar-se-ão três teorias, demonstradas por Sagan (2000), que focam em diferentes explicações plausíveis para a escolha de doutrinas militares específicas.

A Doutrina Militar é um elemento de suma importância da política de segurança nacional ou grande estratégia de um Estado. A grande estratégia é uma cadeia político-militar que compõe os meios e fins sobre os quais a segurança deve ser proporcionada. Desse modo, a grande estratégia deve identificar as possíveis ameaças e, por conseguinte, as soluções e recursos tanto políticos quanto econômicos e militares para combatê-las. É necessário, então, o estabelecimento de prioridades entre as ameaças e soluções devido ao ambiente anárquico em que o Estado se encontra, tendo em vista que os recursos nacionais são escassos. Assim, o Estado deve ter um conjunto de regulamentações de modo a especificar como as forças militares nacionais (e, portanto, a cooperação entre os diferentes tipos de forças) deverão ser estruturadas e utilizadas contra ameaças ou a favor de oportunidades, possuindo, preferencialmente, modos de cooperação especificados entre os diferentes gêneros de força (POSEN, 1984, p. 13). Para Posen (1984, p. 13), a doutrina militar é definida como um subcomponente da grande estratégia que se relaciona diretamente com os meios militares.

Os Estados e, portanto, suas doutrinas militares, dispõem de um modo preferido de um grupo de serviços, um único serviço ou um subserviço para travar guerras. Esta preferência é o reflexo do entendimento dos oficiais militares e, em menor grau, dos líderes civis, sobre o que é (ou não) possível e necessário no âmbito militar. O julgamento pelos militares é baseado na tecnologia militar, na geografia nacional, nas capacidades do adversário e nas habilidades da própria organização militar. Consoante a isto, a doutrina militar reflete nas forças que são adquiridas pela organização militar do país, ou seja, é possível descobrir e analisar a doutrina militar de qualquer país ao se basear no inventário de armas que o mesmo possui. Nesse sentido, é normal que os Estados foquem em um tipo de força em detrimento de outra por diversas razões, podendo ser por questões geográficas, tecnológicas, econômicas ou políticas (POSEN, 1984, p. 14).

De modo geral, as operações militares podem ser divididas em três categorias: ofensivas[19], defensivas e dissuasivas. A primeira visa desarmar um adversário ao destruir suas forças armadas. A segunda aspira em impedir que o adversário alcance o objetivo almejado, enquanto que a última propõe punir um agressor ao aumentar o custo da batalha ao adversário (POSEN, 1984, p. 14).

Isto posto, a doutrina militar é deveras importante por duas grandes razões: política e segurança de um Estado. De modo geral, as doutrinas adotadas pelo Estado, incontestavelmente inseridas dentro do sistema existente, afetam a qualidade da vida política internacional. A depender do caráter da mesma (ofensiva, defensiva ou dissuasiva), elas podem afetar a probabilidade e a intensidade tanto das corridas armamentistas quanto das guerras que podem ser travadas. Isto é, o caráter da doutrina afeta a percepção e reação dos Estados em relação aos outros. Ademais, a doutrina pode afetar a segurança do Estado que a possui, pois a mesma tem o potencial de prejudicar os interesses securitários estatais caso não esteja integrada aos objetivos políticos da grande estratégia, ou seja, caso a doutrina militar não seja capaz de fornecer ao líder do Estado as ferramentas adequadas e necessárias à busca de um objetivo específico. Consoante a isto, quando a doutrina militar não é capaz de acompanhar as mudanças nos âmbitos políticos, tecnológicos e militares, ou responder e se adaptar às mudanças políticas, às capacidades dos adversários e à tecnologia militar disponível, quando não tem capacidade suficiente de inovar em meio ao ambiente internacional anárquico e dinâmico, tal doutrina pode levar o Estado à derrota (POSEN, 1984, p. 16).

Posen (1984), portanto, parte de uma análise realista, em que os Estados, inseridos no meio anárquico, devem se preocupar com sua defesa e, consequentemente, observar seus vizinhos de modo cauteloso, tendo em vista que tanto a doutrina quanto a capacidade militar de um Estado não são difíceis de esconder, ao contrário das intenções por trás. Desse modo, uma arma adquirida para defesa pode ser interpretada como (também) para atacar, de modo que, o que um Estado pode considerar como sendo provedor da sua segurança, outros podem entender a mesma situação como a diminuição da sua. Percebe-se, portanto, o dilema de segurança concomitante com a doutrina militar: quanto mais ofensiva for uma doutrina, mais tensão será percebida pelos outros Estados (POSEN, 1984, p. 16-17).

[19]Um exemplo de doutrina militar ofensiva é a já conhecida Blitzkrieg, ou seja, o método de combate utilizado para conquistar a vitória de maneira rápida. Desde pouco depois de sua criação, Israel se utiliza deste método em aspectos operacionais. Apesar das inovações tecnológicas, o método de combinar diferentes forças para a guerra de alta velocidade permaneceu idêntico (POSEN, 1984, p. 14).

Outrossim, um princípio da doutrina ofensiva é que um primeiro ataque eficaz pode terminar uma guerra de forma rápida, barata e bem-sucedida. Aqui, há a crença de que as doutrinas ofensivas são superiores às defensivas, o que faz com que os Estados se sintam ameaçados quando há qualquer aumento nas capacidades militares de outros. Desse modo, a defesa é tida como uma desvantagem, de maneira que a iniciativa na guerra não deve ser concedida ao adversário, principalmente se a doutrina do mesmo é reconhecidamente ofensiva (POSEN, 1984, p. 18-20). Já em relação às doutrinas defensivas e dissuasivas, as mesmas tendem a entrar em guerras mais longas que exigem forças menores. Sendo assim, elas colocam o Estado em uma posição vulnerável a ataques inimigos, mas quando apoiadas por uma conduta de força apropriada, devem limitar reações exageradas e percepções errôneas (POSEN, 1984, p. 24).

Em suma, o grande objetivo da doutrina militar é garantir a sobrevivência do Estado. Caso a grande estratégia esteja em discordância com os fins políticos do país, a possível guerra e derrota podem ocasionar seu fim. Isto significa que ela busca também garantir a segurança estatal em tempos de paz, de modo a ser congruente com as capacidades econômicas, políticas e humanas do Estado. Se bem-sucedida, ela poderá dissuadir seus inimigos de atacar e minimizar consequências de cada tipo de doutrina militar. Já em tempos de guerra ou crise, a doutrina militar terá seus aspectos qualitativo e quantitativo, fornecidas em tempo de paz, postos à prova (POSEN, 1984, p. 25).

A grande estratégia, portanto, remete a uma cadeia em que os fins são políticos e os meios, militares. Nesse sentido, a eficácia ou não é extremamente dependente da dimensão em que esses fins e meios estão inter-relacionados. Em certo ponto, essa integração político-militar é proveitosa, já que o uso da força e da ameaça são fundamentais no ambiente anárquico, apesar de não serem destituídos de algum custo (POSEN, 1984, p. 25). Portanto, há dois princípios fundamentais da grande estratégia: a integração política securitária integrada e a perspectiva de longo alcance (DROR, 2006, p. 854). Outrossim, a inovação ou estagnação na doutrina militar podem afetar esta integração e, portanto, a probabilidade de vitória ou derrota, ou seja, pode afetar a segurança nacional, tendo em vista que impactam se os meios estão ou não disponíveis para as políticas nacionais (POSEN, 1984, p. 29-30). Por vezes, militares podem inovar de maneiras discordantes dos objetivos políticos estatais, mas, por vezes, podem até não conseguir inovar.

Ademais, uma das principais transformações na guerra moderna e na estratégia remete à tecnologia. A mesma conseguiu não somente ocupar um papel importante, mas também seus impactos no pensamento militar podem ser claramente identificados: passamos a ter a tecnologia como a principal razão para o surgimento do nível operacional de guerra, como a criadora

da dimensão aérea e posteriormente do espaço sideral e do ciberespaço, por exemplo. A tecnologia não foi somente algo que foi incorporado, mas também algo que está envolvido e aprofundado em questões operacionais. Por exemplo, tem-se que a tecnologia acabou por ampliar a guerra no sentido de que houve um afastamento da guerra e da sociedade do campo de batalha direto (KOBER, 2015, p. 138-139). Tanto a inovação quanto a estagnação na doutrina militar podem afetar a segurança nacional, seja por meio da integração ou pela probabilidade de vitória ou derrota. Atualizar uma doutrina leva tempo e desorganiza a força militar (POSEN, 1984, p. 29-31).

Como já apontado, os princípios e as ideias primordiais que sustentam, até hoje, a doutrina de segurança israelense, tomaram forma nos anos de 1950. Esta doutrina é composta por uma doutrina oral e, em partes, é formalmente escrita em leis, decisões do *Knesset*, ordens, diretrizes do Alto Comando e do Estado-Maior e manuais de treinamento utilizados pelas diversas áreas das FDI. Princípios que constam na doutrina foram estabelecidos a partir destas fontes, alicerçados no contexto geopolítico, econômico e societário (TAL, 2000, p. vii-viii; FREILICH, 2018b, p. 14).

No caso de Israel, a doutrina de segurança nacional foi forjada a partir de uma desvantagem nas relações de força. Por tal motivo, Israel optou por uma defesa baseada em riscos calculados, sendo um dos mais evidentes o fato das FDI serem estruturadas principalmente para a ofensiva, em detrimento das capacidades defensivas. Outro exemplo é a alta dependência do alerta avançado, proporcionado pela inteligência, em relação ao desenvolvimento das ameaças militares possíveis (TAL, 2000, p. 37).

Israel se torna um caso interessante pois seu papel antecedeu, lógica e cronologicamente, a sua criação de fato. Devido ao sionismo como movimento político, Israel foi pensando, por seus líderes, para ser responsável por proteger e amparar todo o povo judeu, vítima do antissemitismo e perseguições por todo o mundo. Este fato, em maior ou menor grau, influencia tanto na doutrina quanto na estratégia de segurança nacional israelense. Sua localização e seus vizinhos mostraram a Israel que o fim do conflito, instaurado a partir de sua criação, por meios militares, seria apenas possível aos árabes. Isto é, a doutrina de defesa israelense teve por base a suposição de que nunca seria capaz de encerrar o conflito com seus vizinhos por meios militares (TAL, 2000, p. 39-40; FREILICH, 2018b, p. 22).

Desde a sua criação, o conflito instaurado englobou aspectos diplomáticos, militares, territoriais, econômicos, ideológicos, nacionais e religiosos. Por várias décadas, os países ára-

bes, de forma geral, recusaram reconhecer a existência de Israel. Atualmente, o cenário se encontra um pouco mais favorável a Israel, em que alguns acordos foram realizados com seus vizinhos. Após seis guerras, confrontos e violência constante, incluindo os considerados atos terroristas até ameaças de armas de destruição em massa, fazem parte do ambiente em que Israel se encontra. As oscilações do grau das hostilidades, exigem uma vigilância constante (FREILICH, 2018b, p. 15).

A desvantagem quantitativa de Israel não recai somente sobre a população, mas também em recursos e materiais. Além disso, a falta de profundidade estratégica não garante, ao país, a possibilidade de optar entre defesa rígida e flexível, ao contrário dos países árabes (TAL, 2000, p. 41). Sendo assim, as FDI aplicaram uma estratégia de defesa rígida, capaz de manter o território, em vez de uma mais flexível, para destruir forças e forçar uma decisão militar (TAL, 2000, p. 60). Nestas circunstâncias, as várias vitórias israelense não asseguraram, necessariamente, a realização de outros objetivos nacionais. Nesse sentido, Israel se preparou para o longo prazo e formulou uma doutrina de segurança nacional que fosse realista e direta, de modo que as FDI foram engendradas com o objetivo de lutar continuamente por muitos anos (TAL, 2000, p. 41-42). De acordo com Tal (2000, p. 42):

> *The doctrine, formulated in Israel's formative years, immediately after its appearance in the Middle Eastern arena, was distinguished by analytical and critical thought of a creative and generalized nature and of a high level of abstraction. The architects of this approach pinpointed the basic, permanent strategic factors that characterized Israel's circumstances, defined threats and constraints, and determined the goals and aims that could be adopted within the limits of its power*[20].

Outrossim, um dos princípios de combate das FDI remete à necessidade da guerra ser levada de forma rápida ao território do inimigo, justamente por conta da sua carência de profundidade estratégica. Com isto, Israel é capaz de poupar seus civis e preservar sua infraestrutura e bens nacionais, de modo que o caráter ofensivo é uma das características das FDI. Além disso, destaca-se a necessidade da guerra ser rápida e curta, justamente pela incapacidade econômica, social e militar de Israel arcar com guerras longas (TAL, 2000, p. 70-71).

O pensamento estratégico israelense, desde o seu primórdio até hoje, é baseado na crença de que os países árabes, e agora países como o Irã e atores não estatais, como Hamas e Hezbollah, buscam a sua destruição. Certamente, a maioria das decisões remetentes à segurança

[20] A doutrina, formulada nos anos de formação de Israel, imediatamente após o seu aparecimento na arena do Médio Oriente, distinguiu-se por um pensamento analítico e crítico de carácter criativo e generalizado e de elevado grau de abstracção. Os arquitetos dessa abordagem identificaram os fatores estratégicos básicos e permanentes que caracterizaram as circunstâncias de Israel, definiram ameaças e restrições e determinaram as metas e objetivos que poderiam ser adotados dentro dos limites de seu poder (TAL, 2000, p. 42, tradução nossa).

nacional e ao discurso público é fortemente influenciada pelo medo existencial, conhecido como “complexo de Massada” ou “síndrome do holocausto” (FREILICH, 2018b, p. 15-16).

Militarmente falando, a estratégia israelense é estruturada de forma articulada, delineada para aumentar as margens de segurança. Os pilares que sustentam esta estrutura são interdependentes e, por vezes, sobrepostos, de modo que, ao mesmo tempo em que se sustentam, podem compartilhar atributos, enquanto alguns são projetados para se tornarem ativos se e quando seus predecessores falharem. Os pilares da estrutura são: dissuasão; profundidade estratégica artificial; aviso prévio; vantagem qualitativa; e uma estrutura e doutrina de força ofensiva (MEROM, 2003, p. 212).

O primeiro pilar da estratégia militar israelense é composto pela dissuasão, em grande parte porque é a maneira mais econômica de usar a força, mas também porque Israel não poderia alcançar seus objetivos políticos através do uso da força militar. A dissuasão, projetada para convencer os estados árabes de que seus esforços para destruí-lo eram fúteis, tornou-se a peça central da doutrina clássica, o conceito organizador que definia situações, objetivos, conquistas e fracassos. A dissuasão israelense deveria ser alcançada tanto por meio de guerras em grande escala quanto por confrontos militares limitados em andamento, como ataques de retaliação e operações especiais, baseando-se na negação, destruindo as forças atacantes e conquistando território. Isto posto, por conta desta dissuasão, junto com os levantamentos sobre a guerra, Israel aspira a manter uma superioridade militar geral, particularmente no domínio ofensivo (MEROM, 2003, p. 212; FREILICH, 2018b, p. 23).

Em relação à profundidade estratégica artificial, Israel definiu sua fronteira estratégica na forma de “linhas vermelhas,” as quais vão além de suas fronteiras soberanas, incluindo os territórios ocupados desde a guerra de 1967. Essa profundidade é responsável por permitir que Israel observe as mudanças em territórios árabes e, portanto, das suas intenções, ao mesmo tempo em que fornece tempo de mobilização e aumenta a chance de mover a batalha para fora de seu território. Nesse sentido, Israel considera imperativo a transferência do combate ao território inimigo o mais rápido possível, o que condiz com a superioridade das IDF em batalhas de manobra de alto ritmo (EILAM, 2021, p. 246; MEROM, 2003, p. 212-213; FREILICH, 2018b, p. 27).

O subsequente pilar compreende os sistemas de inteligência e de alerta avançado. A coleta e análise de inteligência e sistemas de alerta precoce são consequências diretas da falta de profundidade estratégica, da incapacidade de manter mobilizações frequentes e estendidas de seus militares, do peso crítico do tempo e da capacidade árabe de mudar rapidamente de

operações defensivas para ofensivas. Desse modo, o conceito de aviso prévio ocupa um lugar de suma importância na doutrina de defesa israelense. Concomitantemente, se o pilar da dissuasão falhasse, este pilar deveria alertar Israel para hostilidades iminentes e fornecer tempo suficiente para a mobilização militar (MEROM, 2003, p. 213; FREILICH, 2018b, p. 23-24).

O quarto pilar remete ao desenvolvimento dos multiplicadores de força com forte ênfase na vantagem qualitativa. Devido à sua desvantagem quantitativa em diversas áreas, Israel teria de utilizar seus recursos limitados com o fito de competir qualitativamente e, assim, combater o desequilíbrio. Normalmente, tem-se como vantagem qualitativa a superioridade tecnológica que compensa a inferioridade quantitativa, porém, no nível militar, isso significa melhor treinamento, comando e controle, desenvoltura e, principalmente, superioridade aérea. Sendo assim, tanto as capacidades operacionais e quanto as tecnológicas de Israel possibilitariam que o mesmo número de aeronaves realizasse mais missões, que tanques alcançassem uma porcentagem maior de acertos e que as forças terrestres de Israel conduzissem guerras de maior mobilidade, ao mesmo tempo em que aumentaria a credibilidade de sua dissuasão (MEROM, 2003, p. 213; FREILICH, 2018b, p. 24-25).

Dessa maneira, Israel, ao procurar manter uma vantagem qualitativa e, em maior ou menor grau, uma quantitativa, convencendo seus inimigos de que não podem eliminar Israel ou alcançar objetivos territoriais. Aliás, Israel investe pesadamente em tecnologia não somente para conquistar essa vantagem, mas sobretudo porque serve a um propósito político. O conceito de "poucos contra muitos", ou qualidade sobre quantidade, traz implicações para a política socioeconômica de Israel, pois ajuda a reduzir a dependência do país do apoio estrangeiro e, portanto, aumenta sua liberdade de manobra militar e política (MEROM, 2003, p. 213; FREILICH, 2018b, p. 24-25).

Por fim, o último pilar corresponde à doutrina militar e à estrutura de força das FDI, formulados a partir da falta de profundidade estratégica, a vulnerabilidade da economia à mobilização de longo prazo, a sensibilidade cultural às baixas, dúvidas sobre o poder de permanência e o risco de intervenção internacional precoce durante a guerra. Isto é, a doutrina militar israelense está preocupada com a economia de energia e de tempo e com a velocidade da ação. Esta doutrina clássica era fundamentalmente defensiva estrategicamente (para garantir a sobrevivência do Estado), mas ofensiva operacionalmente (para derrotar seus inimigos de forma rápida, decisiva e econômica) (MEROM, 2003, p. 214-215; FREILICH, 2018b, p. 26-28).

Deste modo, a escalada tática e estratégica são marcas da forma israelense de fazer a guerra. Há, de fato, uma preferência israelense pela escalada, incrustada em um "culto da ofensiva" que é difundido entre os oficiais israelenses. Seria por meio da ofensiva que Israel poderia

determinar o momento, o ritmo, a localização e o curso geral da batalha, transferir a batalha para o território inimigo, trazer a vantagem qualitativa de Israel e facilitar conquistas militares rápidas. O método defensivo, por sua vez, era visto como uma guerra por atrito, de modo que exigiria que Israel dividisse suas forças em lugares diferentes, enquanto o inimigo seria capaz de concentrar suas forças (MEROM, 2003, p. 214-215; FREILICH, 2018b, p. 26-28).

Em suma, os principais elementos desta estratégia defensiva executada ofensivamente são: a guerra ofensiva e de manobra móvel, transferência da batalha para o território inimigo, preempção (mobilização das reservas israelenses logo que a ameaça fosse identificada, antecipando-se ao inimigo para impedi-lo de usar planos de batalha predeterminados, interromper a mobilização e concentração de seus forças e neutralizar suas vantagens quantitativa), defesa inflexível (projetada para manter um posicionamento defensivo avançado permanente no campo, forçando o inimigo a dedicar forças e atrasar e interromper a manobra inimiga) e guerras curtas (MEROM, 2003, p. 214-215; FREILICH, 2018b, p. 26-28).

Todavia, o cenário estratégico mudou significativamente desde que a doutrina clássica de defesa israelense foi formulada. A dissuasão, no pensamento estratégico israelense, não foi projetada para impedir a eclosão de hostilidade, mas sim para prolongar o tempo entre os conflitos, em um sentido mais amplo de continuidade. Sendo assim, o impacto dissuasório das FDI é reforçado não somente pelas vitórias, mas sobretudo pelas operações entre guerras, as quais fazem parte das atividades defensivas constantes de Israel. Tais atividades incluem medidas de segurança, represálias, ataques de comandos, operações especiais em território inimigo e demonstrações de destreza em tecnologia militar, as quais são empregadas para aumentar o sentimento de frustração no campo adversário e aumentar o valor de dissuasão do FDI (TAL, 2000, p. 52; FREILICH, 2018b, p. 166).

A discussão atual é voltada para conflitos de baixa intensidade. Entretanto, o conceito de dissuasão serviu melhor às guerras convencionais contra os países árabes do que serve atualmente. A ascensão de atores não-estatais, com grande foco no Hezbollah e Hamas, e a consequente mudança na natureza dos ataques que Israel enfrenta, fizeram com que o tal conceito de dissuasão se tornasse problemático. A grande diferença entre estes atores e os países árabes é que o primeiro busca uma política estratégica de desgaste. Além disso, estes atores não-estatais enfrentam diretamente a preferência israelense por guerras curtas e decisivas, tendo em vista que promovem uma guerra de atrito de décadas (FREILICH, 2018b, p. 167-168).

De modo geral, a dissuasão israelense tem sido uma combinação de fracasso e sucesso. Apesar de ter sido efetiva contra os países árabes, atualmente foi incapaz de impedir que o

terrorismo se tornasse uma ameaça estratégica, seja contra os próprios atores não-estatais, seja com os países que lhes forneceram refúgio, armas e outras formas de assistência. A dissuasão específica (projetada para evitar grandes operações militares, especialmente ataques surpresa, ao estabelecer várias "linhas vermelhas", cuja violação provocaria uma resposta israelense) amenizou, de certa forma, o comportamento árabe, mas não impossibilitou a eclosão de guerras, grandes operações ou disparos de foguetes e mísseis contra Israel. Já a dissuasão estratégica (projetado para evitar uma guerra geral ou em grande escala, convencendo o adversário de que os custos e riscos superariam os benefícios) impediu, efetivamente, qualquer Estado árabe de atacar Israel desde 1973, mas levou seus adversários estatais e não-estatais a promover respostas assimétricas um tanto quanto problemáticas. Diante destas respostas, Israel parece adotar paulatinamente a abordagem da negação para a dissuasão baseada em punições (FREILICH, 2018b, p. 170-174).

A adesão a uma estratégia ofensiva permaneceu enraizado à estratégia israelense, conforme publicado no *IDF Strategy*, apesar dos embates inconclusivos com Hezbollah e Hamas. Recentemente, os fatores passaram a forçar um movimento de repensar o papel da defesa na doutrina militar. Por exemplo, a própria mudança na natureza da guerra fornece oportunidades para operações defensivas, especialmente aquelas adequadas às capacidades tecnológicas avançadas. Desse modo, a abordagem defensiva se tornou mais palpável, a partir das limitações da dissuasão israelense em relação ao Hezbollah e ao Hamas, bem como a conquista territorial não ser mais uma estratégia viável ou desejada. Estes conflitos irregulares, em geral, demonstram um nítido declínio na ofensiva israelense como ferramenta para atingir objetivos estratégicos. Assim, o aprimoramento da defesa reduz o número de possíveis baixas (principal razão para as respostas e escaladas de Israel atualmente) e de danos potenciais à infraestrutura crítica, possibilitando mais tempo e flexibilidade para que os líderes possam tomar decisões (EILAM, 2021, p. 252; FREILICH, 2018b, p. 183-184).

De modo geral, quando o assunto são as guerras irregulares, a vantagem quantitativa de Israel continua a ser extremamente importante, apesar de possuir um papel parcial. Mesmo assim, manter a vantagem qualitativa continua sendo um princípio e foco primário da doutrina de defesa de Israel, embora as mudanças transformaram esta manutenção exponencialmente mais difícil. Concomitante a isso, Israel foi capaz de desenvolver rapidamente, econômica e cientificamente, sua capacidade militar por meio do seu conhecimento tecnológico, principalmente ao desenvolver respostas de alta tecnologia às ameaças, tornando-se líder mundial em formas avançadas de guerra. Isto posto, os adversários de Israel reconheceram sua incapacidade de competir com a superioridade qualitativa israelense e, alguns, por conseguinte, recorreram a

respostas irregulares de baixa tecnologia, destinadas a neutralizar tais vantagens tecnológicas (FREILICH, 2018b, p. 186-187).

A transferência da guerra para o território inimigo se tornou ainda mais complicado, pelo menos em terra, justamente por conta das alterações estratégicas e operacionais dos novos inimigos e da natureza da guerra. Nesse sentido, a partir do princípio de que nenhum inimigo deve conquistar o território (ou partes dele), Israel é obrigado a manter sua defesa inflexível. Por fim, este novo tipo de ameaça reduziu a capacidade israelense de conduzir uma guerra móvel rápida, o qual levou a uma guerra mais prolongada, colidindo com o princípio de guerras curtas (FREILICH, 2018b, p. 187-191).

Em suma, Irã e Hezbollah são as principais ameaças que Israel enfrenta atualmente. O Irã é o adversário estatal mais complexo. Além disso, o *home front* e a retaguarda militar israelense são, agora, o campo de batalha principal. Isto posto, a dissuasão e os pilares estratégicos clássicos podem não ter mais o efeito desejado, tendo em vista os combates assimétricos que se instauraram. Dessa maneira, os adversários de Israel persistirão em usar respostas assimétricas na forma de terrorismo intensificado e programas de armas de destruição em massa. Nesta situação, portanto, Israel adota uma postura mais defensiva, a qual passou a ser definida como um quarto pilar estratégico e fez com que o país adotasse barreiras físicas (FREILICH, 2018b, p. 334-337).

Enfim, a doutrina militar de um país são planos sobre quando e como a força militar deve ser empregada. Por este motivo, as doutrinas militares são diferentes a depender do país, podendo ser mais ofensiva ou defensiva em seu caráter, além de como definem as forças militares, inimigos e capacidades industriais e, assim, quais precisam ser destruídos durante uma guerra. Há três teorias que focam em diferentes explicações plausíveis para a escolha de doutrinas militares específicas (SAGAN, 2000, p. 17).

A primeira se refere à teoria da organização, a qual examina os processos de tomada de decisão das organizações militares e os interesses dos oficiais. Nesta teoria, é possível identificar duas características comuns das organizações militares que levam a padrões nos tipos de doutrinas militares preferidas. Em primeiro lugar, as organizações militares não são racionais por inteiro e utilizam procedimentos simplificadores com o fito de entender e responder à incerteza do sistema internacional. Em segundo lugar, os líderes e membros das organizações militares estão preocupados com a segurança do Estado, bem como a proteção da sua própria força organizacional, autonomia e prestígio (SAGAN, 2000, p. 18).

Outrossim, o argumento da teoria da organização é de que estas características convergem em uma preferência pela doutrina militar ofensiva. Sendo assim, os interesses funcionais de uma organização e suas rotinas fazem com que os oficiais militares mantenham certos preconceitos enraizados a favor de doutrinas ofensivas, as quais diminuem a incerteza organizacional, uma vez que os militares desenvolverão planos de guerra para coordenar operações e, posteriormente, implementá-los, em vez de reagir aos planos do inimigo. Isto posto, a doutrina ofensiva requer forças maiores e, por conseguinte, o desenvolvimento desta doutrina pode gerar um aumento no orçamento e no tamanho da organização militar (SAGAN, 2000, p. 18).

A teoria da organização também proporciona previsões sobre cinco aspectos particulares da doutrina militar. Primeiramente, a partir da perspectiva organizacional, há uma forte tendência dos militares optarem pelas guerras preventivas, as quais dependem do poder militar para derrotar o adversário de forma decisiva. Ademais, os militares são menos inclinados a levar em consideração fatores políticos, pois estes podem arguir contra a guerra preventiva, bem como a opinião de civis ou de governos aliados, tendo em vista que os formuladores de guerra são treinados para se concentrar em ações operacionais, eficiência e a busca pela vitória militar (SAGAN, 2000, p. 19).

Segundo, os militares são céticos em relação à capacidade de controlar a escalada e, portanto, possuem interesses em negar que as autoridades civis se intrometam no planejamento operacional. Nesse sentido, os oficiais sustentam a opinião de que a força deve ser empregada ou de maneira decisiva ou não ser usada de todo. Terceiro, o desígnio no que tange às operações decisivas muito provavelmente fará com que os oficiais defendam em larga escala, em que uma retaliação antecipada seria preferível ao segundo ataque. Esta propensão pode levar os oficiais a rejeitar as opções de uso limitado, em tempos de paz, e à execução de tais opções em guerra (SAGAN, 2000, p. 20-21).

Em quarto lugar, os oficiais preferem armas e doutrinas que gerem resultados mensuráveis de maneira fácil, ao passo que procuram reduzir a incerteza no planejamento da guerra. Por último, as organizações militares normalmente apoiam a continuidade de suas missões tradicionais e a preferência em se antecipar ao inimigo, desencorajando o uso de operações inovadoras para reduzir a vulnerabilidade (SAGAN, 2000, p. 21-22).

A teoria organizacional não somente identifica preconceitos e preferências militares, mas também abarca três formas de como esses interesses influenciam a política estatal. Em primeiro lugar, as organizações militares possuem a capacidade de determinar diretamente a doutrina dos Estados que não possuem os rudimentos do controle civil sobre os militares. Em segundo lugar, as organizações civis normalmente não estão preparadas e tampouco equipadas

para influenciar os planos e procedimentos de guerra, mesmo em Estados que detém o controle civil oficial das forças armadas. Aliás, esta vertente pode aceitar que a influência militar em relação às doutrinas e às estratégias, em maior ou menor grau, é maior durante o período de paz, quando os incentivos para a supervisão civil são reduzidos. Porém, esta supervisão é limitada pela complexidade do planejamento militar, de modo que a intervenção civil pode ser extremamente restringida em períodos de crise ou de guerra, pois não há tempo o suficiente para alterar os planos ou retreinar as forças armadas (SAGAN, 2000, p. 22-23 e 30).

Em último lugar, se os civis forem informados dos planos militares, os oficiais, naturalmente, exercerão pressões fortes com o fito de manter as preferências doutrinárias. Além disso, os teóricos desta vertente conjecturam que grande parte dos líderes organizacionais valoriza a autonomia ou o território tanto quanto, ou até mais, que ter recursos à disposição. A autonomia é importante pois garante que os membros da organização determinem quais missões devem ser cumpridas. Assim, os oficiais devem pressionar fortemente para maximizar sua autonomia e se opor a quaisquer inovações técnicas ou processuais que tirem de suas mãos o poder de tomada de decisão operacional. Na medida em que preferências organizacionais determinam a política estatal em novos estados proliferantes, seja porque os militares estão no poder e, portanto, tomam decisões importantes por conta própria ou porque exercem forte influência por meio de manobras políticas e burocráticas, espera-se um sistema de comando mais descentralizado (SAGAN, 2000, p. 37).

Em suma, a teoria da organização propõe que os oficiais militares possuem uma forte tendência em favorecer doutrinas ofensivas, guerras preventivas e decisivas, de modo que provavelmente apoiarão doutrinas de direcionamento de forças contrárias e podem não constituir forças de segundo ataque (SAGAN, 2000, p. 22-23).

A segunda abordagem remete à teoria realista, das Relações Internacionais, utilizada para compreender o motivo dos Estados estarem propensos a desenvolver diferentes doutrinas militares. Partindo dos pressupostos realistas, os Estados, em geral, constroem dois comportamentos de equilíbrio: o equilíbrio interno (aumentando suas próprias capacidades de armas) e equilíbrio externo (ganhando força militar por meio de alianças com outros Estados). Apesar de haver discordância no quesito do objetivo principal, podendo ser o de proteção (o que incentiva estratégias mais defensivas para proteger o *status quo*) ou a busca em maximizar seu poder (o que incentiva políticas mais ofensivas e revisionistas), há a concordância de que os Estados devem estar cientes de seu poder atual em relação aos outros e constantemente vigilantes para que não surjam novas ameaças de outros Estados (SAGAN, 2000, p. 23-24).

Para os realistas, tanto a doutrina militar quanto a guerra é a continuação da política por outros meios. Barry Posen (1984) é um grande exemplo desta corrente, ao passo que infere um associado de previsões realistas sobre que tipos de doutrinas militares gerais os diferentes Estados adotarão. Como já abordado, tem-se que os Estados que desejam alterar o *status quo* devem possuir armas e doutrinas ofensivas com o fito de atingir seus objetivos de guerra. Os Estados que não podem defender na terra, tendem a favorecer doutrinas ofensivas, pois estas lhes permitem concentrar forças limitadas e levar a guerra ao território inimigo. Além disso, os Estados que enfrentam, concomitantemente, adversários, podem aderir às doutrinas ofensivas para que possam enfrentar separadamente seus inimigos. Não obstante, os que estão satisfeitos com o *status quo* buscam adotar uma doutrina mais defensiva, justamente por não possuir ambições territoriais. Por fim, países que detém aliados com forte poder do *status quo* podem ser encorajados a adotar uma doutrina defensiva com o fito de manter a aliança (SAGAN, 2000, p. 24).

Em geral, os realistas apontam que os líderes de potências militares, quando confrontam adversários em potencial ou mais fracos, ponderarão a guerra preventiva. Caso esta seja rejeitada, a razão poderá estar relacionada mais aos custos esperados da guerra do que por questões morais ou restrições de políticas internas. Ademais, o realismo oferece previsões sobre por que e quando os Estados desenvolverão doutrinas que enfatizam forças retaliatórias seguras e dissuasão de segundo ataque. Desse modo, caso o inimigo tenha desenvolvido forças militares suficientes para tornar a guerra preventiva e os primeiros ataques impossíveis, o desenvolvimento de forças de segundo ataque será a maior prioridade do Estado. No curto prazo, o Estado deverá aceitar a condições de dissuasão mútua, mas poderá buscar programas de armas que possam fornecer vantagens militares futuras (SAGAN, 2000, p. 25).

Apesar dos realistas concordarem na questão de que os Estados devem se concentrar no poder militar de seus adversários, eles discordam sobre o equilíbrio militar, isto é, se um sistema de armas aumenta ou diminui a probabilidade do uso de outros sistemas de armas. Enquanto alguns realistas argumentam que, Estados que detém armas convencionais e não convencionais, possam adotar "doutrinas de contra-dissuasão", os neorrealistas, como Kenneth Waltz, argumentam que, neste caso, os Estados serão cautelosos ao explorar suas armas para outros fins que não a dissuasão básica, uma vez que os riscos de retaliação dispendiosa se tornam graves (SAGAN, 2000, p. 26).

Entretanto, ambos os campos concordam que os líderes devem levar em consideração tanto o equilíbrio relativo das capacidades militares entre seu Estado e seus adversários quanto às reações específicas do inimigo às investigações militares. Os Estados, na visão realista,

quando se encontrarem em uma posição onde creem ser necessário compensar a superioridade militar convencional de um adversário, adotarão a doutrina que enfatiza as opções de ataque limitado, o que, por sua vez, aumenta as apostas no conflito, sem necessariamente escalando uma retaliação de grande proporção. Este tipo de doutrina pode transformar guerras limitadas em uma competição na tomada de riscos (SAGAN, 2000, p. 26).

A teoria realista indica que a doutrina militar deve estar integrada à grande estratégia do Estado, prevendo que os sistemas de comando e controle devem, também, estar integrados à doutrina. Nesse sentido, o principal fator que determina se o Estado desenvolverá tais sistemas assertivos é a natureza da doutrina militar, determinada, por sua vez, pela natureza da ameaça representada pelos adversários. Em geral, estadistas que enfrentam adversários que não podem ameaçar sua infraestrutura de comando e controle podem se dar ao luxo de um sistema de comando e controle altamente assertivo. Portanto, o realismo sugere que a natureza das ameaças à segurança internacional determina as doutrinas. Diferentes doutrinas estratégicas produzem diferentes sistemas de comando (SAGAN, 2000, p. 39-40).

A terceira e última vertente teórica se concentra na influência da política e cultura doméstica na doutrina militar. A teoria da cultura estratégica é baseada por diferentes formas de influências culturais em relação aos tomadores de decisão, não se restringindo à busca racional de segurança nacional ou interesses organizacionais operacionais afins. Os líderes estatais, nesse sentido, agem de acordo com o que acreditam ser um comportamento conveniente, podendo ou não estar em conformidade com os interesses e objetivos compartilhados. Esta perspectiva cultural entende o pilar da doutrina militar em experiências históricas e mitos, crenças religiosas e normas resultantes, de modo que diferentes Estados (ou organizações), em condições estratégias análogas, provavelmente desenvolveriam doutrinas militares diferentes (SAGAN, 2000, p. 30).

Nesse sentido, uma inovação proporcionada pelos neoculturalistas remete ao foco no desenvolvimento e consequência das normas culturais relativas. Estas normas, por sua vez, são vistas como visões difundidas dentro de uma comunidade específica, de qual comportamento é apropriado e legítimo. Entretanto, as normas podem não ser universalmente aceitas, o que significa que diferentes Estados, ou grupos e organizações domésticas, podem ter visões dissonantes sobre o que é legítimo ou não. Sendo assim, a perspectiva normativa tem sido usada para explicar porquê alguns estados dedicam enormes recursos econômicos e humanos para desenvolver forças militares avançadas de alta tecnologia (SAGAN, 2000, p. 33).

Destarte, as normas podem influenciar o comportamento do Estado na ausência de "necessidade" militar. Os realistas, por vezes, aceitam que as normas morais influenciam o comportamento, mas apenas quando a segurança do Estado não está gravemente ameaçada. Os neoculturalistas, aliás, também aceitam que condições de extrema necessidade podem fazer com que os estadistas relutantemente quebrem paradigmas. Entretanto, a principal diferença entre ambos concerne se as normas realmente influenciam as percepções de necessidade dos estadistas e, por conseguinte, seu comportamento. Normas que são sempre quebradas não são significativas. No entanto, as normas que redefinem ou limitam o domínio da necessidade podem ser significativas (SAGAN, 2000, p. 34).

Diferentemente do realismo e da teoria organizacional, a teoria da cultura estratégica apresenta diferentes perspectivas sobre líderes civis e militares. Os líderes civis não são vistos propriamente como estadistas, mas sim políticos e, por conseguinte, esforçam-se para influenciar a política militar, ou seja, não para maximizar a segurança nacional, mas para promover seus próprios interesses políticos domésticos. Isto é, esse esforço não tenta influenciar diretamente a doutrina militar em si, mas seu objetivo remete à influência da estrutura militar que, por sua vez, pode influenciar os interesses políticos domésticos. Desse modo, oficiais militares superiores e as instituições lideradas pelos mesmos não estão unissonamente entrelaçados às doutrinas ofensivas. Embora os oficiais militares possam acreditar que a ofensiva oferece vantagens tanto para a segurança nacional quanto para os interesses organizacionais, eles também mantêm fortes crenças culturais sobre quais forças militares são mais adequadas para missões militares específicas. Outrossim, a crença nada mais é do que o produto da história da organização e da doutrinação dos oficiais por meio do treinamento militar. Diferentes organizações, portanto, possuem diferentes experiências e regimes de treinamento, o que faz com que as crenças culturais, onde diferentes doutrinas militares são apropriadas para tarefas variadas (SAGAN, 2000, p. 31-32).

Outrossim, políticos poderão aplicar restrições orçamentárias e arsenais militares que atendem aos seus interesses políticos internos, o que causa um impacto indireto na doutrina militar. Isto é, autoridades políticas, ao mesmo tempo em que podem decidir impor severas restrições orçamentárias ao número de armas ou sistemas de lançamento relacionados no arsenal estratégico do Estado, também podem pressionar por gastos em sistemas de armas específicas, pois os aumentos orçamentários beneficiam eleitores domésticos ou apoiadores burocráticos. Além disso, estas autoridades não estariam tomando decisões doutrinárias, mas a escolha de compras poderiam ser influentes, tendo em vista que, a depender do tipo de arma, pode ser

mais fácil ou difícil tê-la sob controle. Se os oficiais militares acreditam que doutrinas específicas dependem do número de armas disponíveis, por exemplo, as restrições orçamentárias podem influenciar, indiretamente, a escolha doutrinária (SAGAN, 2000, p. 32-33).

Nesta teoria, o sistema de comando e controle do Estado pode ser fortemente influenciado por interesses políticos domésticos e tradições de tomada de decisão e por experiências históricas específicas e mitos relativos ao início da guerra. Sendo assim, diferentes Estados mantêm diferentes normas culturais sobre se a autoridade política deve ser altamente centralizada ou mais amplamente compartilhada por meio de alguma forma de sistema de freios e contrapesos. Tais tradições culturais, bem como as instituições construídas em torno delas, podem ter um forte impacto sobre os líderes do Estado. Outrossim, as crenças dos líderes sobre a probabilidade de ataques surpresa na guerra também é influenciada pelo fator cultural estratégico. Cabe notar que tais crenças não seriam baseadas em características técnicas objetivas de sistemas de armas específicos ou no equilíbrio estratégico, mas sim nas memórias e interpretações da história militar, de modo que os líderes que foram vitimados por ataques surpresa em guerra seriam extremamente sensíveis, talvez até obcecados. Tais temores poderiam levar os líderes a manter altos níveis de alerta militar em tempos de paz e encorajariam a delegação de autoridade de lançamento de armas não convencionais (SAGAN, 2000, p. 42 e 44).

Em suma, as crenças dominantes na sociedade sobre a probabilidade de ataques surpresa bem-sucedidos podem ter um forte efeito sobre as estruturas nacionais de comando e controle. Os argumentos desta teoria, portanto, calculam que diferentes líderes provavelmente desenvolverão diferentes tipos de sistemas de comando, dependendo de suas culturas domésticas de tomada de decisão, interesses domésticos e as experiências militares do Estado, bem como interpretações dominantes sobre se as guerras começam ou não com ataques surpresa (SAGAN, 2000, p. 45).

Por fim, as três diferentes teorias apontadas por Sagan (2000) ajudam a explicar a estrutura de comando e doutrina dos Estados. Entretanto, a teoria da cultura estratégica é a mais plausível para explicar o caso de Israel. Primeiramente, a teoria organizacional não ajuda a explicar e tampouco aborda os diferentes tipos de doutrinas existentes, criando a suposição de que todos os países tenderiam a possuir uma doutrina ofensiva. Tendo isto em vista, seria necessário um orçamento e uma organização militar grande, o que é praticamente impossível para Israel, tanto por conta do seu tamanho territorial quanto populacional e capacidade econômica. Além disso, afirmar que oficiais militares não tenham ou sejam menos propensos a levar em consideração os interesses políticos parece falho. Outra questão é que o efeito dissuasor das

FDI é reforçado não apenas pela vitória em guerras em grande escala, mas também por operações entre guerras, as quais fazem parte das atividades defensivas de Israel, o que contradiz o fato desta teoria argumenta que os oficiais sustentam a opinião de que a força deve ser empregada ou de maneira decisiva ou não ser usada de todo (TAL, 2000, p. 52).

Já em relação à teoria realista, ela tampouco ajuda a explicar a doutrina e a estratégia israelense, pois não há equiparação entre a ameaça material real com o tamanho do poderio militar de Israel. Ademais, o sistema internacional pode, sim, influenciar e determinar a doutrina, porém fatores internos também devem ser considerados, justamente porque a ideia e o propósito de Israel foram formulados muito antes de sua criação de fato, daí a importância da teoria da cultura estratégica.

É possível notar que o aspecto cultural possui uma forte influência na doutrina militar. Israel como Estado proveniente do sionismo capta tanto experiências históricas quanto mitos, crenças religiosas e normas em sua política, sobretudo militar. Há enraizado, no país e na população, experiências históricas de perseguição e genocídio que os afetam profundamente. Aliás, o próprio mito de David contra Golias fez parte dos primeiros anos do Estado israelense, em uma analogia dos judeus contra os árabes em uma busca pela sobrevivência que, no fim, Israel conseguiu vencer. Neste sentido, o sionismo traz, em conjunto, crenças e experiências históricas que foram capazes de construir um Estado baseado na ideia de este sendo o protetor do povo judeu, o que acabou por produzir certas normas.

A perspectiva normativa, portanto, auxilia na explicação de como e porquê alguns países dedicam enormes recursos econômicos e humanos para desenvolver forças militares avançadas de alta tecnologia. Como abordado no capítulo subsequente, Israel é um desses países. Seus recursos econômicos e capital humano são, em grande parte, voltados para o desenvolvimento da alta tecnologia e do poder cibernético. Este poder, por sua vez, auxilia no *early warning* e no mapeamento de ataques e possíveis ataques que Israel pode vir a sofrer. A crença de ataques surpresas aqui, também, tem a sua importância: o país já sofreu, por exemplo, durante a guerra de Yom Kippur, bem como sua população carrega o fardo histórico das perseguições e ataques contra os judeus. Nesse sentido, a crença é o produto da história da doutrinação dos oficiais por meio do treinamento militar, o qual será abordado no próximo capítulo. É neste sentido que a teoria da cultura estratégica é a mais plausível para explicar a estrutura de comando e a doutrina de Israel.

Em suma, a doutrina militar é importante no que se refere à grande estratégia, a qual remete a uma cadeia político-militar de um Estado. Ao identificar possíveis ameaças ou oportunidades, ela deve garantir a sobrevivência do país. Se, antes, Israel detinha uma postura muito

mais ofensiva devido aos seus inimigos árabes, atualmente ele detém uma postura mais defensiva justamente por conta da alteração destes inimigos. Desse modo, a vantagem quantitativa de Israel continua a ser extremamente importante, apesar de possuir um papel parcial.

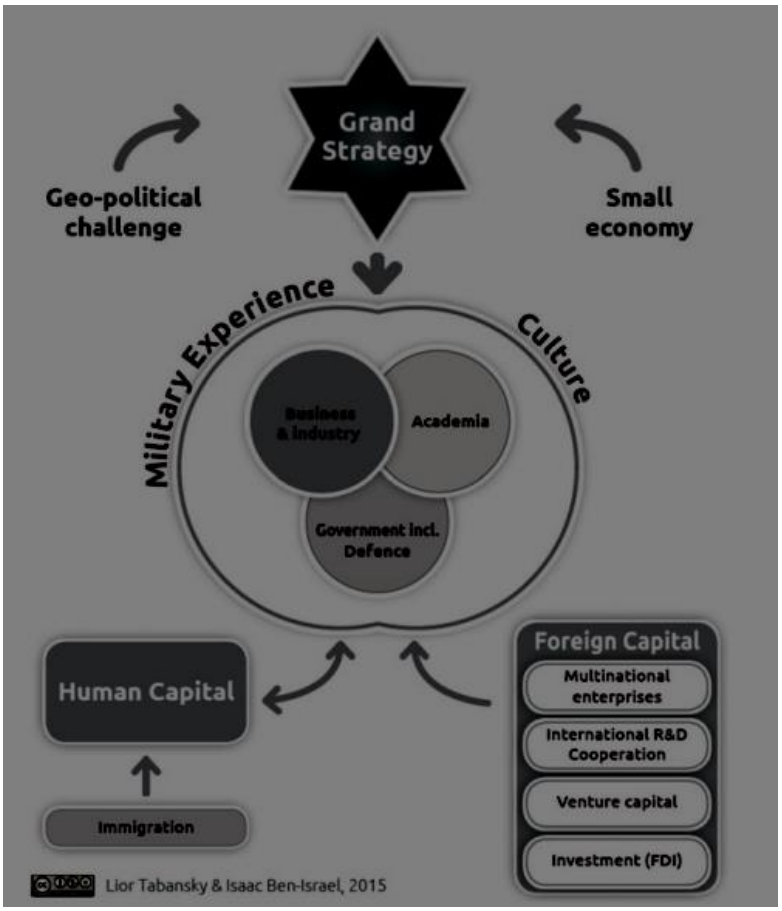
A grande estratégia israelense é estruturada de forma articulada, delineada para aumentar as margens de segurança. Aliás, os pilares desta estrutura remetem, em alguns aspectos, à doutrina de Ben Gurion, tais como dissuasão, profundidade estratégica artificial, aviso prévio, vantagem qualitativa. Para melhor compreensão, o próximo capítulo tratará sobre como essa vantagem qualitativa foi e é construída em Israel.

5 CONTEXTO

Neste capítulo, demonstrar-se-á o contexto tecnológico existente em Israel e como este se relaciona com o ecossistema nacional de inovação. Visa-se, portanto, confirmar a relação entre a grande estratégia israelense e seu ecossistema e como ambos são importantes no que se refere ao entendimento do poder cibernético em Israel. Assim sendo, apresentar-se-á dados sobre o sistema de Pesquisa e Desenvolvimento (P&D) no país, bem como programas governamentais que incentivam a aprendizagem tecnológica e cibernética, além de como o serviço militar realiza um papel crucial na formação deste capital humano. Ademais, evidenciar-se-á a relação intrínseca entre governo e instituições privadas no desenvolvimento deste poder, bem como a relação com a educação nacional e seus respectivos projetos. Por fim, apresentar-se-á a classificação geral de Israel de acordo com critérios utilizados para medir sua capacidade cibernética. Para além disso, além dos dados agregados, expor-se-á programas, iniciativas e organizações que estão envolvidas no ecossistema nacional de inovação, local em que se insere a cibersegurança de Israel. Este ecossistema é composto pelos serviços prestados pelo P&D de empresas nacionais e estrangeiras e de defesa, pelas FDI, pelo governo e pelas universidades, os quais serão expostos nesta ordem.

Israel é um dos poucos países líderes em alta tecnologia, tal como a ciência da computação, eletrônica e tecnologias da informação. Estes são os componentes mais palpáveis da tecnologia de segurança cibernética. O ecossistema da inovação existente em Israel é a consequência de sua grande estratégia, sendo esta voltada para a vantagem qualitativa com o fito de aumentar a viabilidade e a segurança nacional na conjuntura geopolítica um tanto quanto desafiadora. Este ecossistema, o qual possui base nas idiossincrasias culturais, cria o cenário propício ao desenvolvimento de capital humano qualificado e inovador, bem como a ciência e a tecnologia de ponta (TABANSKY; ISRAEL, 2015, p. 16). A imagem abaixo demonstra como este ecossistema interage.

Figura 8 - Ecossistema nacional de inovação se origina da grande estratégia



Fonte: TABANSKY; ISRAEL, 2015, p. 16

Israel ocupa o 20º lugar no Índice de Competitividade Global geral de 2019. Seu desempenho está quase inalterado em relação ao ano anterior, apesar de já ter ocupado o 16º lugar de acordo com o relatório de 2017-2018. O país é um *hub*[21] de inovação, ocupando o 15º lugar no pilar Capacidade de Inovação, devido ao seu ecossistema bem desenvolvido. Israel gasta mais do que qualquer país em P&D (4,3% do PIB) e é onde a cultura empreendedora é mais forte, a aceitação do fracasso empresarial é mais alta e as empresas adotam mais mudanças e as empresas inovadoras crescem mais rapidamente. Israel também pode contar com uma força de trabalho altamente qualificada, com uma média de 13 anos de escolaridade, ocupando o 12º lugar (WORLD ECONOMIC FORUM, 2019, p. 17).

O país também ocupa o 2º lugar, ficando apenas atrás dos Estados Unidos, pela facilidade de encontrar trabalhadores com as habilidades adequadas, bem como pela disponibilidade

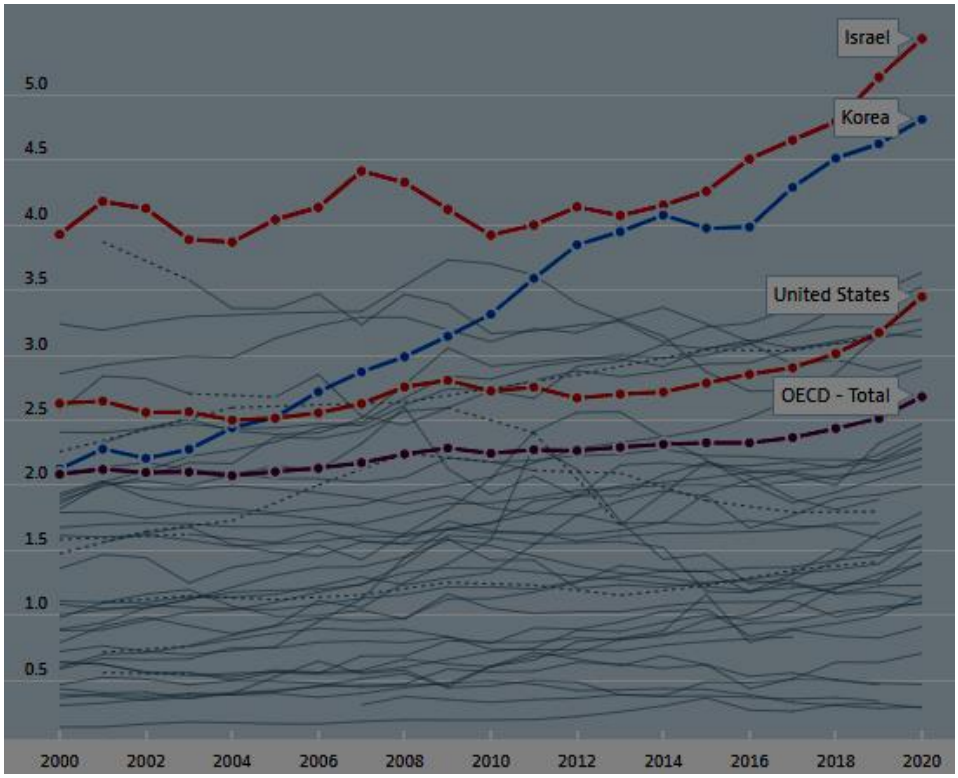
[21]Os *hubs* de inovação são ambientes físicos ou virtuais onde pessoas de áreas diferentes se reúnem para estabelecer conexões e gerar negócios (HUB.RO, 2020).

de capital de risco, que também apoia um setor privado florescente e inovador. Não obstante, a taxa de adoção de tecnologia básica (45º) está bem abaixo da média da OCDE. Outras áreas com espaço para melhorias incluem instituições, devido a preocupações persistentes de segurança (42º), regulamentação pesada (69º) e baixo compromisso com a sustentabilidade (81º). Finalmente, a eficiência do mercado de Israel ocupa o 32º e sofre de uma relativa falta de concorrência e de barreiras à entrada (WORLD ECONOMIC FORUM, 2019, p. 17).

O desenvolvimento das tecnologias de informação e comunicação (ICT) foi alimentado pelas demandas geopolíticas, pelo menos inicialmente. O P&D de defesa teve um impacto considerável no início do setor industrial, no sistema de ensino superior nas áreas de ciência e engenharia (devido a alta demanda por trabalhadores altamente qualificados) na comunidade de pesquisa e na estrutura da força de trabalho da indústria de ICT, principalmente devido aos fundos investido pelo governo israelense em equipamentos e capacidades voltados para a defesa. Todavia, as empresas multinacionais respondem por uma parcela significativa dos gastos com pesquisa na indústria israelense. Nesse sentido, no que se refere à pesquisa acadêmica e pesquisa científica, Israel se classifica 45º lugar entre os países da OCDE para patentes relacionadas a ICT. De acordo com *Center for Strategic and International Studies*, 5% da produção econômica total em Israel está em tecnologias de ICT (WORLD ECONOMIC FORUM, 2019, p. 17; CSIS, 2016, p. 8)

Um dos maiores pontos fortes de Israel é seu capital humano, infraestrutura de pesquisa e alta intensidade de pesquisa. Israel sustenta essa taxa extraordinariamente alta de gastos em P&D, apesar dos desafios geopolíticos. Esse ecossistema de inovação é resultado do grande objetivo estratégico de buscar a vantagem qualitativa (TABANSKY; ISRAEL, 2015, p. 16-17). O gráfico abaixo exemplifica a colocação de Israel em comparação com a Coréia (2º lugar), Estados Unidos e a classificação geral dos países da Organização para a Cooperação e Desenvolvimento Econômico (OCDE).

Figura 9 - Gastos internos brutos em P&D de Israel, Coreia, Estados Unidos e OCDE



Fonte: OCDE, 2022

Na década de 1990, Israel era um Estado com uma economia em dificuldades e uma indústria de alta tecnologia insignificante. Porém, Israel se tornou um gigante tecnológico com um setor de alta tecnologia sofisticado e inovador a partir das questões de segurança exigidas com as quais tinha de lidar. Atualmente, a representação de empresas israelenses de alta tecnologia na *National Association of Securities Dealers Automatic Quotation System* (NASDAQ) supera Grã-Bretanha, Alemanha, Japão e Coreia do Sul. Ademais, Israel tem sido considerado um dos principais focos de inovação do mundo há mais de uma década (TABANSKY, 2020, p. 57).

É interessante notar que as FDI contribuíram para o sucesso em alta tecnologia e segurança cibernética de Israel, pois percebem a tecnologia cibernética como um importante multiplicador de força qualitativo. Quase três décadas atrás, várias áreas interessadas dentro das FDI haviam se empenhado significativamente em inovações radicais que hoje seriam chamadas de cibernética. Tendo isto em vista, a *Maf'at* tem impulsionado e facilitado inovações ousadas em P&D cibernética. Paralelamente, as principais partes cibernéticas interessadas – Inteligência, C4I, Forças Aéreas e Especiais – possuem a capacidade de realizar P&D e aquisição sob medida

para apoiar suas missões. Além disso, *Maf'at* e INCB lançaram um plano de P&D cibernético de uso duplo (civil e defensivo) chamado MASAD em 2012, com o fito de fortalecer e avançar as capacidades de Israel no ciberespaço, transformá-lo em um país líder em cibertecnologia e, assim, servir como um novo motor de crescimento para a economia israelense (TABANSKTY, 2020, p. 57-58; ISRAEL, 2012).

A grande política de P&D de defesa realiza extensa pesquisa focada que, por vezes, vem a se concretizar em sistemas avançados, intensivos e integrados de TI. Exemplos são a aquisição e processamento de inteligência, munições guiadas com precisão, UAVs e defesa de mísseis (TABANSKY; ISRAEL, 2015, p. 21). Ademais, Israel é considerado vital no mundo digital, especialmente em TI, *software* e internet, com um mercado que cresceu quase 400% na última década. Mais de 100 empresas de software israelenses estão ativas em computação em nuvem e na entrega de serviços empresariais e de consumo pela Internet, considerada a próxima revolução no mercado de TI. A indústria de *software* de Israel atraiu a atenção dos líderes globais de tecnologia. Muitas empresas, incluindo HP, IBM, Microsoft e Oracle, estabeleceram operações e centros de fabricação no país. Além disso, empresas, especialmente estadunidenses, identificaram Israel como um destino privilegiado para estabelecer centros de P&D. Ter uma presença de P&D em Israel oferece uma oportunidade de alavancar talentos locais e aprimorar as tecnologias existentes, colaborando com empresas israelenses em campos de *software* (ITA, 2022).

Outrossim, a importância dos valores culturais na condução da inovação tem sido cada vez mais reconhecida. Há, de certo modo, uma tradição judaica de erudição e desenvolvimento no que tange à arte da interpretação, a qual possui o objetivo de atender às necessidades modernas encontradas no Estado de Israel. Desde a sua criação, há a sensação de uma ameaça iminente, o que provocou uma cultura de improvisação e de *make-do*, utilizados para resolver problemas de forma criativa, porém com recursos escassos (TABANSKY; ISRAEL, 2015, p. 18).

Apesar de a improvisação não fazer parte do código oficial das FDI, esta é incentivada pela cultura militar interna (TABANSKY, 2020, p. 58). A tradição militar israelense celebra a capacidade de seus oficiais de se orientar rapidamente, confiar no julgamento pessoal, pensar rápido ao enfrentar a incerteza, tomar a iniciativa e dar soluções imediatas. Flexibilidade e improvisação são aspectos essenciais do treinamento dos oficiais israelenses, de modo que se tornaram uma virtude mais importante do que agir de acordo com o planejamento prévio. Como a capacidade de improvisar a partir da incerteza provou ser bem-sucedida, foi preservada, apesar

de o estabelecimento posterior de instituições e regulamentos formais (ADAMSKY, 2010, p. 117-118).

O lado positivo deste tipo de conduta é a rápida aprendizagem organizacional, a adaptação técnico-tática e a exploração eficaz de linhas curtas de comunicação. A desvantagem, entretanto, é que o eventual sucesso permanece dependente de um planejamento detalhado e trabalho em equipe no nível tático-tecnológico de alguns serviços e nas indústrias de defesa (ADAMSKY, 2010, p. 117).

No que tange à estrutura social, o individualismo coexiste em Israel com uma orientação grupal bem desenvolvida. Este tipo de individualismo se expressa em uma atitude casual em relação às regras e regulamentos, na autoconfiança e no pouco respeito pela autoridade imposta. No entanto, a lealdade israelense tende a se concentrar nos objetivos coletivos e no bem-estar da sociedade. Os "pais fundadores" de Israel conceberam uma notável informalidade de comportamento e desatenção à hierarquia por meio de uma série de normas sociais igualitárias. Tendo uma estrutura organizacional enxuta e burocracia militar simples, os sistemas militares e de defesas israelenses são informais e igualitários e promovem muitas ideias inovadoras de baixo para cima por meio de atalhos organizacionais informais (ADAMSKY, 2010, p. 110).

De modo geral, os israelenses são caracterizados pela comunicação informal direta; curta distância do poder e percepção de igualdade de status; abordagem orientada para a tarefa; ousadia (*Hutzpah*); e respeito mínimo *a priori* à autoridade. Estas características, acompanhadas de uma educação formal, são aprofundadas pelo ecossistema existente no país. Aliás, a imigração massiva de judeus qualificados de todo o mundo enriqueceu o capital humano (TABANSKY; ISRAEL, 2015, p. 18).

Aliás, o serviço militar israelense molda a ética de trabalho de seus soldados e as habilidades adquiridas em uma idade tão jovem treinam os soldados para assumir riscos e se concentrar na missão. Isto é, as redes sociais criadas durante o serviço auxiliam na explicação do envolvimento de veteranos em empreendimentos de risco, bem como o efeito das ligações com os militares em várias empresas e seus desempenhos. Nesse sentido, a forma como esses soldados se comportam mais tarde na vida, especificamente no que diz respeito às suas carreiras, é influenciada pelo período servido no exército (BARAM; ISRAEL, 2018, p. 5).

Outras explicações propõem ver o militar como agente de socialização, oferecendo o termo "Capital Militar" que se desenvolveu durante o processo de socialização militar. Nesse

processo, os soldados adquirem novas habilidades (capital humano[22]), novas redes sociais (capital social[23]) e novas normas sociais e códigos de comportamento (capital cultural[24]). Estes três tipos de capital juntos e o conjunto de características que esse processo de socialização produz são identificados como o capital militar por Swed e Butler (2015, p. 124). Estes autores argumentam que a socialização das FDI (capital militar) define a demografia dos trabalhadores e seu comportamento e desempenho, tendo em vista que os soldados em serviço absorvem o capital militar, ou parte dele, e o "exportam" para a esfera civil, onde se adéquam bem, especialmente no setor de alta tecnologia. Desse modo, esse capital militar os ajuda a ter sucesso na indústria de alta tecnologia assim que deixam as forças armadas (BARAM; ISRAEL, 2018, p. 5; SWED; BUTLER, 2015, p. 124-125).

Embora o capital militar seja a fusão dos três tipos de capital, ele está centrado na instituição e na cultura militar e, portanto, seria distinto de outros tipos de capital na sociedade. O processo de socialização dos soldados das FDI, que promove esse capital, se traduz mais tarde em habilidades de trabalho, redes e ética na indústria de alta tecnologia quando esses veteranos são contratados. Cerca de 90% dos trabalhadores em alta tecnologia são veteranos e 87,4% dos gerentes no mercado israelense é composta também por veteranos (SWED; BUTLER, 2015, p. 126; CBS, 2010).

Outro elemento importante em relação à estrutura elementar e ao capital humano é o sistema elaborado desenvolvido com o fito de maximizar a eficácia das FDI. Normalmente quando se pensa em cultura militar, pensa-se em hierarquias firmes, obediência inabalável e aceitação da inferioridade do soldado em relação ao resto. Porém, as FDI não fazem jus a esta descrição. Em Israel é muito comum que grande parte da população já tenha servido às forças armadas, onde sua cultura é trabalhada durante um serviço obrigatório (SENOR; SINGER, 2009, p. 41). O recrutamento obrigatório de jovens de 18 anos, sendo de 2 anos para mulheres e 3 anos para homens, além do dever de reserva subsequente. Isto possibilita melhorar o capital

[22]De acordo com a definição da Organização para Cooperação e Desenvolvimento Econômico (OCDE), o capital humano é tido como a reserva de conhecimento, habilidades e outras características pessoais, as quais auxiliam as pessoas a serem mais produtivas. A educação formal e informal, a prática e a experiência de trabalho retratam o investimento em capital humano (OECD, 2022).

[23]De acordo com a definição de Bourdieu (1986, p. 247), o capital social se refere ao agregado dos recursos reais ou potenciais que estão ligados à posse de uma rede durável de relações mais ou menos institucionalizadas de conhecimento mútuo e reconhecimento, isto é, a participação em um grupo que fornece a cada um de seus membros o respaldo do capital coletivo.

[24]De acordo com Bourdieu (1986, p. 243), o capital cultural pode existir em três formas: no estado corporificado, ou seja, na forma de disposições duradouras da mente e do corpo; no estado objetivado, na forma de bens culturais (quadros, livros, dicionários, instrumentos, máquinas etc.), que são o traço ou a realização de teorias ou críticas a essas teorias, problemáticas etc.; e no estado institucionalizado, uma forma de objetivação que deve ser destacada porque confere propriedades inteiramente originais ao capital cultural que se espera garantir.

humano e, durante o serviço militar, impulsionar a estratégia de buscar qualidade (TABANSKY; ISRAEL, 2015, p. 18; TABANSKY, 2020, p. 58).

Nesse sentido, as FDI desenvolveram um sistema complexo com o objetivo de avaliar o potencial dos recrutas e atribuir um treinamento adequado aos mesmos, além de uma carreira. Este sistema, portanto, contribui consideravelmente para a participação de especialistas em ciência e tecnologia. Esta medida foi adotada para combater a vasta inferioridade geopolítica na região e maximizar as forças de defesa desde a Guerra de 1948 (TABANSKY; ISRAEL, 2015, p. 18; TABANSKY, 2020, p. 58).

Durante o alistamento, o serviço militar dos israelenses é adiado até que completem os estudos acadêmicos pagos pelas FDI e, após a conclusão, geralmente atuam como oficiais em posições que sejam equivalentes ao conhecimento adquirido (TABANSKY; ISRAEL, 2015, p. 19). O período de reserva foi criado com o objetivo de aumentar o poder de combate. Homens e mulheres servem na reserva até os 40 ou 50 anos, a depender da ocupação militar. Há, também, subgrupos menores de pessoal altamente qualificado, os quais são retidos em suas unidades e convocados para operar como técnicos ou desenvolvedores. Esses reservistas servem, principalmente, como uma conexão entre a indústria, a academia, o governo e as FDI. O serviço de reserva desempenha um papel essencial e complexo na criação, desenvolvimento e sustentabilidade do ecossistema de inovação israelense (TABANSKY; ISRAEL, 2015, p. 20).

Aliás, a escassez de mão de obra, por exemplo, é responsável pelo que talvez seja a característica mais incomum das FDI: o papel de suas forças de reserva. Diferentemente de outros países, as forças de reserva são a espinha dorsal das forças armadas de Israel. Na maioria das forças armadas, as forças de reserva são construídas como apêndices do exército, o qual é a principal linha de defesa do país. Israel, no entanto, é tão pequeno e superado em número por seus adversários que nenhum exército poderia ser grande o suficiente para se defender contra um ataque total. Logo após a Guerra da Independência, os líderes de Israel decidiram por uma estrutura militar única, dominada pelas reservas, pela qual os reservistas não apenas governariam unidades inteiras, mas também seriam comandados por oficiais da reserva (SENOR; SINGER, 2009, p. 45).

Unidades de reserva de outras forças armadas podem ou não ser comandadas por oficiais do exército permanente, mas recebem semanas ou até meses de treinamento de atualização antes de serem enviadas para a batalha (SENOR; SINGER, 2009, p. 45). Em suma, as forças das FDI são constituídas, sobretudo, de reservas. É desse modo que Israel é capaz de manter uma das maiores forças armadas do mundo em relação à sua população e garantir um caráter civil à

mesma. Assim, sua estrutura é baseada em três componentes: uma força militar de carreira governada por regulares, uma força militar permanente de conscritos e uma força militar de reserva (TAL, 2000, p. 62).

O sistema de reservas de Israel não é apenas um exemplo da inovação do país; é também um catalisador para isso. Como a hierarquia é naturalmente diminuída, o sistema de reserva ajuda a reforçar esse *ethos* caótico e não hierárquico que pode ser encontrado em todos os aspectos da sociedade israelense, tanto na sala de guerra quanto na sala de reuniões (SENOR; SINGER, 2009, p. 46). Outrossim, os perfis dos trabalhadores israelenses de alta tecnologia contêm algum tipo de capital militar muito elevado. Além disso, o mercado de trabalho em alta tecnologia demonstra uma preferência por aqueles com capital militar. De fato, o serviço militar em unidades tecnológicas é percebido como uma vantagem que muitas vezes equivale a um diploma universitário (TABANSKY, 2020, p. 58). Embora as empresas israelenses ainda busquem experiência no setor privado, o serviço militar fornece a métrica convencional para os empregadores (SENOR; SINGER, 2009, p. 68).

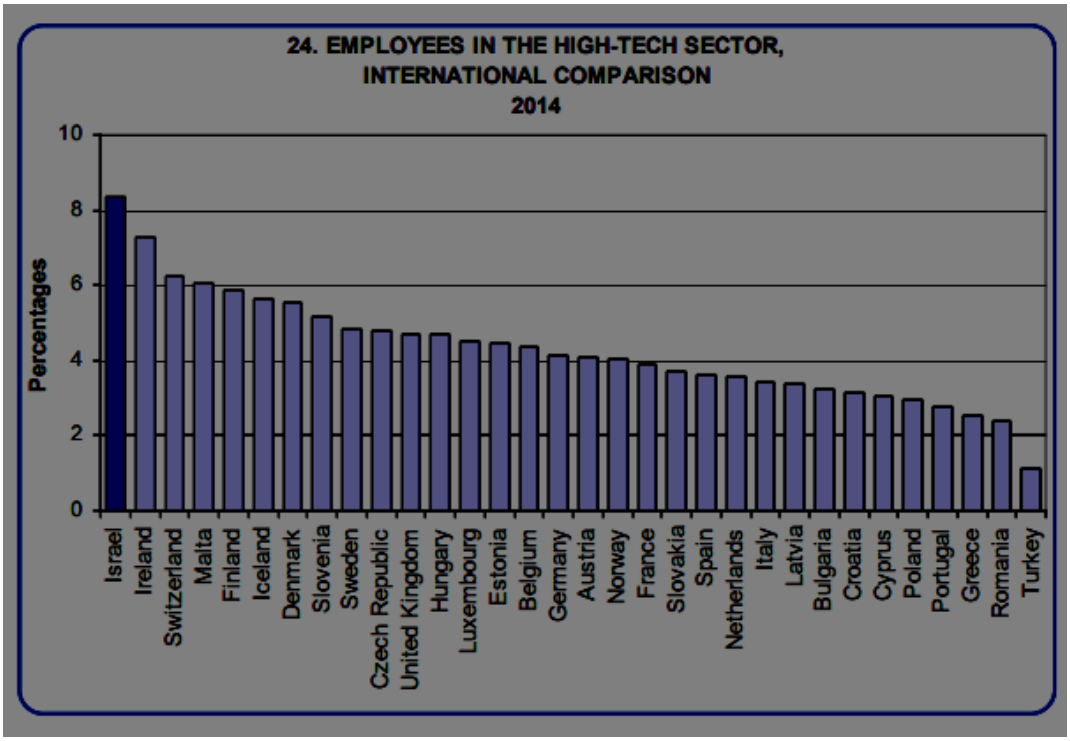
Um fato curioso é que as FDI possuem pouco pessoal em níveis hierárquicos superiores, tendo poucos coronéis e mais tenentes. A consequência de haver menos oficiais superiores para emitir comandos implica uma maior iniciativa individual nos escalões inferiores (SENOR; SINGER, 2009, p. 44). Destarte, a cultura organizacional das FDI é orientada para a missão, justamente por conta da alta intensidade de engajamento contínuo com os desafios imediatos. Isto é, há uma cultura em que se espera que soldados e oficiais do exército se utilizem da improvisação para cumprir sua missão (em situações de não combate). Tanto a criatividade quanto a inteligência são extremamente valorizadas. O serviço militar traz consigo treinamento profissional, laços sociais e uma ética de trabalho que influenciam a força de trabalho de alta tecnologia e a cultura da indústria de alta tecnologia (TABANSKY; ISRAEL, 2015, p. 20).

Por vezes, o passado militar acaba sendo mais importante do que o acadêmico. Em entrevistas de emprego, perguntarem onde o candidato serviu no exército. Aliás, há vagas de emprego disponíveis destinadas a ex-alunos da 8200. Há, sobretudo, uma associação de ex-alunos da 8200 que possuem uma reunião anual. Mas, em vez de usar o tempo juntos para refletir sobre batalhas passadas e nostalgia militar, é voltado para o futuro: os ex-alunos estão focados em redes de negócios. São nestas reuniões que empreendedores e ex-alunos da 8200 bem-sucedidos fazem apresentações na reunião sobre suas empresas e indústrias (SENOR; SINGER, 2009, p. 58; 8200BIO, 2022).

Aliás, a *start-up National Central*, por meio da organização *Scale Up Velocity*, e em estreita parceria com a indústria de alta tecnologia, desenvolveu e executou soluções para a

escassez de capital humano de alta tecnologia. As soluções realizadas focam na captação e expansão de talentos por meio de programas de treinamento para iniciantes tanto de populações minoritárias quanto soldados de combate que foram liberados para cargos em equipes centrais de P&D, com ênfase em projetos práticos e habilidades sociais adicionais. Uma ênfase especial é colocada na qualidade do treinamento, no envolvimento ativo de empresas de alta tecnologia em todas as fases dos programas e no desenvolvimento de um programa fundamental para permitir sua expansão com o fito de fornecer soluções seletivas para a escassez de capital humano (START-UP NATION, 2022, p. 32).

Figura 10 - Comparação internacional do percentual em relação ao total de trabalhadores ativos, formado pelos funcionários no setor de alta tecnologia



Fonte: CBS, 2017, p. 27

Como parte da iniciativa *Combat Soldiers for High-Tech*, uma iniciativa conjunta entre a *start-up Nation Central*, as FDI, a *Atidim*[25], o *Department for Released Soldiers* do Ministério da Defesa e dezenas de empresas de alta tecnologia, dois programas foram desenvolvidos:

[25]Iniciativa educacional e social, estabelecida em 2000, oferece, aos jovens da periferia, apoio financeiro, acadêmico e social no que se refere ao ingresso no ensino superior e seguimento em carreiras de alta tecnologia, indústria, defesa e serviço público (ATIDIM, 2022).

Data4s e Cyber4s, ambos com parceria estratégica com as FDI e a indústria de alta tecnologia. Os dois programas foram desenhados com o objetivo de facilitar a integração de soldados de combate liberados na indústria de alta tecnologia. Aliás, imagem acima mostra uma comparação entre países sobre a porcentagem de número de funcionários no setor de alta tecnologia. Tendo em vista que a maioria da população israelense já serviu ao exército, tem-se que grande parte desta porcentagem seja de ex-soldados. Nesse sentido, os soldados que participam dos programas são submetidos a rigoroso processo de seleção e são treinados para serem desenvolvedores e analistas de dados. Os programas abrangem treinamento tecnológico profundo, seminários para fortalecer as habilidades sociais, projetos práticos com empresas de alta tecnologia e assistência na colocação de empregos (START-UP NATION, 2022, p. 32).

As FDI, por meio de suas diversas áreas de tecnologia, tornaram-se o principal estímulo para a difusão das tecnologias computacionais e sua aplicação em toda a economia. Além de cursos de TI internos, as FDI, em 2012, iniciaram o curso *Cyber Shield,* o qual treina soldados para proteger os principais sistemas militares no ciberespaço. Este é um programa de treinamento de elite que dura mais de quatro meses. Seus participantes aprendem a manter a segurança da informação, treinando em parte praticando a defesa de redes internas contra ataques simulados (TABANSKY; ISRAEL, 2015, p. 19; YWN, 2013).

Por fim, Israel possui um modelo único de reintegração de veteranos em um país onde o serviço militar é percebido como vantajoso. Israel atrai veteranos, identificados como uma população valorosa, para profissões que considera essenciais, oferecendo benefícios. Essas relações correspondem ao papel social das FDI no contexto israelense e ao serviço obrigatório. De acordo com Swed e Butler (2015, p. 135), há razões para acreditar que um aglomerado de capital militar facilita a reintegração e permite que os veteranos cumpram seu potencial.

Em relação ao papel do governo, um exemplo de um programa que possui consequências significativas na inovação de longo prazo por meio do investimento em capital humano, desenvolvimento de habilidades empreendedoras e tecnológicas aplicadas durante o serviço das FDI é o *Talpiot*. Esta é a unidade mais seletiva e que submete seus soldados ao curso de treinamento mais longo das FDI. Este é um programa de treinamento de elite, de aproximadamente 40 meses, e aqueles que entram no programa se inscrevem por mais seis anos nas forças armadas, o que faz com que o serviço mínimo seja de nove anos (TABANSKY; ISRAEL, 2015, p. 19; SENOR; SINGER, 2009, p. 58-59).

A ideia de *Talpiot* surgiu após a Guerra de Yom Kipur, em 1973. A ideia de juntar os jovens mais talentosos do país e oferecer o mais intensivo treinamento tecnológico que as universidades e os militares tinham a oferecer. Há mais de 30 anos, o programa, administrado por

Maf'at[26] (Diretoria de Pesquisa e Desenvolvimento de Defesa), escolhe anualmente cerca de 2% dos melhores alunos do ensino médio. Posteriormente, *Maf'at* é responsável por atribuir a cada *Talpion* (como são chamados os cadetes que participaram do *Talpiot*), a uma unidade específica nas FDI para seus próximos seis anos de serviço regular (SENOR; SINGER, 2009, p. 60).

Não obstante, o objetivo último do programa não é proporcionar aos alunos uma gama ampla de conhecimento, mas sim transformá-los em líderes orientados para a missão e solucionadores de problemas. A criatividade e a independência são incentivados por meio da atribuição de missão após missão, com orientação mínima. Ademais, a estratégia subjacente por trás do desenvolvimento do programa, isto é, fornecer treinamento para produzir soluções de problemas inovadoras e adaptáveis, é visível em grande parte das forças armadas e parece fazer parte do *ethos* israelense (SENOR; SINGER, 2009, p. 60-61).

Destarte, *Talpiot* recebeu diversas críticas pelo seu alto elitismo. Um dos principais argumentos era que não se sabia se o programa valeria a pena. Além disso, muitos alegaram que o programa é um fracasso, justamente porque a maioria dos graduados não permanece nas forças armadas além dos nove anos exigidos e tampouco termina nos altos escalões das FDI. Isto posto, embora o programa tenha produzido apenas cerca de 650 graduados em três décadas e o treinamento seja otimizado para manter a vantagem tecnológica, a combinação de experiência de liderança e conhecimento técnico é ideal para criar empresas novas. Graduados em *Talpiot* se tornaram alguns dos principais acadêmicos e fundadores das empresas mais bem-sucedidas em Israel (SENOR; SINGER, 2009, p. 60).

O governo israelense também possui o Fundo de Capital Humano para Alta Tecnologia, o qual é destinado a criar soluções inovadoras práticas, ampliar os canais de entrada em alta tecnologia e melhorar o capital humano em posições de P&D e outras posições na indústria de alta tecnologia. Nos últimos dois anos, este fundo tem sido a principal plataforma para treinamentos extra-acadêmicos de alta tecnologia. Ademais, está liderando grandes mudanças no mercado israelense, como um caminho dinâmico e rápido com alta flexibilidade operacional para o desenvolvimento de uma gama de habilidades profissionais, tanto tecnológica quanto empresarial (START-UP NATION, 2022, p.33).

Já no primeiro edital lançado em meados de 2020, foram escolhidos 18 programas diferentes para promover populações sub-representadas no setor – mulheres, árabes, ultraortodoxos e da periferia, além de programas para integrar novos imigrantes e residentes que retornam do

[26]Esta diretoria coordena projetos de P&D entre as FDI, instituições de pesquisa, as indústrias de defesa e os braços governamentais relevantes, tal como a Agência Espacial Israelense. *Maf'at* é paralela ao DARPA *(Defense Advanced Research Projects Agency)* dos Estados Unidos.

exterior com experiência de alta tecnologia. Os programas receberam uma doação total de aproximadamente 19 milhões de ILS[27] (aproximadamente 5 milhões de dólares em 2022) para treinar cerca de 2.800 participantes nos anos de 2021-2022. Já a segunda edição, em 2021, foram doados, para os 49 programas selecionados, um total de cerca de 54 milhões de ILS (quase 16 milhões de dólares) e capacitar cerca de 13.600 participantes nos anos de 2022-2023 (START-UP NATION, 2022, p.33).

É interessante notar que este programa de apoio foi lançado com o fito de enfrentar a crise de empregos devido à pandemia. Diversas bolsas foram aprovadas para que entidades e empresas realizassem processos de formação para profissões de tecnologia e empresariais, sendo estas profissões que estão em crescimento. Nesse sentido, são estas as profissões de P&D na indústria de alta tecnologia que são tidas como um dos recursos mais importantes que preservam a posição de liderança e a competitividade do Estado de Israel, contribuindo para sua economia. Assim, o programa visa apoiar diversas soluções que auxiliam na construção de uma infraestrutura necessária para que empresas possam ser capazes de auxiliar a indústria tecnológica israelense (START-UP NATION, 2022, p.33; ISRAEL INNOVATION AUTHORITY, 2022). Aliás, o *Center for Strategic and International Studies*, em seu estudo sobre a escassez internacional de habilidades de segurança cibernética, afirma que Israel tem a maior taxa de gastos do governo em educação como porcentagem do gasto total do governo, chegando a 19% (CSIS, 2016, p. 9)

Por fim, Israel possui políticas governamentais e leis fundamentais na promoção da inovação. Por exemplo, a Lei de Incentivo à Pesquisa e Desenvolvimento Industrial (Lei de P&D de 1984), em que principais regulamentações são *royalties* e propriedade intelectual, tem como objetivo incentivar as empresas israelenses a investir em projetos de P&D, com o governo compartilhando o risco inerente a tais projetos (TABANSKY; ISRAEL, 2015, p. 23).

O crescimento econômico de um país depende em grande parte da capacidade de gerar melhorias científicas e tecnológicas e de assimilá-las nos processos de produção, bem como em novos bens e serviços. Essas melhorias são criadas por meio de atividades científicas e tecnológicas inovadoras que transformam ideias abstratas em bens e serviços duráveis e constituem a principal fonte de crescimento econômico. A economia israelense há muito enfatiza P&D e inovação como bases. As capacidades desenvolvidas e implementadas para fins militares e de inteligência, tanto no setor militar quanto no civil, produziram um efeito significativo na eco-

[27]Moeda israelense denominada Novo Shekel Israelense (ILS).

nomia. Por exemplo, Israel atualmente aloja centros de P&D da maioria das empresas multinacionais de TI de alta tecnologia (MNCs), tais como Intel, IBM, Microsoft, Google, HP, Yahoo!, Facebook, Oracle, SAP, Cisco, Siemens e EMC. Ademais, em parte por causa da política de inovação aberta e da transferência de conhecimento, é comum que alunos das FDI fundem *startups* e empresas de TI (TABANSKY; ISRAEL, 2015, p. 22-23).

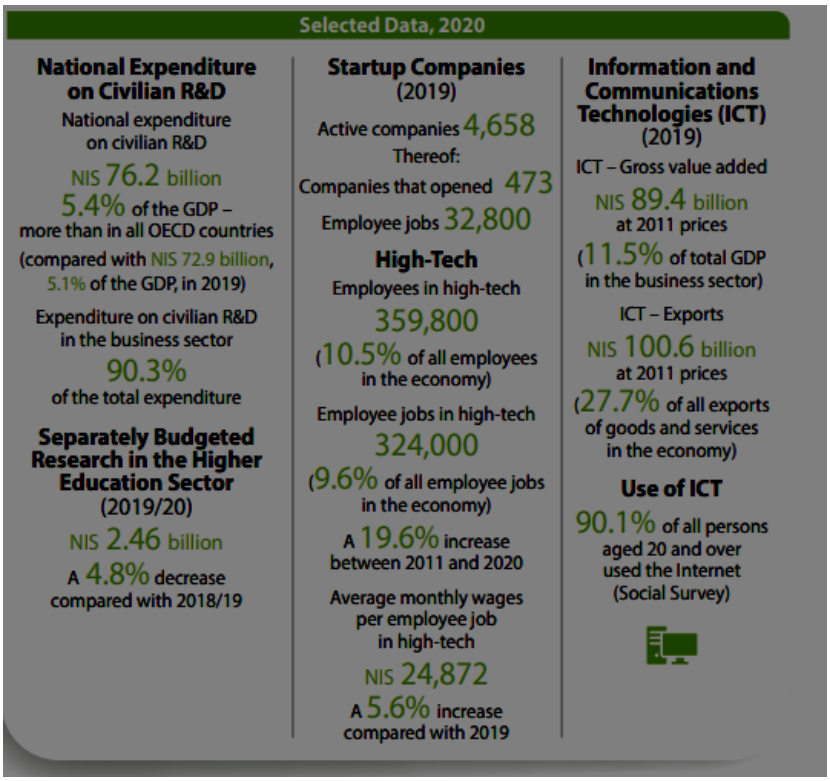
Por exemplo, *CyberSpark*, o ecossistema de inovação cibernética israelense, em Be'er Sheva, é o projeto mais palpável de parceria de defesa cibernética público-privada, criado em 2014 como uma parceria do INCB, do Município de Beersheba, da Universidade Ben Gurion e de parceiros industriais como EMC (RSA), Lockheed Martin, IBM, Deutsche Telekom, JVP Cyber Labs e Elbit. *CyberSpark* tem por objetivo desenvolver e testar novas ideias e conceitos sobre segurança cibernética. As FDI e o CERT-IL também estão envolvidos nas iniciativas do *CyberSpark*, de modo que incluem a comunidade e realizam seminários executivos para o pessoal de segurança cibernética de todo o mundo. Desde o seu lançamento, o *CyberSpark* criou um ecossistema de múltiplas partes interessadas, como governo, academia, indústria, governo local e sociedade civil. Ao trabalhar tão de perto, as partes podem aprender umas com as outras. Desse modo, os militares e o governo realocaram órgãos importantes de sua defesa cibernética para lá, além do setor privado. O governo pretende aumentar a força de trabalho do *CyberSpark* para 2.500 funcionários até 2026 e atrair as principais empresas globais. EMC, Deutsche Telekom, PayPal, Oracle, IBM e Lockheed Martin já abriram escritórios (OCDE, 2020; CSS, 2020, p. 18; IISS, 2021, p. 72; CCDCOE, 2017, p. 14-15; PRESS, 2014).

Além deste programa, existem cerca de 20 centros de P&D de segurança cibernética estabelecidos em Israel por corporações multinacionais para desenvolver soluções de segurança para o mercado global, tais como PayPal, IBM, VMWare, General Electric, Cisco, CA Technologies, McAfee e Ciscom. Atualmente, várias outras corporações globais também estão estabelecendo centros cibernéticos em Israel (CCDCOE, 2017, p. 15). Além disso, há o *CyberNet+*, uma plataforma de troca de informações anônimas, que permite que as FDI cooperem e troquem informações cruciais com o setor privado. Apesar dessas parcerias público-privadas não serem oficiais, elas melhoram os ecossistemas de cooperação (CSS, 2020, p. 18; IISS, 2021, p. 72). Destarte, com o fito de avançar e aumentar a conscientização pública sobre as ameaças no ciberespaço e os meios de enfrentá-las[28], o INCD organiza e financia conferências, tais como *Cyber Week* ou *Cybertech*, criando um espaço cujo objetivo é discutir questões cibernéticas e aumentar a conscientização sobre ameaças cibernéticas (CSS, 2020, p. 18).

[28]Como proposto pela Resolução 3611.

Com mais de 300 centros de P&D, as empresas americanas constituem cerca de 55% de todos os centros de P&D em Israel. Corporações como Intel, IBM, Google, Cisco, Motorola, Philips, Apple, Microsoft e muitas outras investiram e estabeleceram centros de pesquisa em Israel para aproveitar o talento local. Há mais de 6.000 *startups* na economia de Israel, 5 vezes a concentração de *startups per capita* na União Europeia. Existem, além disso, há 80 unicórnios[29] israelenses, com 42 empresas ingressando no clube Unicorn somente em 2021. Uma mudança notável para 2022 é o aumento de empresas iniciantes relacionadas à Inteligência Artificial (IA). Embora Israel tenha apenas 0,1% da população mundial, o país atrai 13% do investimento global em segurança cibernética, ocupa o primeiro lugar globalmente em gastos com P&D por PIB e atrai a segunda maior taxa de financiamento de capital de risco per capita do mundo, depois Cingapura (ITA, 2022). Além disso, o setor empresarial israelense corresponde a quase 80% do total de gastos em P&D no país. As despesas de negócios em pesquisa e desenvolvimento (BERD, na sigla em inglês) como proporção do PIB é a segunda mais alta da OCDE (TABANSKY; ISRAEL, 2015, p. 22).

Figura 11 - Dados sobre ciência, tecnologia e comunicações em Israel

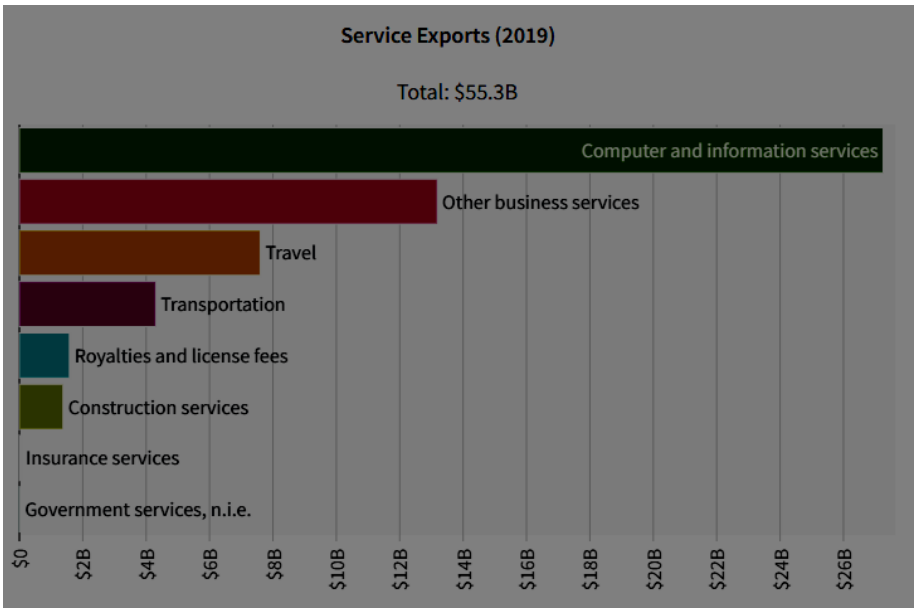


Fonte: CBS, 2021, p. 22

[29]Empresas unicórnios são empresas privadas avaliadas em US$ 1 bilhão ou mais na bolsa de valores.

A imagem acima contém alguns dados importantes quando analisadas as empresas israelenses, tecnologia e o gasto em pesquisa e desenvolvimento. Israel gasta cerca de 5.4% de seu PIB em pesquisa e desenvolvimento, mais que todos os países da OCDE. Além disso, houve um aumento de 5.6% na criação de *startups* em 2019. Existem aproximadamente 424 empresas de segurança cibernética em Israel, e a medição do setor em 2019 estimou as exportações israelenses chegaram a US$ 55,3 bilhões em serviços, sendo os principais serviços de informática e informação (US$ 27,3 bilhões) (OEC, 2022; STATISTA, 2022). A imagem abaixo apresenta os produtos exportados por Israel, demonstrando a importância dos serviços de informática e informação.

Figura 12 - Gama de exportação de serviços israelenses em 2019



Fonte: OEC, 2022

No que tange à academia, as universidades israelenses hospedam quatro dos 50 melhores departamentos de Ciência da Computação. Todas as universidades têm empresas de transferência de tecnologia (TTC) para fornecer as estruturas legais para a comercialização de invenções feitas por professores, alunos e pesquisadores, protegendo descobertas com patentes e trabalhando em conjunto com líderes do setor para trazer inovações científicas do laboratório para o mercado. Essas empresas servem de elo com a indústria, trazendo descobertas científicas realizadas nas universidades para a atenção da indústria, o que facilita a comercialização dos frutos da pesquisa (TABANSKY; ISRAEL, 2015, p. 23 e 26). Nesse sentido, as empresas de

transferência de tecnologia associadas a todas as universidades israelenses fornecem um mecanismo pronto para cooperação com o setor empresarial, protegendo a pesquisa acadêmica e a propriedade intelectual (CCDCOE, 2017, p. 15).

A estratégia formulada é tratada de forma cooperativa, isto é, o INCD criou, financiou e coordenou projetos em toda a economia israelense. Um dos exemplos é o estabelecimento e o cofinanciamento de Centros de Pesquisa Cibernética na maioria das universidades de pesquisa. Estes centros são responsáveis por realizar pesquisas científicas independentes. Outros exemplos são os programas de incentivo à inovação em parceria com a *Israel Innovation Authority* (TABANSKY, 2020, p. 54).

Já em relação à educação secundária, Israel disponibiliza programas de estudo e treinamento de segurança cibernética em todo o país. Exemplos destes programas são *Magshimim*, o qual funciona como medida de enriquecimento aos alunos da periferia geográfica e social após terminarem a escola. O principal programa do Centro de Educação Cibernética, *Magshimim*, visa que o conhecimento e as ferramentas adquiridas aumentem as chances dos alunos a ingressar nas unidades tecnológicas de elite das FDI e continuar uma carreira em alta tecnologia. Dessa forma, o programa atende à crescente demanda por especialistas em segurança cibernética, além da mobilidade social. Este é um curso de três anos com atividades como *hackathons*[30], acampamentos de verão e visitas a empresas de alta tecnologia. O objetivo de longo prazo é criar futuros líderes empresariais e acadêmicos em locais distantes do ecossistema de *startups* de Israel. Muitos dos alunos contratados por empresas de alta tecnologia para empregos de meio período enquanto ainda estão no ensino médio ou antes do alistamento (RASHI FOUNDATION, 2022a; LEICHMAN, 2015; ISRAEL, 2014).

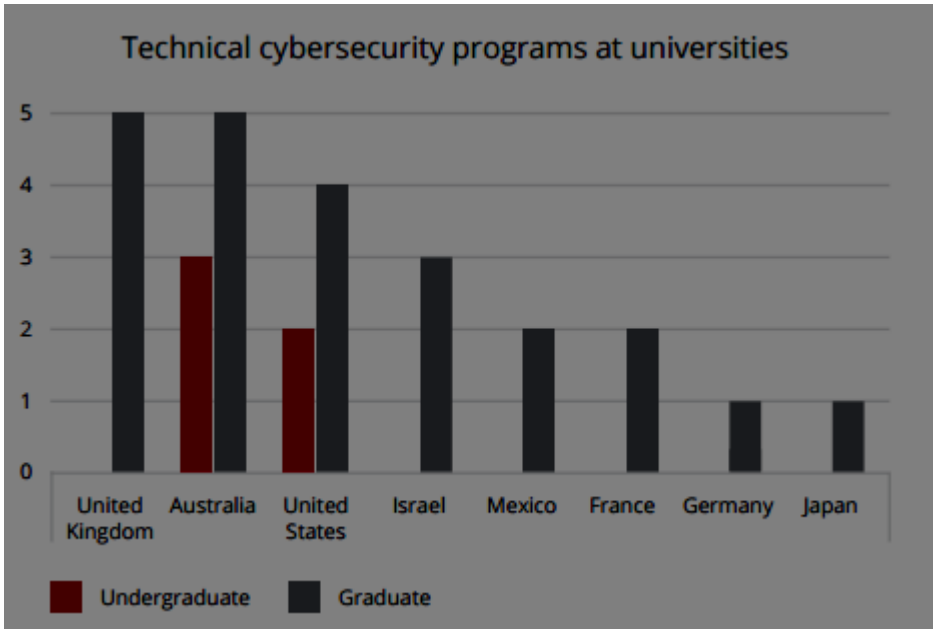
Ademais, o programa *Gvahim* prepara os alunos para um exame de admissão do ensino médio em segurança cibernética, matemática e ciência da computação. Outros exemplos de programas são: *Mamriot*, o qual fornece a adolescentes mulheres conhecimentos e habilidades em cibernética e computadores que possam aplicar em tarefas de tecnologia no serviço militar ou civil e, eventualmente, em carreiras de alta tecnologia; *StarTech*, sendo este um programa de tecnologia para alunos do ensino médio que os apresenta as tecnologias atualizadas enquanto desenvolvem habilidades de autoaprendizagem e trabalho em equipe; e *Science Leadership*, que visa despertar o interesse das crianças pela ciência e tecnologia por meio de atividades de aprendizagem experiencial, com os jovens atuando como conselheiros e enriquecendo suas próprias habilidades e conhecimentos (RASHI FOUNDATION, 2022b; 2022c; 2022d).

[30]*Hackathons* são maratonas de programação. O nome surgiu a partir da junção das palavras inglesas *"hack"* e *"marathon."*

Outrossim, um dos programas disponíveis na graduação, *Excellenteam in Academia*, é a expansão do programa *Excellenteam* que funcionou com sucesso por três anos. O modelo da *Excellenteam in Academia* é baseado no bem-sucedido currículo de *bootcamp* da *Excellenteam*. O programa destina-se aos melhores alunos de graduação como parte do último ano de estudos de Ciência da Computação, com o fito de prepará-los para a entrada no mercado de trabalho de alta tecnologia. *Excellenteam in Academia* é ministrado como um curso acadêmico de aspecto prático, o qual inclui amplo treinamento tecnológico por meio do envolvimento ativo da indústria de alta tecnologia como mentores, entrevistadores simulados e fornecedores de projetos da vida real de suas empresas. Atualmente, o curso está em andamento como piloto no Centro Acadêmico Lev da Faculdade de Tecnologia de Jerusalém, na Faculdade Acadêmica Hadassah da Universidade Aberta e no seminário feminino de Beit Bracha (START-UP NATION, 2022, p. 32; SCALE-UP TEAM, 2022).

Todos esses programas recebem apoio do Ministério da Educação, das FDI e do INCB (CCDCOE, 2017, p. 16). Portanto, Israel utiliza as instituições acadêmicas e industriais em vez de uma academia militar dedicada ou um instituto de pesquisa de defesa (TABANSKY; ISRAEL, 2015, p. 21; GVAHIM, 2022). A imagem abaixo mostra quantos programas técnicos de segurança cibernética nas melhores universidades existem no Reino Unido, na Austrália, nos Estados Unidos, em Israel, no México, na França, na Alemanha e no Japão. Nesse quesito, Israel encontra-se em quarto lugar, com pelo menos, três programas.

Figura 13 - Programas técnicos de segurança cibernética nas melhores universidades

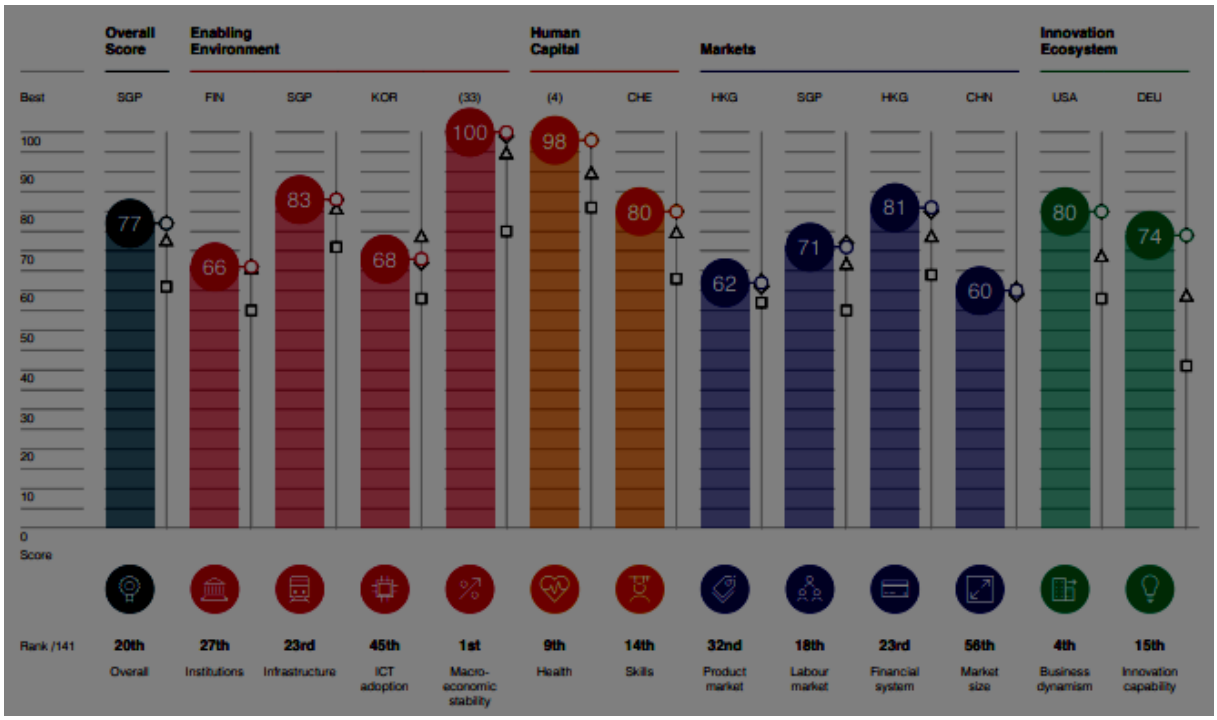


Fonte: CSIS, 2016, p. 10

Um dado interessante é que Israel publica uma porcentagem desproporcional (cerca de 1%) das publicações científicas do mundo em muitos campos, como química e ciências da computação. O *Weizmann Institute of Science* foi um dos primeiros do mundo (em 1958) a criar uma organização para a utilização comercial de suas pesquisas. Atualmente, organizações afins existem em todas as universidades israelenses. O estabelecimento de parques industriais, de base científica, adjacentes aos *campi* universitários obteve grande sucesso comercial. As universidades, da mesma forma, criaram empresas industriais derivadas para a comercialização de produtos específicos com base em suas pesquisas, muitas vezes em parceria com empresas locais e estrangeiras. Institutos interdisciplinares de pesquisa e testes estão funcionando em universidades em campos científicos e tecnológicos vitais para a indústria do país, atendendo áreas como construção, transporte e educação como pontos focais nacionais para P&D aplicado (ISRAEL, 2021d).

Outrossim, Israel está conectado a várias redes globais de pesquisa e desenvolvimento, incluindo a *Next Generation Internet*, a *Internet 2 Network* dos EUA, a rede de dados GEANT da União Europeia para a comunidade de pesquisa e educação e o Sétimo Programa-Quadro (FP7), o Ponto de Presença com sede em Londres, o *Global Forum for Cyber Expertise*, e a extensão *Mediterranean Consortium Quantum* (Q-Med). A cooperação contínua em pesquisa de ICT e segurança cibernética entre os setores industrial e acadêmico em Israel é apoiada e facilitada, em particular, pelo Gabinete do Primeiro-Ministro, o Ministério da Ciência e o Cientista Chefe do Ministério da Autoridade Nacional Econom para Inovação Tecnológica. Dentro do Ministério da Defesa e em cooperação com as FDI, *Maf'at* lidera iniciativas semelhantes e possui uma unidade de pesquisa cibernética dedicada (CCDCOE, 2017, p. 16).

Figura 14 - Visão geral do desempenho de Israel em poder cibernético



Fonte: WORLD ECONOMIC FORUM, 2019, p. 294

A imagem acima apresenta as notas conferidas ao desempenho de Israel em relação ao seu ambiente favorável, capital humano, mercados e ecossistema inovador no que tange ao poder cibernético. Em geral, sua pontuação o classifica na 20º posição. Destarte, a ciência e a tecnologia têm sido tradicionalmente e geopoliticamente equalizadores da inferioridade quantitativa de Israel. Isso grande parte devido a era IT-RMA, quando o ramo cibernético amadureceu. Desse modo, o Estado de Israel tem persistentemente, desde aproximadamente os anos 1960-70, identificando e treinando os melhores e mais brilhantes jovens para e durante a adoção obrigatória do serviço militar (ADAMSKY, 2017, p. 122).

Por consequência, jovens tecnologicamente educados e experientes deixam as forças armadas e ingressam na força de trabalho profissional e acadêmica, aprimorando o ecossistema cibernético nacional. As universidades e as escolas de ensino médio israelenses, bem apoiadas pelo governo, garantem uma sólida base científico-acadêmica para fornecer esse capital humano. A proximidade geográfica-institucional, um estilo de comunicação informal, uma atmosfera de negócios não hierárquica e uma cultura de rede garantiram e fizeram de Israel um centro natural para cooperação cibernética, competição e inovação (ADAMSKY, 2017, p. 122-123).

Uma das principais fontes do sucesso do INCD foi a capacidade de capitalizar os graduados dos mais prestigiados programas de ensino superior militar-tecnológico das FDI, em

particular do *Talpiot*. Tal quadro permitiu que o INCD superasse um grande problema de pessoal característico das organizações de política cibernética em todo o mundo, onde especialistas com formação cibernética têm dificuldade em abraçar perspectivas estratégicas holísticas, enquanto "estrategistas-generalistas" são analfabetos em relação à mecânica profunda do reino cibernético (ADAMSKY, 2017, p. 123).

Em resumo, Israel é um dos poucos países líderes em alta tecnologia, sendo a mesma um dos sintomas mais palpáveis da tecnologia de segurança cibernética. Argumenta-se, portanto, que o ecossistema da inovação existente em Israel é a consequência de sua grande estratégia, sendo esta voltada para a vantagem qualitativa com o fito de aumentar a segurança nacional. Aliás, esta grande estratégia e, por conseguinte, o ecossistema, possui base nas idiossincrasias culturais, criando o cenário propício ao desenvolvimento de capital humano qualificado e inovador, bem como a ciência e a tecnologia de ponta. Estas bases culturais de improvisação e a tomada de decisão sequencial permitem a ação sem a necessidade de formular objetivos e opções claramente articulados e priorizados, os quais facilitam a tomada de decisão em tempos de mudança e crise. Isto, por sua vez, conecta a grande estratégia e a doutrina militar. Todo o conjunto formal e informal relacionados tanto à conjuntura militar, ao contexto tecnológico e às bases culturais, criam um ambiente propício ao desenvolvimento de *startups*, por exemplo.

O cenário instaurado serve o poder cibernético. Se, por um lado, a tecnologia foi crucial para garantir a existência e a vantagem qualitativa nos anos primordiais do país, atualmente ela se destaca por um de seus ramos: o cibernético. O âmbito militar, acadêmico, cultural e governamental trabalham, em conjunto, para conquistá-lo. Para compreender quais podem ser as ramificações deste poder, visa-se explorar as capacidades cibernéticas defensivas e ofensivas no próximo capítulo.

6 CAPACIDADES

As capacidades cibernéticas, nos últimos 20 anos, tornaram-se um instrumento importante de poder nacional. Além de ajudar em operações mais tradicionais, como a espionagem, esta capacidade é utilizada para uma variedade de outros fins mais ameaçadores, tais como: reforçar o próprio desenvolvimento econômico por meio de roubo de propriedade intelectual; ameaçar interromper instituições financeiras, indústrias, usinas nucleares, redes de energia e infraestrutura de comunicações (infraestrutura crítica); interferir em processos democráticos; degradar ou interromper capacidades militares e restringir a capacidade de outro Estado de desenvolver armas nucleares. Atualmente, o ciberespaço se tornou um domínio importante para a política e a concorrência entre os Estados (IISS, 2021, p. 1).

As ameaças direcionadas aos Estados e, por conseguinte, aos seus cidadãos, podem ser diversas e variadas. Nesse sentido, os Estados, ao incorporar capacidades cibernéticas em suas estratégias nacionais de investimento, suas doutrinas e planos militares, aumentando o ritmo de suas atividades cibernéticas, buscando mitigar os riscos que as ameaças cibernéticas representam para suas economias digitais, infraestrutura nacional crítica e cidadãos, o que implica um investimento considerável em recursos de proteção cibernética. Isto posto, os Estados estão fomentando o domínio cibernético, tendo em vista que sua prosperidade econômica, bem como sua segurança nacional e influência geoestratégica, dependem, atualmente, de seu gerenciamento de riscos cibernéticos. Compreender o desenvolvimento e o uso do poder cibernético pelos Estados se tornou crucial ao passo que a prosperidade nacional, a segurança e a política se valem cada vez mais dependentes do ciberespaço (IISS, 2021, p. 2).

O recente estudo sobre capacidades cibernéticas e poder nacional realizado pelo *International Institute for Strategic Studies*, de 2021, oferece um panorama interessante acerca de 15 países[31]. Em geral, os 15 países tiveram certa dificuldade em moldar estruturas políticas consideradas duráveis em relação ao ciberespaço, seja com o objetivo de explorar novas oportunidades ou defender contra novas ameaças. Tendo em vista uma das características principais do ramo cibernético, o dinamismo obrigou os Estados a realizar constantes avaliações e revisões dos principais documentos nacionais de estratégia, de modo que as estruturas tradicionais do governo, a gestão corporativa e a organização social lutam para se adaptar a tempo (IISS, 2021, p. 4-5).

[31]Estados Unidos, Reino Unido, Canadá, Austrália, França, Israel, Japão, China, Rússia, Irã, Coréia do Norte, Índia, Indonésia, Malásia e Vietnã.

Além disso, os países estudados (incluindo as principais potências cibernéticas, tais como os EUA) ainda se encontram nos estágios iniciais de aceitação das implicações estratégicas que o ramo cibernético traz. Não obstante, acordos internacionais implementados por países com o fito de amortecer impulsos competitivos, alguns entendem o ciberespaço como um campo de competição existencial, onde países disputam a capacidade de desenvolver estratégias para o desenvolvimento nacional e depois implementá-las de modo eficaz. Entretanto, dentre os países analisados, poucos possuem alta efetividade neste sentido. Em algumas situações, países menores se encontram em uma melhor classificação do que países maiores, como é o caso de Israel (IISS, 2021, p. 5).

Em geral, as potências cibernéticas pressionam para obter uma resposta da "sociedade como um todo" em relação à segurança nacional, isto é, uma estreita parceria e o compartilhamento de informações entre setores público e privado, academia e parcerias civis-militares, bem como esquemas inovadores de *upskilling* (desenvolvimento de habilidades já existentes) e educação e campanhas destinadas a aumentar a conscientização da população. Cada tipo de governo (autoritário ou democrático-liberal) e método *(top-down* ou *bottom-up)* implementado possui pró e contras, mas as democracias-liberais, as quais possuem uma abordagem mais distribuída com a inovação nacional amplamente impulsionada pelo setor privado e pela academia, parecem possuir o método mais efetivo, com a governança equilibrada entre os governos nacionais, o setor privado, organizações não-governamentais e academia. De acordo com o estudo, os 15 países estão desenvolvendo este tipo de respostas (IISS, 2021, p. 6). Nesse sentido, eles estão reconhecendo a importância de fomentar as empresas de segurança cibernética, tendo em vista que as mesmas são essenciais para formar um setor industrial efetivo. Entretanto, apenas Estados democráticos-liberais estão conseguindo alcançar este objetivo (IISS, 2021, p. 172).

Existem abordagens para o desenvolvimento e uso da capacidade cibernética, particularmente a ofensiva, pelas principais potências. Países maiores e com maior poder de investimento, tanto pessoal quanto orçamentário, separam as capacidades militares de propriedade civil, em que os laços civis-militares são mais fortes. Por outro lado, países menores, como Israel, tendem a ter uma abordagem civil-militar mais fundida, o que visa a compensar a escassez de recursos por meio da maior agilidade operacional (IISS, 2021, p. 5).

A mensuração da capacidade do poder cibernético é complicada, tendo em vista que os indicadores, muitas vezes, são difíceis de serem mensurados ou até impalpáveis e invisíveis. Por exemplo, há de se levar em consideração o capital humano, o orçamento e a qualidade das tecnologias disponíveis e que estão sendo utilizadas. O primeiro é particularmente custoso de

mensurar, pois o número de pessoas alocadas a papéis cibernéticos não consideram setores públicos e privados mais amplos que influenciam a capacidade cibernética.

Além disso, o esforço dedicado ao efeito militar também é difícil, pois as parcerias entre as forças armadas, as organizações civis e o setor privado são feitas de maneiras e proporções diferentes a depender do país. O tamanho do investimento financeiro em capacidades cibernéticas se encontra na mesma situação. Destarte, um dos fatores que leva ao desenvolvimento do poder cibernético é, por exemplo, a vontade política e a qualidade das operações cibernéticas com o fito de atingir objetivos políticos específicos. Apesar da escassez de profissionais qualificados neste ramo, países que carecem de recursos e conhecimento podem compensar através de alianças internacionais. França, Israel e Japão estão entre os Estados que também têm alianças cibernéticas mutuamente benéficas (IISS, 2021, p. 6-7).

Como já mencionado, os Estados já alteraram suas estratégias, doutrinas e estruturas militares com o objetivo de reconhecer tanto as oportunidades quanto as ameaças advindas das tecnologias cibernéticas. Os EUA e a China prevêem que guerras futuras sejam travadas em um ciberespaço. Sendo assim, fatores como a escala da vulnerabilidade cibernética em sistemas herdados, o potencial nacional ciber-industrial e de habilidades, a extensão da confiança na capacidade de inteligência civil, o compromisso da liderança e a resistência dos militares tradicionalistas foram fundamentais para que ocorresse essa transformação. Aliás, em maior ou menor grau, a expansão do desenvolvimento e uso de capacidades cibernéticas pelos países foi intensificada por choques estratégicos (IISS, 2021, p. 8-9).

De modo geral, a estratégia e a doutrina publicadas dentre os países estudados demonstram alterações notáveis na prática, especialmente no equilíbrio entre as políticas de segurança cibernética e as políticas sigilosas para usos militares, políticos e de inteligência de ativos cibernéticos. Atualmente, os 15 países possuem algum tipo de estratégia, doutrina ou política publicada pelo menos em uma área do poder cibernético. Entretanto, nenhum país se encontra satisfeito com seu próprio nível de maturidade em estratégia cibernética, muito por conta da rapidez com que as ameaças e desenvolvimentos cibernéticos se dão. Destarte, é visível como a cultura política de cada país é determinante nos arranjos de governança, comando e controle (IISS, 2021, p. 171).

Outrossim, nenhum Estado foi capaz de progredir o suficiente para permitir que suas respectivas forças armadas reivindiquem capacidades cibernéticas bem integradas e disseminadas. Com exceção de Israel, nenhum Estado pôde difundir suas capacidades cibernéticas por meio de sua estrutura de força. Aliás, há indícios de que ela pode levar a problemas de comando

e controle, apesar da estreita integração entre as capacidades cibernéticas das forças armadas e das principais agências de inteligência, as quais parecem ser fundamentais para a transformação militar (IISS, 2021, p. 173).

O estudo também aponta que especialmente por causa da ausência de um ataque cibernético significativamente destrutivo, a taxa média de progresso na reforma da política cibernética não é rápida, ou seja, os processos reformatórios podem levar cerca de uma década para produzir uma mudança considerável. Um dos maiores impedimentos para este progresso é o capital humano qualitativo, i.e. força de trabalho qualificativa e, novamente, Israel parece ser outra exceção, pois adotou uma abordagem suficientemente radical para melhorar a qualificação de seus cidadãos (principalmente por meio do recrutamento militar) (IISS, 2021, p. 173). Por fim, os Estados mais capacitados ciberneticamente (EUA e China) concordam que a capacidade cibernética sustenta o poder militar e pode afetar radicalmente a tomada de decisões e o controle da maioria dos sistemas militares e formações de força. O relatório do IISS atesta que a noção tradicional de equilíbrio de poder baseada em arranjos geopolíticos está sendo substituída paulatinamente pela ideia de um equilíbrio de poder informacional (IISS, 2021, p. 174).

De acordo com *The Hague Centre for Strategic Studies*, em seu estudo C*yber Arms Watch: An Analysis of Stated & Perceived Offensive Cyber Capabilities,* considera-se que há uma falta de transparência no que tange à sua capacidade cibernética israelense. Embora as estratégias israelenses identifiquem abertamente o ciberespaço como um domínio de guerra e se refiram ao estabelecimento e aos esforços contra adversários, os quais minam os interesses nacionais, os documentos oficiais não vão além do reconhecimento de capacidades ofensivas, e nenhuma das doutrinas militares divulgadas ao público possui princípios básicos de engajamento (HCSS, 2022, p. 99).

Não obstante, o país é percebido pelo resto do mundo como um dos que detém uma das capacidades cibernéticas militares mais desenvolvidas e pronta para ser utilizada com o fito de alcançar seus objetivos estratégicos nacionais. Pelo menos duas instituições, em Israel, são encarregadas por implementá-los: a Direcção C4I, para operações de defesa, e a Unidade 8200, para operações ofensivas. Com efeito, operações cibernéticas ofensivas contra adversários regionais, as quais incluem ações de inteligência e estratégicas, como *Stuxnet*, *Flame*, *Duqu*, e atividades cibernéticas e eletromagnéticas táticas, tais como a Operação Orchard, serão abordados doravante. Ambos os estilos de operações têm sido constantemente atribuídos a Israel (HCSS, 2022, p. 99). Para tanto, o país trabalha em estreita colaboração com seus aliados, em destaque com os EUA. Ademais, a forte base da indústria de segurança cibernética israelense é considerada de alto valor agregado para as forças armadas (HCSS, 2022, p. 105).

Figura 15 - Comparação dos 10 principais poderes cibernéticos em 2020 e 2022

Rank	2020	2022
1	US	US
2	China	China
3	UK	Russia
4	Russia	UK
5	Netherlands	Australia
6	France	Netherlands
7	Germany	ROK
8	Canada	Vietnam
9	Japan	France
10	Australia	Iran

Fonte: BELFER CENTER, 2022, p. 10.

O instituto Belfer Center, em seu estudo denominado *National Cyber Power Index 2022*, apresenta, na imagem acima, uma comparação entre os dez principais países detentores de poderes cibernéticos em 2020 e 2022. Neste estudo, foram utilizados 29 indicadores que, por sua vez, contribuem para tanto a intenção quanto as capacidades. Além disso, foram avaliadas estratégias nacionais de todos os países estudados para, enfim, rastrear o poder cibernético como um conjunto interconectado e em evolução com as políticas e capacidades que incorporam a amplitude das atividades de um Estado. O instituto, portanto, mediu estratégias governamentais, capacidades para operações defensivas e ofensivas, alocação de recursos, capacidades do setor privado, como empresas de tecnologia, força de trabalho e inovação (BELFER CENTER, 2022, p. 2-3).

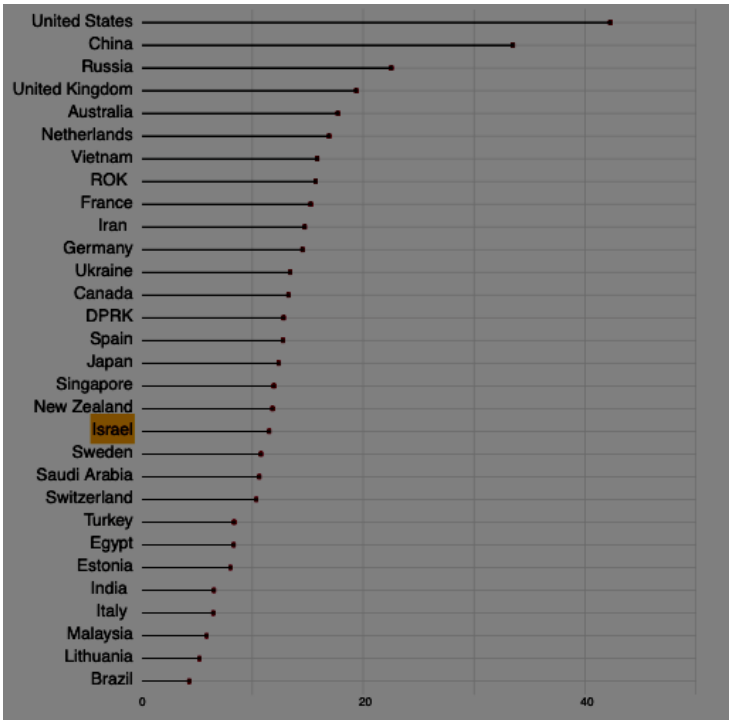
É interessante notar que, devido à natureza dos dados, as alterações que ocorreram não podem ser tidas como absolutas, no sentido de que as informações coletadas são somente aquelas fornecidas publicamente e, portanto, devem ser vistas como uma alteração relativa do poder cibernético. Nesse sentido, vale evidenciar que alguns Estados não disponibilizam dados. Um dos maiores desafios em se estudar o poder cibernético remete à sensibilidade e classificação de documentos, tais como o número de militares, capacidades de inteligência, capacidades destrutivas, defensivas e de espionagem e sua dependência de estruturas domésticas de segurança nacional (BELFER CENTER, 2022, p. 14).

Outra questão chave é que nenhum Estado que se vale de meios cibernéticos, como o *ransomware*, declarará ou publicará abertamente suas operações ofensivas (realizadas ou em

andamento), bem como o número de funcionários trabalhando nestas operações, principalmente se essas operações forem bem-sucedidas o suficiente para não serem detectadas e não relatadas publicamente. China, Israel, Irã e Coreia do Norte são exemplos particulares desse tipo de Estado e sigilo e, por conseguinte, são subclassificados (BELFER CENTER, 2022, p. 14).

Tendo isto em vista, e a partir das informações aqui expostas e dos relatórios utilizados, pode-se afirmar que Israel é subclassificado, especialmente porque, em alguns relatórios, Israel não ofereceu as informações necessárias para que houvesse uma análise efetiva de sua capacidade. Cada relatório, entretanto, possui a sua própria metodologia e seus resultados podem divergir ligeiramente. Não obstante, os países não parecem ter posições tão divergentes. Em geral, Israel ocupa boas posições: 36º de acordo com o *National Cyber Security Index* e *Global Cybersecurity Index*, 23º e 22º no *ICT Development Index* e *Networked Readiness Index*, respectivamente (NCSI, 2021). De acordo com Kaspersky (2021), Israel é o 103º país mais atacado no mundo. A imagem abaixo mostra a classificação mais recente, a qual inclui os 30 principais países no que se refere ao poder cibernético.

Figura 16 - Índice nacional de poder cibernético: classificação geral 1-30



Fonte: BELFER CENTER, 2022, p. 10.

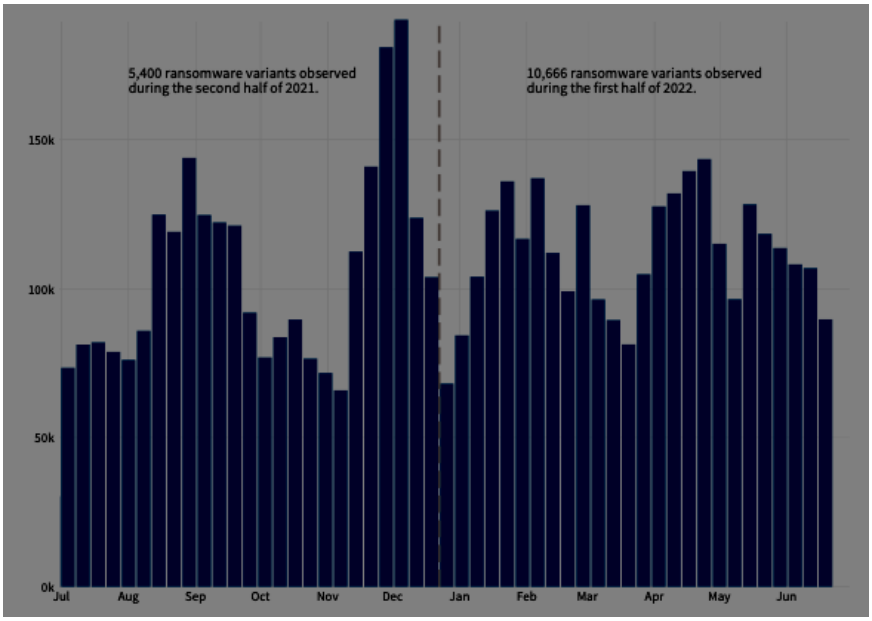
Com a ascensão da interconectividade mundial, do desenvolvimento e incorporação da tecnologia de ponta e do progresso do mundo cibernético, agentes passaram a desenvolver ferramentas e agarrar as oportunidades advindas das lacunas existentes. Mais recentemente, o ano de 2021 foi intrigante, pois novas ameaças surgiram e agentes de ameaças evoluíram, ininterruptamente, suas táticas utilizadas com o objetivo de manter ou melhorar a própria posição no cenário geral de ameaças. Neste ano, o *ransomware* (ataques direcionados projetados para paralisar as redes das vítimas) permaneceu como a ameaça mais séria enfrentada pelas organizações, principalmente por ser extremamente lucrativo para quem o pratica. Agora, o *ransomware* é, definitivamente, o ponto central de todo o ecossistema do crime cibernético, financiando um número cada vez maior de grupos de ataque afiliados e fornecendo novos fluxos de renda para uma ampla gama de invasores, como *spammers*, operadores financeiros de cavalos de Tróia e especialistas em invasões (SYMANTEC, 2021a, p. 1).

Para além do r*ansomware*, houve outros desenvolvimentos iminentes, tais como o aumento na escala e na ambição dos ataques à cadeia de suprimentos (*supply chain)*. *SolarWinds* e *Kaseya* são exemplos deste tipo de operação onde encontraram um novo multiplicador de força para suas táticas. Porém, talvez o ataque mais chamativo tenha sido o *ransomware* direcionado ao oleoduto, *Colonial Pipeline*, nos Estados Unidos. Ataques cujo objetivo é financeiro não é a única ameaça. Estados também possuem incentivos a causar perturbações e criar pânico entre seus rivais. Nesse sentido, há uma gama cada vez maior de adversários altamente motivados e com recursos cada vez maiores (SYMANTEC, 2021a, p. 2).

Outra tendência que surgiu, durante 2021, foram quadrilhas de *ransomware* visando os setores de saúde, ou seja, os mais afetados pela pandemia do COVID-19. Por exemplo, o serviço nacional de saúde da Irlanda, o *Health Service Executive*, sofreu ataques, os quais foram realizados quando os serviços hospitalares estavam sob forte pressão, com os atacantes provavelmente acreditando que isso funcionaria a seu favor e forçaria as autoridades a ceder às suas demandas. O estudo realizado pela Symantec (2021a, p.2) demonstra todas as detecções de *ransomware* de janeiro de 2020 a setembro de 2021. Apesar da diminuição de ataques, a baixa nos números se deveu, majoritariamente, aos ataques relativamente pouco sofisticados e indiscriminados, mas sobretudo no maior foco contra grandes organizações. Embora as detecções gerais de *ransomware* estejam diminuindo, os ataques direcionados estão aumentando. Nesse sentido, o número de organizações vítimas de ataques direcionados aumentou de cerca de 80 em janeiro de 2020 para mais de 200 em setembro de 2021. Este fato é, em partes, promovido pelo do *ransomware-as-a-service* (RaaS) (SYMNTEC, 2021a, p. 2).

Para os desenvolvedores de *ransomware*, RaaS foi essencial, pois, ao alugar suas ferramentas para outros invasores em troca de uma parte dos lucros, os operadores de *ransomware* podem maximizar suas receitas e fornecer um caminho para invasores que podem não ter as habilidades para criar sua própria operação de *ransomware.* Isto significa um aumento na quantidade de adversários que as organizações têm de enfrentar, tendo em vista que mais agentes utilizam o mesmo *ransomware*, porém com táticas, técnicas e procedimentos (TTPs) diferentes. Observa-se, portanto, que houve um aumento na sofisticação e complexidade dos RaaS (SYMANTEC, 2021a, p. 5). A figura abaixo mostra o volume semanal de *ransomware* nos últimos seis meses de 2021 e nos primeiros seis de 2022.

Figura 17 - Volume semanal de ransomware de 2021 (jul-dez) a 2022 (jan-jun)



Fonte: FORTINET, 2022, p. 13

Outra importante tendência que auxilia para o aumento dos ataques é o aparecimento dos *Initial Access Brokers* (IABs). Este tipo de ataque consiste em agentes que obtiveram acesso às redes e que, posteriormente, vendem normalmente para operadores de *ransomware*. Os IABs permitem que os mesmos evitem o processo oportuno de encontrar e comprometer organizações vulneráveis, liberando-os para se concentrarem em extorquir suas vítimas (SYMANTEC, 2021a, p. 3).

Em 2020, aplicativos voltados ao público foram vítimas de um aumento de invasores que objetivavam explorar as vulnerabilidades existentes, com o fito de obter acesso às redes das

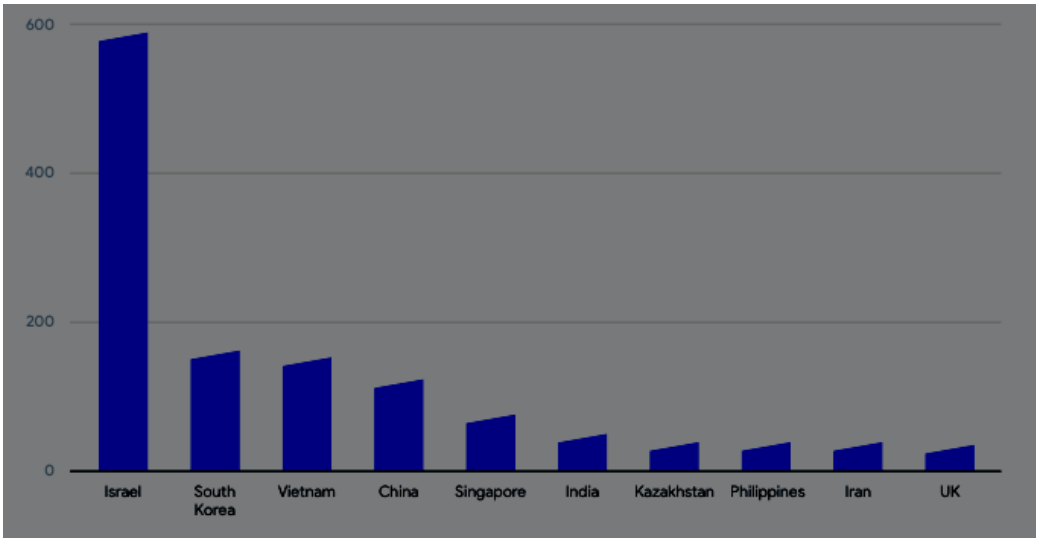
organizações. Por vezes, estes ataques são explorações de vulnerabilidades de dia zero[32], mas, mais frequentemente, o foco está nas vulnerabilidades corrigidas recentemente e na busca por sistemas não corrigidos. O maior exemplo remete à descoberta de várias vulnerabilidades críticas no Microsoft Exchange Server, conhecidas coletivamente como *ProxyLogon* (SYMANTEC, 2021a, p. 6).

Destarte, muitos desenvolvedores de *ransomware* utilizam ferramentas legítimas ou recursos já existentes das próprias organizações para alcançar seus objetivos. De certa maneira, esta tática auxilia os invasores a permanecerem indetectáveis e poupa tempo e recursos na produção de suas próprias ferramentas. Em geral, as táticas utilizadas podem ser divididas em 12 categorias: acesso inicial; execução; persistência. Escalonamento de privilégios; evasão de defesa; acesso a credenciais; descoberta; movimento lateral; coleta; comando e controle; exfiltração; impacto. Dentro dessas categorias, existem 245 técnicas de ataque distintas (SYMANTEC, 2021a, p. 12).

Em relação aos ataques à infraestrutura nacional crítica (INC), estes podem ser os mais perigosos caso sofram ataques cibernéticos efetivos, pois as redes de infraestrutura crítica possuem a capacidade de afetar a sociedade como um todo. Atualmente, as redes de infraestrutura crítica cresceram a ponto de executar os sistemas de comando e controle, gerenciar a logística, permitir o planejamento e as operações da equipe e são a espinha dorsal dos recursos de inteligência, bem como podem interromper os serviços públicos que as pessoas usam diariamente, como energia, água, transporte, dentre outros (SYMANTEC, 2021a, p. 8; ANDRESS; WINTERFELD, 2014, p. 5).

[32]Este termo é utilizado para descrever as vulnerabilidades de segurança recentemente descobertas, das quais *hackers* podem utilizar para atacar os sistemas. Um ataque, neste momento, acontece quando os *hackers* se valem desta vulnerabilidade antes que os desenvolvedores tenham a chance de consertá-la (KAPERSKY, 2022).

Figura 18 - Distribuição geográfica de envios relacionados a ransomware



Fonte: VIRUSTOTAL, 2021, p. 5

Na figura acima, Israel se destaca em envios relacionados ao *ransomware*, com uma alta de quase 600% em comparação com sua linha de base[33]. Não obstante, em 2021, a Point Software Technologies Ltd., empresa israelense e fabricante de *firewalls* de segurança cibernética, publicou que houve um aumento de 93% nos ataques globais de *ransomware*, sendo 20% em setembro e outubro, 41% de abril e outubro e 93% de 2020 a 2021. No primeiro semestre de 2021, Israel viu, em média, 2,5 vezes mais ataques de segurança cibernética do que a média global. Em outra perspectiva, as organizações israelenses viram uma média de 1.000 ataques semanais por organização, ou seja, um aumento de 76% desde o início de 2021, em comparação com o aumento de 29% na média global (SOLOMON, 2021; VIRUSTOTAL, 2021, p. 5). Apesar disso, Basel (2020) considera Israel como um dos países com menor risco de sofrer lavagem de dinheiro e financiamento do terrorismo (posição 130 de 141 países analisados).

Destarte, *Computer Network Attack* ou Ataque à Rede de Computadores (CNA) é um termo militar definido como "ações tomadas através do uso de redes de computadores para interromper, negar, degradar ou destruir informações residentes em computadores e redes de computadores, ou os próprios computadores e redes" (ANDRESS; WINTERFELD, 2014, p. 181). Vale salientar que há uma grande diferença em como essas atividades são conduzidas por Estados-nação e agentes não-estatais. Quiçá, a única semelhança existente entre ambos seja a

[33]O relatório não deixa claro qual é a linha de base de Israel.

de que pequenos grupos ou indivíduos podem manejar armas parecidas com um nível de eficácia semelhante ao de um Estado. Isto é, um indivíduo com acesso ao sistema de comando e controle de uma grande rede de *bots* pode causar prejuízos e estragos, mas não detém capacidade de transpor o ataque para o nível de guerra convencional (ANDRESS; WINTERFELD, 2014, p. 181).

Em resumo, a diferença consta na escala das capacidades e a abrangência do processo de ataque. Nesse sentido, a maioria dos indivíduos invasores não tomam medidas destrutivas. Na guerra cibernética total, ou seja, onde haveria uma maior intenção de impacto, o qual levaria à destruição total ou, pelo menos, à desativação de infraestrutura crítica ou de sistemas que fornecem proteção contra um ataque convencional. Isto posto, a capacidade cibernética adiciona novas dimensões aos métodos tradicionais de guerra, o que implica a consideração de fatores físicos, eletrônicos e lógicos da guerra, bem como as ações e o tempo (ANDRESS; WINTERFELD, 2014, p. 181-182).

O processo de ataque normalmente é aplicado em um sistema específico ou em um conjunto de sistemas. De acordo com Andress e Winterfeld (2014, p. 184), há sete etapas: reconhecimento, varredura, acesso, escalonamento, escape (*exfiltrate*), assalto e sustentação. O primeiro processo seria realizado de forma geral, com o fito de mapear e descobrir informações sobre o ambiente. Nessa circunstância, a engenharia social é uma ferramenta possivelmente útil, pois permite acessar os sistemas sem precisar recorrer ao espectro de ataques, o que possibilita descobrir senhas compartilhadas usadas em outros serviços ou aplicativos, encontrar nomes de contas pesquisando o ambiente físico daqueles que trabalham ou qualquer outra tática semelhante. Além disso, há a possibilidade de detectar credenciais do tráfego de rede se protocolos menos seguros forem permitidos, tais como *telnet, File Transfer Protocol* (FTP) ou *Post Office Protocol* (POP) (ANDRESS; WINTERFELD, 2014, p. 185).

O processo de varredura se dá mais pela busca de possíveis vulnerabilidades durante o reconhecimento. Nesta fase, informações potencialmente mais específicas do sistema operacional são verificadas. Apesar de ser um processo demorado, pode ser útil, pois há a possibilidade de descobrir informações muito específicas, como versões de banco de dados de mensagens de erro, nomes de usuários em potencial ao conduzir ataques de injeção de *Structured Query Language* (SQL) por meio da interface da *Web* e qualquer número de outros *bits*, informações adicionais sobre o sistema operacional, como informações específicas sobre *patches*, tempo de atividade ou qualquer um de outros itens que podem potencialmente permitir obter informações

por meio de inferência. A coleta dessas pequenas informações pode ajudar no processo de escalonamento (ANDRESS; WINTERFELD, 2014, p. 186).

O acesso pode ocorrer por meio de uma variedade de ferramentas e métodos. Para além da engenharia social ou clonagem de cartões de acesso, outro caminho potencial é o ataque contra sistemas individuais que pertencem aos usuários do sistema em foco. Esse ataque utiliza vulnerabilidades no *software,* como um navegador da *Web,* e-mail como método de entrega ou uma unidade USB, como um vetor de ataque. Ademais, também é possível realizar ataques utilizando sistemas operacionais comuns ou de exploração de aplicativos. Particularmente em ambientes de trabalho não técnicos. Particularmente, tais ataques têm um alto grau de sucesso, embora sem tanto sucesso em ambientes altamente seguros. Destarte, é importante que o atacante possa testar os ataques em um ambiente mais semelhante possível do real alvo, pois permite não somente testar as ferramentas, mas também ajudar a desenvolver planos de contingência para compensar possíveis problemas que possamos encontrar ao atacar (ANDRESS; WINTERFELD, 2014, p. 187-188).

Após estas etapas, pode-se obter o que é conhecido como escalonamento de privilégios (adicionais ou atualizados). Quando se tenta obter acesso a contas com um maior nível, tem-se o escalonamento vertical de privilégios. Já quando se tenta obter a contas diferentes, porém do mesmo nível, há o escalonamento horizontal de privilégios. Ambas podem ser realizadas por uma variedade de métodos, tais como usar um conjunto diferente de explorações, tirar proveito de configurações incorretas ou configurações inseguras, utilizar os privilégios de aplicativos (como aqueles que executam *backups*), ou acessar e modificar *shell scripts* que não são protegidos adequadamente, com o objetivo de passar comandos ou obter acesso direto a um *shell* do sistema operacional (ANDRESS; WINTERFELD, 2014, p. 187-188).

Já em relação ao escape, uma das principais preocupações é encontrar todos os dados que possam ser valiosos e exportá-los para um outro local acessível ou ao próprio sistema. Esta etapa é um ataque principalmente contra a confidencialidade e potencialmente contra a disponibilidade. Isto posto, é possível utilizar desde ferramentas e protocolos criados especificamente ou genericamente para mover dados, métodos *out-of-band*[34] para permitir subverter as medidas de segurança projetadas especificamente para impedir tais esforços. Em casos simples, a transferência pode ser realizada por *File Transfer Protocol* (FTP), *Secure Copy Protocol* (SCP), *Extensible Messaging and Presence Protocol* (XMPP) ou qualquer um de outros protocolos co-

[34]Este termo se refere às atividades que ocorrem fora da frequência específica de telecomunicações. Normalmente é utilizado para falar sobre mensagens ou sinalização multicanais.

muns. Entretanto, é necessário a criação de ferramentas apropriadas para mover dados em alguns casos. Aqui, *netcat* pode ser uma ferramenta muito poderosa para mover dados de maneira personalizada, pois permite configurar portas específicas em cada extremidade da conexão e até mesmo retransmitir os dados por meio de sistemas para extraí-los (ANDRESS; WINTERFELD, 2014, p. 188).

Em seguida, o ataque é utilizado na guerra cibernética para provocar perturbações. Em termos militares, podemos realizar os 5Ds: engano, perturbação, negação, degradação e destruição. Dessa maneira, ataques de negação de serviço (DoS) e DDoS são uma ocorrência frequente, tendo em vista a facilidade com que podem ser executados. Estes tipos de ataques são, geralmente, lançados contra servidores da *Web*, de e-mail, FTP e infraestrutura organizacional, mas também contra componentes tecnológicos de sistemas de controle de acesso físico. Nesta etapa, o desempenho do sistema e das redes, a produção industrial e a degradação de dados sejam alterados de forma a influenciar decisões, por exemplo (ANDRESS; WINTERFELD, 2014, p. 189-190).

Por fim, após concluir todas as etapas, é preferível que o acesso posterior seja garantido, criando novas contas, abrindo serviços em portas adicionais, instalando *software* de comando e controle, colocando *backdoors* em aplicativos, dentre outros. Caso não seja realizado, é possível que a invasão seja identificada ou outro invasor também obtenha acesso e compartilhe o controle do sistema, o que pode desencadear uma investigação e provavelmente cortar o acesso adquirido. Vale ressaltar que durante todas as etapas, o fim último será o ocultamento, que pode ser por meio de *proxies* ou máquinas intervenientes empregadas como uma conexão intermediária antes do ataque, falsificação de IP ou qualquer um de outros métodos que podemos usar para disfarçar o ponto de origem. Além disso, é possível pagar evidências da intrusão, ao limpar todas as ferramentas movimentadas e remover ou alterar entradas de registro. Porém, também é possível deixar os rastros e alterá-los para que apontem para uma outra fonte, isto é, atribuir falsamente um ataque a outra fonte, causando confusão e consternação significativas (ANDRESS; WINTERFELD, 2014, p. 190-191).

Talvez o caso mais emblemático que envolva Israel é o *Stuxnet*. Acredita-se que o ataque tenha se iniciado em 2007 por meio de um *malware* implantado em centrífugas em uma usina de enriquecimento de urânio no Irã, apesar de só ter sido descoberto e divulgado em 2010, tendo já infectado aproximadamente 100.000 hospedeiros, 60% dos quais no Irã e 40% em outros países. Este caso é o primeiro exemplo de que um ataque cibernético pode ter impactos físicos

e danificar infraestruturas críticas. A arma digital, que se acredita ter sido criada em uma parceria entre Israel e Estados Unidos, alterou a velocidade da centrífuga e a danificou, diminuindo sua produção em um terço. Este foi um ataque altamente sofisticado que pretendia infectar o software *Siemens Step7* em computadores que controlam controladores lógicos programáveis (PLCs), porém um erro no código fez com que ele se espalhasse para um computador que havia sido conectado às centrífugas (SYMANTEC, 2021b, p. 14; TABANSKY; ISRAEL, 2015, p. 66).

Outra parceria realizada entre os Estados Unidos e Israel foi o vírus *Flame*, o qual também visava sabotar o programa nuclear iraniano. Este vírus, por sua vez, possibilitou que Israel tirasse capturas de tela, visualizasse o tráfego de rede e recuperasse informações de computadores infectados. Destarte, há indícios de que Israel teria utilizado ferramentas cibernéticas em cooperação a operação de combate, como o ataque aéreo ao reator nuclear sírio em 2007, supostamente realizado. Demais relatórios concluem que, para tanto, Israel teria assumido o controle dos sistemas de radar sírios e os reprogramou temporariamente para se passar despercebido, principalmente enquanto o ataque estava em andamento (FREILICH, 2018b, p. 229-230).

Para fins defensivos, *Computer Network Defense* ou Defesa de Rede de Computadores (CND) são "ações tomadas para proteger, monitorar, analisar, detectar e responder a atividades não autorizadas dentro dos sistemas de informação e redes de computadores do Departamento de Defesa" (ANDRESS; WINTERFELD, 2014, p. 193). Aqui, muitas estratégias e táticas desenvolvidas e utilizadas pela CNA podem servir para fortalecer a defesa, além de ser possível encontrar abordagens civis e militares extremamente semelhantes, justamente por conta do uso das mesmas táticas e equipamentos. Militarmente falando, a defesa de rede de computadores pode estar em paralelo às estratégias e táticas utilizadas na defesa convencional, no sentido em que as posições defensivas, postos de escutas, patrulhas e afins, bem como as estratégias da guerra convencional, podem ser ajustadas à guerra cibernética. Apesar de não ser totalmente eficiente, é possível testar conceitos antigos no âmbito cibernético, o que pode prejudicar a defesa na área da CND (ANDRESS; WINTERFELD, 2014, p. 193).

Destarte, vale examinar o que está sendo defendido caso ocorra um ataque. Informações confidenciais geralmente são categorizadas como informações de identificação pessoal ou informações de saúde do paciente, as quais, quando comprometidas, podem levar a uma variedade de atividades fraudulentas. Já quando essas informações estão relacionadas às forças armadas e ao governo, são categorizadas como não classificadas (U), não classificadas apenas para uso oficial (U//FOUO), confidenciais (C), secretas (S) e extremamente secretas (TS). As informações armazenadas por tais instituições podem conter ordens de operações, planos de guerra,

movimentos de tropas, sistemas de coleta de inteligência ou quaisquer itens críticos para seu funcionamento. Apesar de haver inúmeras leis e regulamentos muito rígidos com o objetivo de proteger tais informações, ainda há muito a se fazer (ANDRESS; WINTERFELD, 2014, p. 194-195).

Medidas empregadas com o fito de proteger as informações podem ser descritas como a tríade clássica da *Central Intelligence Agency* (CIA): confidenciabilidade, integridade e disponibilidade dos dados. A primeira se refere a conservá-los longe do alcance daqueles que não estão autorizados. O segundo se refere à prevenção de alterações não autorizadas tanto nos dados quanto nas funções do sistema, o que normalmente implica controles de acesso e criptografia, considerando tanto os dados em repouso quanto os dados em movimento, justamente porque o lugar onde um dado se encontra em um dado momento, pode ser necessário a utilização de ferramentas de segurança diferentes. Especificamente, *hashes* ou resumos de mensagens, como MD5 e SHA1, são frequentemente usados para garantir que mensagens ou arquivos não tenham sido alterados, criando uma impressão digital dos dados originais que podem ser rastreados ao longo do tempo (ANDRESS; WINTERFELD, 2014, p. 195-196).

Por fim, a disponibilidade se refere à acessibilidade quando preciso. A garantia deste envolve resiliência frente aos ataques com capacidade de corromper ou negar acesso aos dados, de modo que o ambiente deve ser robusto o suficiente para lidar com interrupções do sistema, problemas de comunicação ou de energia e quaisquer problemas que possam nos impedir de acessar os dados. A disponibilidade geralmente é obtida por meio do uso de *backups* (ANDRESS; WINTERFELD, 2014, p. 195-196).

Isto posto, a autentificação, a autorização e a auditoria (AAA) são princípios que consentem a realização, de forma prática, da proteção de dados. É por meio desta tríade em que se pode tanto controlar quanto rastrear como os dados são acessados e por quem, o que, por sua vez, permite aplicar as políticas existentes com o fito de manter a segurança. A autenticação é o meio pelo qual se verifica a identidade de um indivíduo ou sistema em relação a um conjunto de credenciais apresentadas. Após isso, é possível verificar as atividades essa identidade específica pode realizar. Assim, a auditoria fornece a capacidade de monitorar quais atividades ocorreram em um determinado sistema, o que também permite equilibrar as cargas do sistema (ANDRESS; WINTERFELD, 2014, p. 196-197).

Em termos gerais, quando há um problema securitário, pode-se aplicar um *patch*, alterar uma configuração ou acumular infraestrutura de segurança adicional para corrigir o problema. Entretanto, quando o problema é social, tem-se o que é, talvez, a maior vulnerabilidade, pois

falhas humanas acontecem e não podem ser corrigidas com algum programa ou ferramenta. Apesar de as medidas técnicas para evitar certas atividades indesejáveis, ou políticas claras sobre comportamentos e procedimentos, questões humanas devem ser tratadas, principalmente, a partir de uma maior conscientização sobre as questões securitárias com treinamento adequado e organização congruente (ANDRESS; WINTERFELD, 2014, p. 198).

Para além da parte de conscientização, há também a formação holística de segurança. Há, em instituições governamentais, o treinamento constante com instruções sobre comportamento seguro e adequado para o uso de meios de comunicação, os quais são constantemente usados para enganar ou tentar obter informações por meio de engenharia social. Além disso, é importante ter algum tipo de formação complementar capaz de atender às especificidades, tais como engenheiros e desenvolvedores (ANDRESS; WINTERFELD, 2014, p. 199-200).

Em um ambiente de rede de pequeno ou médio porte, normalmente de empresas ou corporações, as medidas protetivas contra ataques cibernéticos são proativas por natureza e abarcarão o monitoramento das atividades e proteção do sistema. Todavia, em um ambiente muito maior, que opera em âmbito nacional ou global, o monitoramento em grande escala se torna extremamente difícil, o que implica em um encolhimento do conjunto de dados a serem inspecionados. Atualmente, muito do esforço que está sendo feito na CND está nas áreas de política e de conformidade, particularmente nos círculos governamentais, tendo em vista que as estratégias para monitoramento em massa estão em sua infância (ANDRESS; WINTERFELD, 2014, p. 200).

Uma das principais soluções para uma defesa eficaz está na política de segurança, onde políticas podem definir as expectativas e o comportamento dos desenvolvedores e usuários, a configuração dos *softwares*, sistemas, redes e afins. Vale ressaltar que qualquer política implementada que não detém a devida autoridade para aplicá-la é totalmente inútil e frequentemente ignorada (ANDRESS; WINTERFELD, 2014, p. 200).

Atualmente, a grande maioria das redes que integram a internet não estão segmentadas em fronteiras nacionais. Esta insuficiência juntamente à ampla variedade de métodos de comunicação faz com que o *Intrusion Detection System* (IDS) e o *Intrusion Prevention System* (IPS), ou seja, ferramentas que examinam o tráfego na rede, tanto para detectar quanto para prevenir acessos não autorizados, protegendo-a da exploração das fragilidades, sejam tecnicamente difícil de serem implementados. Entretanto, há duas estratégias fundamentais para realizar a detecção e prevenção de intrusos: estruturação das redes com o fito de fornecer uma quantidade limitada de conexões fora da área a ser monitorada e protegida, ou implementação de ISD/IPS

amplamente distribuídos (FERNANDES, 2022; ANDRESS; WINTERFELD, 2014, p. 201-202).

Avaliação de vulnerabilidade e teste de penetração são duas das principais ferramentas do CND, mas apenas uma parte do chamado *Red Team*[35], utilizada tanto por instituições governamentais quanto comerciais. Apesar de expor algumas vulnerabilidades das quais os invasores podem tirar proveito, esta avaliação não apresenta uma imagem completa de como os sistemas podem estar vulneráveis. Para isto, é necessário utilizar esforços, ferramentas e testes mais minuciosos. O *Penetration Testing* é um exemplo de teste que pode ser realizado a partir de uma perspectiva de caixa branca (menos dispendioso), na qual se recebe informações sobre o ambiente a ser atacado, ou pode ser feito a partir de uma perspectiva de caixa preta (representa um ataque externo), na qual não há informações adicionais que um invasor normalmente teria. Tendo isto em vista, é interessante que o teste permita ataques, justamente porque a ausência do mesmo pode provocar uma sensação de falsa segurança, já que não estaria servindo o seu propósito de usar os mesmos métodos que os invasores em potencial usarão (ANDRESS; WINTERFELD, 2014, p. 202-203).

O *Disaster Recovery Planning* ou Planejamento de Recuperação de Desastres (DRP), como CND, pode permitir resistir ou recuperar de ataques, interrupções e desastres efetivos. Em geral, o DRP se concentra na infraestrutura de TI *versus* operações comerciais sustentadas e remete às medidas realizadas por meio de *backups* dos dados e da utilização de graus de sistemas e infraestrutura redundantes. Entretanto, um dos princípios mais vitais de uma estratégia defensiva bem-sucedida é a defesa em profundidade. Este é um conceito militar que apresenta uma abordagem em camadas: defesas no nível da rede (*firewalls* e IDS/IPS), do host (f*irewalls* de *software* e ferramentas *antimalware*), do aplicativo (controles de acesso) e dos dados (criptografia). As medidas de segurança em cada camada podem variar de acordo com o ambiente em questão, apesar do princípio de impedir o invasor o suficiente para que os elementos de detecção descubram suas atividades e que as medidas de segurança sejam ativadas é o mesmo em cada camada (ANDRESS; WINTERFELD, 2014, p. 203-204).

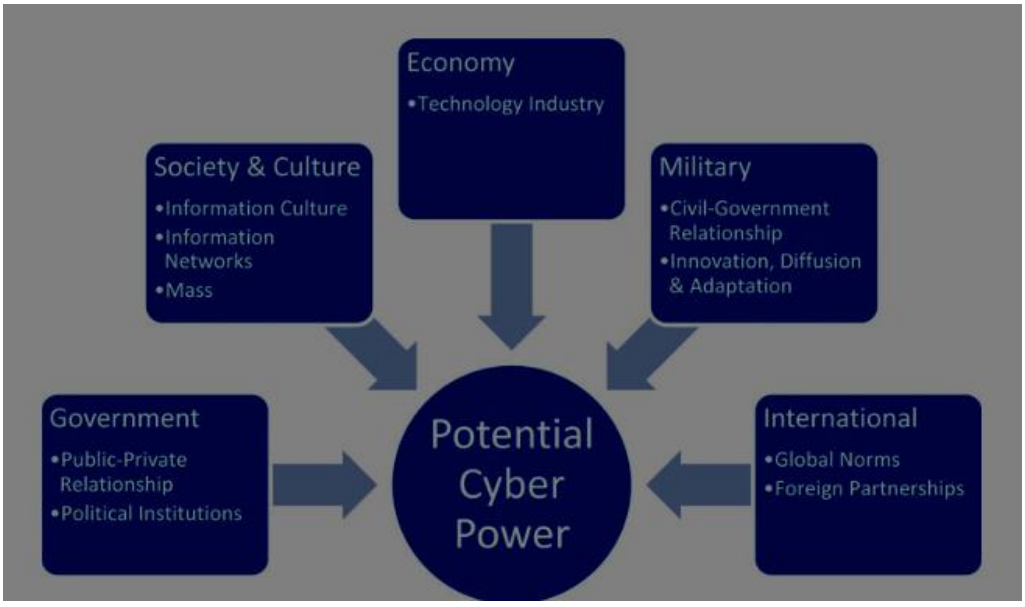
Um exemplo de operação defensiva é a Operação Orchard, quando as Forças Aéreas Israelenses (FAI) bombardearam e destruíram um complexo de edifícios, localizados no leste da Síria, os quais escondiam a construção de um reator nuclear refrigerado a grafite. O papel da

[35]Um "time vermelho" se refere aos "*hackers* éticos" que auxiliam organização no processo de identificação de vulnerabilidades, testando e lançando ataques em um ambiente controlado (XMCYBER, 2022).

capacidade cibernética neste exemplo foi fundamental em superar a defesa aérea síria ao esconder os sinais dos oito caças das FAI no espaço aéreo monitorado. Nesse sentido, isto somente foi possível graças à invasão de um computador que infiltrou e neutralizou temporariamente os radares de defesa aérea e sistemas de comunicação (TABANSKY; ISRAEL, 2015, p. 65).

O espaço cibernético passou a ocupar papéis cada vez mais centrais no que tange às funções estatais, tais como operações militares e projeção de poder, tendo em vista que a troca econômica e a distribuição de informações, na guerra moderna, demandam redes e operações com o objetivo de alcançar os efeitos desejados. Militarmente falando, os oficiais se encontraram reféns das redes do ciberespaço para comandar, controlar, organizar e lutar, isto é, o emprego efetivo deste poder implica vitória ou derrota (BEBBER, 2017, p. 426). Não obstante, um dos problemas encontrados na literatura que trata sobre a definição deste poder é o fato de definirem *post hoc* em vez de *ex antes*. Por conta disto, utilizar-se-á a definição utilizada por Bebber (2017) de que o poder cibernético potencial advém dos "recursos humanos e materiais disponíveis dentro de um ambiente estratégico que podem ser utilizados para gerar efeitos no e através do ciberespaço" (BEBBER, 2017, p. 427). A figura 19 resume as variáveis estruturais e sistêmicas que constituem o ambiente estratégico. Nesse sentido, a eficácia cibernética remete à "capacidade de traduzir o poder cibernético em apoio a fins políticos nacionais no e por meio do ciberespaço" (BEBBER, 2017, p. 427).

Figura 19 - Poder cibernético potencial e os fatores domésticos e internacionais



Fonte: BEBBER, 2017, p. 427

Em relação ao fator governamental, tanto a organização política quanto as instituições espelham a cultura e a história de um país e desempenham um papel direto no uso da informação, do poder cibernético e na organização das forças cibernéticas. Ao compreender os meios pelos quais o poder cibernético é organizado politicamente, sua distribuição e o processo que determina quando e como o poder cibernético será utilizado, é possível enxergar a capacidade de resposta e agilidade de um Estado (BEBBER, 2017, p. 428).

Estados, em geral, tendem a se organizar de acordo com fatos históricos e culturais com o fito de reproduzir uma visão de mundo. A abordagem cultural de um Estado em relação à informação e seus valores ajuda a compreender quais atividades cibernéticas o mesmo envolve. Aqui, ideologia e objetivos nacionais também terão um papel vital para entender que tipo de atividades cibernéticas são apropriadas e, caso haja conflito, qual função o ciberespaço pode desempenhar. Desse modo, essas informações sobre o país também são importantes na arquitetura de informação a ser desenvolvida (BEBBER, 2017, p. 427-428).

Os tipos de redes, sejam elas físicas e virtuais ou nacionais e importadas, incluem fibra e cabo, sem fio, transmissão e mídia, bem como as redes sociais que permitem a interação humana e econômica, além da infraestrutura crítica, tais como transporte, serviços públicos, redes financeiras e redes de informações de saúde. Para entender como um Estado acumula poder cibernético e o traduz em eficácia, é necessário entender a arquitetura dessas redes, i.e. como foram estabelecidas e o grau de resiliência, proteção e dependência do Estado em tecnologias nacionais e importadas. Destarte, é a partir destas redes de informações, as quais incluem redes militares e de inteligência sensíveis à infraestrutura pública crítica, que Estados serão capazes de projetar poder e alcançar seus objetivos estratégicos (BEBBER, 2017, p. 428).

Não menos importante, o tamanho da população e a escala geográfica do país ainda são importantes, mesmo no espaço cibernético, pois a capacidade de lançar grandes quantidades de operadores pode afetar a capacidade de controle de informação e, por conseguinte, a eficácia cibernética. No que tange a isso, a inovação tecnológica (sistemas autônomos e inteligência artificial) pode compensar, em certo grau, uma população pequena. Apesar disso, o tamanho de uma população e do país podem ser cruciais em questões operacionais e técnicas e como o Estado calcula o risco e como o cálculo do risco orienta seu comportamento (BEBBER, 2017, p. 430).

Evidentemente, a indústria de tecnologia é primordial para colocar as forças cibernéticas em prática e, portanto, permitir seu poder. As capacidades da indústria de tecnologia são uma

função de fatores: acesso a recursos, habilidade e qualidade da força de trabalho, acesso a capital e investimento e regulamentação governamental da atividade econômica, bem como proteção da propriedade privada e dos direitos de propriedade intelectual. Apesar desses fatores serem uma indicação, não é mais possível determinar com claridade quais ferramentas estão disponíveis para os países influenciarem o crescimento e a mudança em suas indústrias de tecnologia nacionais justamente por conta da globalização (BEBBER, 2017, p. 428).

Outrossim, leis, cultura, valores e política auxiliam na explicação da relação entre o setor privado e a governança civil em um país. Nesse sentido, as ferramentas escolhidas pelo Estado para influenciar o setor privado na área de tecnologia da informação são importantes para as relações civis-governamentais. Tais ferramentas podem incluir, por exemplo, mecanismos para orientar o desenvolvimento tecnológico, como agências de pesquisa e desenvolvimento financiadas pelo Estado, a utilização dos sistemas públicos de ensino e formação para desenvolver competências técnicas e informáticas da população, bem como autoridades que os Estados capacitam suas CERTs para agir (BEBBER, 2017, p. 429).

Além disso, a difusão, a inovação e a adaptação também fazem parte do fator militar na formação da potência cibernética. Primeiramente, a inovação pode se dar por mudanças drásticas na estrutura organizacional, alocação de recursos, estratégia e doutrina, englobando o procedimento de adaptação das instituições e práticas de fazer a guerra às mudanças tecnológicas e/ou desenvolvimentos sociais e políticos. A difusão, por sua vez, remete à interação internacional ou na própria estratégia de mudança militar concomitante à inovação na dinâmica doméstica e organizacional da mudança militar. Isto posto, política, economia, sociedade, cultura e âmbito militar são fatores que permitem a difusão e a inovação da RMA (BEBBER, 2017, p. 430).

No que concerne ao internacional, normas globais, costumes, leis internacionais e tratados tentam regular e padronizar redes, sistemas e conteúdo de informação e podem impactar sua eficácia, tanto por meio de restrições ou agindo como um facilitador, com o objetivo de que os Estados alterem os conjuntos de regras. É neste sentido que parcerias e alianças internacionais podem alterar a capacidade dos Estados no que tange à projeção de poder cibernético, isto é, Estados pequenos podem gozar de benefícios ao participarem de alianças (BEBBER, 2017, p. 429).

Uma das maiores complexidades em examinar a eficácia cibernética é o fato de que o poder cibernético não se encontra somente no âmbito militar ou governamental, mas também com indivíduos e setor privado. Entretanto, Bebber (2017) utiliza a cadeia causal da eficácia

militar de Brooks (2007), a qual inclui exibe certos atributos, tais como integração, capacidade de resposta, habilidade e qualidade. Bebber (2017), aqui, adiciona um: a reputação.

A integração se refere ao grau em que as atividades cibernéticas estão verticalmente consistentes com as políticas, estratégias e táticas, as quais se reforçam mutuamente. A capacidade de resposta concerne à capacidade de adaptar as atividades cibernéticas de um estado às suas próprias capacidades, às capacidades de seus adversários e às restrições externas (BEBBER, 2017, p. 430). A habilidade, por sua vez, é a capacidade das forças cibernéticas, incluindo o ramo militar, político, de inteligência e civil, em áreas críticas, incluindo a capacidade de assimilar novas tecnologias, adotar novas estratégias e táticas, explorar pontos fracos e incorporar treinamento e desenvolvimento. Qualidade é a capacidade de fornecer, às forças cibernéticas, equipamentos altamente eficientes. Por fim, a reputação remete à percepção das capacidades cibernéticas estatais compartilhadas por adversários e atores. Ademais, os Estados também avaliam a anseio do outro em usar o poder cibernético para alcançar seus objetivos nacionais e sob quais circunstâncias o poder seria empregado (BEBBER, 2017, p. 430-431).

Por fim, a eficácia cibernética emerge a partir da capacidade de produzir uma força cibernética qualificada, integrada, responsiva e respeitável. Em outros termos, a eficácia depende de como as forças e os meios pelos quais os países organizam sua conduta em relação ao desenvolvimento técnico, tático, operacionais e estratégico são empregados. Destarte, um Estado pode ter suas forças cibernéticas separadas por funções de acordo com a lei e a política, enquanto outros podem centralizá-las em uma instituição, a qual desempenha funções de segurança interna e externa. É a partir disso que surgem as especificidades da doutrina, estrutura de força, atividades, capacidades, táticas, adaptabilidade, agilidade, sofisticação de técnicas e tolerância ao risco (BEBBER, 2017, p. 431).

Em síntese, é possível concordar a respeito das principais características do poder cibernético. Em primeiro lugar, é necessário que haja estratégias, doutrinas e conceitos operacionais coerentes e integrados para que este poder seja eficaz. Em segundo lugar, a sofisticação do treinamento é crucial para proporcionar a condução de atividades cibernéticas avançadas. Além disso, o tipo de pessoas recrutadas para as forças cibernéticas é fundamental para a sua eficácia, tendo em vista que a falha humana é a mais difícil de ser evitada. Em quarto lugar, leis e regras formais demonstram como um país enxerga as operações do ciberespaço e se elas são centrais para o mesmo alcançar seus objetivos estratégicos nacionais. Em quinto, o atributo de qualidade da eficácia cibernética depende das atividades associadas à aquisição de tecnologia da informa-

ção, tanto de *hardware* quanto de *software.* Ademais, a capacidade de identificar, fornecer recursos, desenvolver, testar e avaliar capacidades para obter vantagens no ciberespaço são essenciais para que um Estado possa exercer o poder cibernético. Por fim, infraestruturas alternativas ao espaço público da internet são necessárias para que o poder cibernético seja entregue (BEBBER, 2017, p. 431-434).

Enfim, Israel se destaca na formulação de capacidades cibernéticas, pois é o único Estado capaz de difundir suas capacidades cibernéticas por meio de sua estrutura de força. Aliás, a ausência de uma doutrina militar dogmática e os traços culturais da sociedade israelense permitem a flexibilidade necessária para lidar com o poder cibernético. Um dos maiores impedimentos para que haja progresso na reforma da política cibernética de modo eficaz é o capital humano qualitativo, o qual, Israel, em seu ecossistema, detém.

Sendo assim, observa-se que tanto a organização política quanto as instituições israelenses espelham a cultura e a história do país e desempenham um papel direto no uso da informação, do poder cibernético e na organização das forças cibernéticas. Em Israel, o tamanho da população e a escala geográfica importam desde a sua criação e, atualmente, a tecnologia em conjunto com o capital humano são capazes de suprir a vantagem qualitativa necessária para garantir a sobrevivência do Estado.

Apesar da falta de transparência no que tange à sua capacidade cibernética israelense, o país é percebido pelo resto do mundo como um dos que detém uma das capacidades cibernéticas militares mais desenvolvidas e pronta para ser utilizada com o fito de alcançar seus objetivos estratégicos nacionais. Não obstante, a sua confiança em tecnologia e, por conseguinte, no poder cibernético, deixa Israel vulnerável a ataques, mas sua capacidade defensiva faz com que o país seja considerado como um dos mais seguros, ciberneticamente falando. Conclui-se, portanto, que Israel detém capacidades cibernéticas defensivas e ofensivas.

7 CONCLUSÃO

Apesar das pesadas restrições de segurança quanto ao acesso às informações, foi possível concluir, por meio desta dissertação, que o poder cibernético, em Israel, está ancorado em um amplo ecossistema de capacidades industriais, científicas e de pessoal especializado, bem como na existência de unidades especializadas, civis e militares, e de uma doutrina específica de uso do poder cibernético para a sustentação do poder estatal.

Se, por um lado, a tecnologia da informação possibilitou a criação e o desenvolvimento do espaço cibernéticos e dos seus riscos, por outros, os traços culturais nacionais e a grande estratégia são elementos não técnicos cruciais para o entendimento da política e do poder cibernético na segurança cibernética nacional. Particularmente, a análise da segurança cibernética israelense requer uma perspectiva estratégica. Isto é, esta segurança não é somente uma questão de conquista e execução de sua capacidade técnica cibernética. Ela é, sobretudo, uma questão política, a qual envolve fatores culturais, políticos e organizacionais que desempenham um papel chave no caso israelense (TABANSKY; ISRAEL, 2015, p. 71).

Nesse sentido, o poder cibernético se adequa de maneira quase perfeita à grande estratégia israelense por alguns motivos: primeiramente, fornece uma vantagem qualitativa sem exigir grandes recursos naturais ou mão de obra; em segundo lugar, fornece uma vantagem temporal e informacional (alerta precoce); oferece menor grau de mortalidade e destruição em relação às alternativas cinéticas

De fato, as FDI foram vitais para o desenvolvimento da capacidade nacional de segurança cibernética, pois conduziu a maior parte do amadurecimento de seu capital humano e do desenvolvimento de P&D, principalmente em relação à tecnologia da informação. Aliás, elas consideram o espaço cibernético como um âmbito propício para alcançar a vantagem operacional decisiva. Este grau de confiança atesta sua maturidade tecnológica, doutrinária e organizacional no que se refere à segurança cibernética. Portanto, a capacidade cibernética israelense é a consequência direta do progresso científico e tecnológico concomitantemente ao desenvolvimento de seu capital humano, encontrado no ecossistema existente. Isto é, o conjunto ímpar de fatores históricos, culturais, geopolíticos, econômicos, organizacionais e políticos orientam a postura de segurança cibernética de Israel, suas capacidades e políticas (TABANSKY; ISRAEL, 2015, p. 71-72).

Os capítulos dois, três e quatro, sobre a governança, comando e controle, estratégia e doutrina militar israelenses, respectivamente, proporcionaram a visão analítica primordial em relação à grande estratégia e ao ecossistema de inovação israelenses. Esta foi desenvolvida para cumprir o *Tfisat HaBitachon* em um ambiente hostil e para buscar a vantagem qualitativa. O ecossistema, por sua vez, é uma consequência direta da grande estratégia, sendo este o principal impulsionador tanto da segurança quanto da economia nacional do país. Este fato é comprovado pelos dados de P&D, da qualidade das instituições acadêmicas e da educação de sua população, das parcerias realizadas pela tríade governo-indústria-academia e pelas FDI fornecidas no capítulo quatro. Todos estes fatores moldam o capital humano israelense por meio dos traços culturais, da experiência militar, acadêmica e empresarial. Além disso, também foi tratado sobre o processo de formulação das políticas direcionadas a criar e melhorar a segurança cibernética, sendo estas vitais para a constituição das capacidades cibernéticas.

Por fim, em relação às características principais do poder cibernético, Israel detém um alto grau de sofisticação em relação aos seus treinamentos, de modo que é capaz de proporcionar a condução de atividades cibernéticas avançadas. Além disso, todo o investimento direcionado ao seu capital humano faz com que o tipo de pessoas recrutadas para as forças cibernéticas seja do mais alto grau de qualidade disponível, o que evita, portanto, a frequência da falha humana. Estas operações somente são possíveis graças ao alto grau de desenvolvimento tecnológico informacional, incluindo *hardware* e *software.*

As leis e regras formais israelenses demonstram a centralidade do poder cibernético para o país alcançar seus objetivos estratégicos nacionais. Israel se destaca na formulação das capacidades ofensivas e defensivas, pois elas se fundem no conjunto de capacidades militares e de provimento de segurança do Estado. Além da análise que foi realizada nesta dissertação, uma agenda possível de pesquisa futura seria a realização de estudos quantitativos e qualitativos sobre o conteúdo dos documentos, visando o entendimento mais contextualizado sobre os discursos do país a respeito de suas operações no ciberespaço. Ademais, é possível, para futuros pesquisadores, aprofundarem-se nos temas das capacidades cibernéticas, capacidade espacial ou até mesmo nuclear de Israel, bem como o peso das relações com os EUA

REFERÊNCIAS

8200BIO. **Why are we here?** 2022. Disponível em: https://bio.8200.org.il/#introduction. Acesso em: 01 set. 2022.

ADAMSKY Dmitry, The Israeli Odyssey towards its National Cyber Security Strategy, **The Washington Quarterly.** Londres, v. 40, n. 2, pp. 113-127, 2017.

ADAMSKY, Dima. **The Culture of Military Innovation:** The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, The US, and Israel. Stanford, California: Stanford University Press. 2010.

ALWAREBYTES. **DdoS.** 2022. Disponível em: https://www.malwarebytes.com/ddos. Acesso em: 19 ago 2022.

ANDRESS, Jason. WINTERFELD, Steve. **Cyber Warfare:** Techniques, Tactics and Tools for Security Practitioners. 2. ed. Estados Unidos: ELSEVIER. 2014.

ATIDIM. **The Power of Atidim.** 2022. Disponível em: https://atidim.org/en/about/. Acesso em: 20 dez. 2022.

BARAM, Gil; ISRAEL, Isaac. The Academic Reserve: Israel's Fast Track to High-Tech Success. **Israel Studies Review,** v. 34, n. 2, pp. 1-22, 2018.

BASEL. **Basel AML Index: 9th Public Edition:** Ranking money laundering and terrorist financing risks around the world. 2020.

BELFER CENTER. **National Cyber Power Index 2022.** 2022.

BOURDIEU, P. The forms of capital. *In:* RICHARDSON, J., **Handbook of Theory and Research for the Sociology of Education**. Westport, CT: Greenwood. 1986, pp. 241–58.

BROOKS, Risa. The Impact of Culture, Society, Institutions, and International Forces of Military Effectiveness. *In:* BROOKS, Risa; STANLEY, Elizabeth (eds.). **Creating Military Power: The Sources of Military Effectiveness.** Stanford: Stanford University Press. 2007, pp. 1-26.

CENTRAL BUREAU OF STATISTICS. CBS. **Development of the High-Tech Sector in Israel in the Years 1995-2007.** 2010. Disponível em: https://www.cbs.gov.il/en/publications/pages/2010/development-of-the-high-tech-sector-in-israel-in-the-years-1995-2007.aspx. Acesso em: 12 set. 2022.

CENTRAL BUREAU OF STATISTICS - CBS. **Israel in Figures:** Selected Data from the Statistical Abstract of Israel. 2021. Disponível em: https://www.cbs.gov.il/he/publications/DocLib/isr_in_n/sr_in_n21e.pdf. Acesso em: 30 ago. 2022.

NATO Cooperative Cyber Defence Centre of Excellence. CCDCOE. COURIEL-HOUSEN. Deborah. **National Cyber Security Organisation:** Israel. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn, 2017.

CEPIK, M. **Espionagem e democracia:** agilidade e transparência como dilemas na institucionalização de serviços de inteligência. Rio de Janeiro: Ed. FGV, 2003.

CONFEDERAÇÃO ISRAELITA DO BRASIL - CONIB. Confederação Israelita do Brasil. **Haganá**. 2022. Disponível em: https://www.conib.org.br/glossario/hagana/. Acesso em: 05 ago 2022.

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES - CSIS. **Hacking the Skills Shortage:** A study of the international shortage in cybersecurity skills. Report. 2016.

CENTER FOR SECURITY STUDIES - CSS, ETH Zürich. BAEZNER, Marie; CORDEY, Sean. **National Cybersecurity Strategies in Comparison:** Challenges for Switzerland. Center for Security Studies Cyber Defence. Zurique, 2019.

CENTER FOR SECURITY STUDIES - CSS. **Israel's National Cybersecurity and Cyberdefense:** Posture Policy and Organizations. 2020.

DALL'AGNOL, Augusto; DUARTE, Érico. Poder militar y disuasión convencional: revisión de la literatura. **Revista de Relaciones Internacionales, Estrategia y Seguridad**, v. 17, n. 1, pp. 101–118, 2022. Disponível em: https://revistas.unimilitar.edu.co/index.php/ries/article/view/5793.

DIMA, Adamsky. The Israeli Odyssey toward its National Cyber Security Strategy. **The Washington Quarterly**, v. 40, n. 2, pp. 113-127, 2017.

DOMBE, Ami Rojkes. Lahav-433 in the Cybercrime Era. **Israel Defense.** 2020. Disponível em: https://www.israeldefense.co.il/en/node/41752. Acesso em: 09 ago 2022.

EILAM, Ehud. The rise and decline of the Israeli offensive. **Comparative Strategy,** v. 40, n. 3, pp. 245-253, 2021.

FERNANDES, Mirian. IDS e IPS: detecção e bloqueio de ameaças! **STARTI.** Julho de 2022. Disponível em: https://blog.starti.com.br/ids-ips/. Acesso em: 10 dez 2022.

FINKEL, Meir. IDF Strategy Documents, 2002-2018: On Processes, Chiefs of Staff, and the IDF. **Strategic Assessment,** v. 23, n. 4, out. 2020.

FORTINET. **Global Threat Landscape Report:** A Semiannual Report by FortiGuard Labs. 2022.

FREILICH, Charles, Israel's National Security Policy. *In:* REUVEN, Hazan; ALAN, Dowty; MENACHEN, Hofnung; GIDEON, Rahat. **The Oxford Handbook of Israeli Politics and Society.** Oxford: 2018a, pp. 1-20.

FREILICH, Charles. **Israeli National Security:** A New Strategy for an Era of Change. New York: Oxford University Press. 2018b.

FREILICH, Charles. National Security Decision-Making in Israel: Improving the Process. **Middle East Journal**, v. 67, n. 2, pp. 257-266, 2013.

GVAHIM. **Gvahim Tech Program.** 2022. Disponível em: https://gvahim.org.il/gvahim-tech/. Acesso em: 06 set. 2022.

HOUSEN-COURIEL; MIMRAN; SHANY. Israel's Version of Moving Fast and Breaking Things: The New Cybersecurity Bill. **Lawfare.** 7 maio 2021. Disponível em: https://www.lawfareblog.com/israels-version-moving-fast-and-breaking-things-new-cybersecurity-bill. Acesso em: 27 jul 2022.

HUB.RO. **Hubs de inovação: o que são e como apoiam a atuação de empreendedores.** Disponível em: https://hub-ro.com.br/blog/hubs-de-inovacao-o-que-sao. Acesso em: 05 set. 2022.

THE INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES - IISS. **Cyber Capabilities and National Power:** A Net Assessment. 2021.

ISRAEL INNOVATION AUTHORITY. **Programs.** 2022. Disponível em: https://innovationisrael.org.il/en/program/human-capital-high-tech-fund. Acesso em: 06 set. 2022.

ISRAEL. IDF. **Military Intelligence Directorate**. 2021c. Disponível em: https://www.idf.il/en/minisites/directorates/military-intelligence-directorate/military-intelligence-directorate/. Acesso em: 03 ago 2022.

ISRAEL. IDF. **Operation Cast Lead.** 2017a. Disponível em: https://www.idf.il/en/minisites/wars-and-operations/operation-cast-lead/. Acesso em: 19 ago 2022.

ISRAEL. INCD. **About Israel National Cyber Directorate**. 2020d. Disponível em: https://www.gov.il/en/departments/about/newabout. Acesso em: 09 ago 2022.

ISRAEL. **Israel National Cyber Directorate.** 2020. Disponível em: https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page. Acesso em: 21 jun. 2022.

ISRAEL. Ministry of Finance. **Financial Statements of the Government of Israel as at December 31, 2006**. 2006. Disponível em: https://www.gov.il/BlobFolder/dynamiccollectorresultitem/financial-reports-2006/he/financial-reports_FinancialReport2006.pdf. Acesso em: 19 ago 2022.

ISRAEL. Ministry of Foreign Affairs. **Science and Technology:** R&D at Universities. 2021d. Disponível em: https://www.gov.il/en/Departments/General/science-and-technology-r-and-d-at-universities. Acesso em: 07 set. 2022.

ISRAEL. Ministry of Justice. **About Ministry of Justice.** 2021a. Disponível em: https://www.gov.il/en/departments/about/about_ministry_of_justice. Acesso em: 06 ago 2022.

ISRAEL. Ministry of Justice. The Office of the State Attorney. **About the Cyber Unit.** 2021b. Disponível em: https://www.gov.il/en/departments/general/cyber-about. Acesso em: 06 ago 2022.

ISRAEL. MOSSAD. **About Us.** 2022a. Disponível em: https://www.mossad.gov.il/eng/about/Pages/default.aspx. Acesso em: 03 ago 2022.

ISRAEL. National Insurance of Israel. **Freedom of Information Law.** 2022b. Disponível em: https://www.btl.gov.il/English%20Homepage/About/FreedomInformation/Pages/default.aspx#:~:text=The%20Freedom%20of%20Information%20Law,Freedom%20of%20Information%20Law%20Supervisor. Acesso em: 19 ago 2022.

ISRAEL. Prime Minister's Office. **Israel National Cyber Bureau and Ministry of Defense Directorate for Research & Development Announce Plan to Advance Dual Civilian-Defense R&D Projects**. 31 out. 2013. Disponível em: https://www.gov.il/en/departments/news/spokemasad311012. Acesso em: 06 set. 2022.

ISRAEL. Prime Minister's Office. **Israel National Cyber Security Strategy in Brief.** 2017b.

ISRAEL. Prime Minister's Office. **PM Netanyahu Attends Conference of Global information Technology Leaders.** 23 jan. 2014. Disponível em: https://www.gov.il/en/departments/news/eventdavosi230114. Acesso em: 06 set. 2022.

ISRAEL. Shabak. **About.** 2020c. Disponível em: https://www.shabak.gov.il/english/about/Pages/about.aspx. Acesso em: 04 ago 2022.

ISRAEL. Shabak. **Information technology**. 2020a. Disponível em: https://www.shabak.gov.il/english/cybertechnology/Pages/technology.aspx. Acesso em: 04 ago 2022.

ISRAEL. Shabak. **Technology and Cyber Division.** 2020b. Disponível em: https://www.shabak.gov.il/english/cybertechnology/Pages/cyber.aspx. Acesso em: 04 ago 2022.

ISRAEL. The Office of the State Attorney. **About The Office of the State Attorney.** 2019. Disponível em: https://www.gov.il/en/departments/about/state_attorney_about. Acesso em: 06 ago 2022.

International Trade Administration. ITA. **Israel - Country Commercial Guide:** Information Communication Technology ICT**.** 2022. Disponível em: https://www.trade.gov/country-commercial-guides/israel-information-communication-technology-ict. Acesso em: 05 set. 2022.

KAPERSKY. **What is a Zero-day Attack? - Definition and Explanation.** 2022. Disponível em: https://usa.kaspersky.com/resource-center/definitions/zero-day-exploit. Acesso em: 23 dez. 2022.

KASPERSKY. **Cyberthreat Real-Time Map.** 2021. Disponível em: https://cybermap.kaspersky.com/. Acesso em: 04 dezembro 2022.

LEICHMAN, Abigail. The surprising source of tomorrow's cyber experts: Social-action program identifies gifted students from periphery towns and trains them to fill an increasing demand for cyber-tech professionals. **Israel21c.** 06 mai. 2015. Disponível em: https://www.israel21c.org/the-surprising-source-of-tomorrows-cyber-experts/. Acesso em: 06 set. 2022.

MEROM, Gil. The Architecture and Soft Spots of Israeli Grand Strategy. *In:* LEE, Bradford; WALLING, Karl. **Strategic Logic and Political Rationality:** Essays in Honor of Michael I.Handel. Londres: Frank Cass, 2003, pp. 207-240.

NATIONAL CYBER SECURITY INDEX - NCSI. **Israel.** 2022. Disponível em: https://ncsi.ega.ee/country/il/. Acesso em: 04 dezembro 2022.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO - OCDE. **Gross domestic spending on R&D.** 2022. Disponível em: https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm. Acesso em: 30 ago. 2022.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO - OEC. **Israel**. 2022. Disponível em: https://oec.world/en/profile/country/isr?depthSelector1=HS2Depth&depthSelector3=SectionDepth. Acesso em: 06 set. 2022.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO - OECD. **OECD Digital Economy Outlook 2020**, Paris: OECD Publishing. 2020.

Organização para a Cooperação e Desenvolvimento Econômico - OECD. **Productivity, human capital and educational policies.** 2022. Disponível em: https://www.oecd.org/economy/human-capital/. Acesso em: 20 dez. 2022.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS - ONU. **UN Fact Finding Mission finds strong evidence of war crimes and crimes against humanity committed during the Gaza conflict; calls for end to impunity.** 2009. Disponível em: https://www.ohchr.org/en/press-releases/2009/10/un-fact-finding-mission-finds-strong-evidence-war-crimes-and-crimes-against?LangID=E&NewsID=91. Acesso em: 19 ago 2022.

PINCHAS, Gil; TISHLER, Asher. The Israeli defense industry. *In:* HARLEY, Keith; BELIN, Jean. **The Economics of the Global Defence Industry.** 1. ed. Londres: Routledge, 2019, pp. 364-377.

PRESS, Viva. CyberSpark moves forward: BGN, EMC and JVP announce creation of a new company: CyberSpark Industry Initiative. **Israel21c.** 16 set. 2014. Disponível em: https://www.israel21c.org/cyberspark-moves-forward/. Acesso em: 06 set. 2022.

RASHI FOUNDATION. **Magshimim.** 2022a. Disponível em: https://rashi.org.il/en/programs/magshimim/. Acesso em: 06 set. 2022.

RASHI FOUNDATION. **Mamriot.** 2022c. Disponível em: https://rashi.org.il/en/programs/mamriot/. Acesso em: 06 set. 2022.

RASHI FOUNDATION. **Science Leadership.** 2022d. Disponível em: https://rashi.org.il/en/programs/science-leadership/. Acesso em: 06 set. 2022.

RASHI FOUNDATION. **StarTech**. 2022b. Disponível em: https://rashi.org.il/en/programs/startech/. Acesso em: 06 set. 2022.

SAGAN, Scott. The Origins of Military Doctrines and Command and Control Systems. *In:* LAVOY, Peter; SAGAN; Scott; WIRTZ, James. **Planning the Unthinkable: How New Powers Will Use Nuclear, Biological and Chemical Weapons.** New York: Cornell University Press, 2000, pp. 16-46.

SCALE-UP TEAM. **Excellenteam.** 2022. Disponível em: https://suvelocity.org/?page_id=4034. Acesso em: 05 set. 2022.

SENOR, Dan; SINGER, Saul. **Start-up National: The Story of Israel's Economic Miracle**. New York: Hachette Book Group. 2009.

SOLOMON, Shoshanna. Check Point reports 93% surge in smart ransomware attacks over past year: In the first half of 2021, Israel saw on average 2.5 times more cybersecurity attacks than globally, Israeli cybersecurity giant says. **Times of Israel.** 26 jul 2021. Disponível em: https://www.timesofisrael.com/check-point-reports-93-surge-in-smart-ransomware-attacks-over-past-year/. Acesso em: 05 dez 2022.

START-UP NATION. Policy Institute. **Israeli High-Tech Human Capital:** A Snapshot 2021-2022. 2022. Disponível em: https://innovationisrael.org.il/en/sites/default/files/Israeli%20High-Tech%20Human%20Capital%20Report_2022_English.pdf. Acesso em: 05 set. 2022.

STATISTA. **Number of active cyber security companies in Israel from 2011 to 2020.** 2022. Disponível em: https://www.statista.com/statistics/1003442/israel-cyber-security-companies/. Acesso em: 06 set. 2022.

SWED, Ori; BUTLER, John Sibley. Military Capital in the Israeli Hi-tech Industry. **Armed Forces & Society,** v. 41, n. 1, pp. 123-141, 2015.

SYMANTEC. **Attacks Against Critical Infrastructure:** A Global Concern. 2021b.

SYMANTEC. **The Threat Landscape in 2021**. 2021a.

TABANSKY, Lior; ISRAEL, Isaac Ben. **Cybersecurity in Israel.** Springer, 2015.

TABANSKY, Lior. Israel Defense Forces and National Cyber Defense. **Connections QJ,** v. 19, n. 1, 2020.

TAL, Israel. **National Security:** The Israeli Experience. Londres: Praeger, 2000.

UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH - UNIDIR. **International Cyber Operations:** National Doctrines and Capabilities. 2021. Disponível em: https://www.unidir.org/cyberdoctrines. Acesso em: 08 nov. 2022.

UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH - UNIDIR. United Nations Institude for Disarmament Research. **Cyber Policy Portal:** Israel. 2022. Disponível em: https://cyberpolicyportal.org/states/israel. Acesso em: 20 ago 2022.

ESTADOS UNIDOS DA AMÉRICA - U.S. DEPARTMENT OF JUSTICE. **What is CIP and Why is it Important?**. Disponível em: https://www.ojp.gov/ncjrs/virtual-library/abstracts/what-cip-and-why-it-important#:~:text=CIP%20pertains%20to%20the%20proactive,economic%20stability%2C%20and%20public%20safety. Acesso em: 09 ago 2022.

VIRUSTOTAL. **Ransomware in a Global Context.** 2021.

WORLD ECONOMIC FORUM. **The Global Competitiveness Report 2015.** 2015. Disponível em: https://www.weforum.org/reports/global-competitiveness-report-2015/?DAG=3&gclid=CjwKCAjwvNaYBhA3EiwACgndgumx5tzF4NXFT2zdx-PImG3HNgGu4ceKt5KgNvX7WMeF4AIgp8KRNpBoCyhMQAvD_BwE. Acesso em: 05 set. 2022.

WORLD ECONOMIC FORUM. **The Global Competitiveness Report 2019.** 2019. Disponível em: https://www.weforum.org/reports/how-to-end-a-decade-of-lost-productivity-growth?DAG=3&gclid=CjwKCAjwvNaYBhA3EiwACgnd-gum469BYj_MN3ThdY8fQ1_ZbY6q_FV27l-fhp7mgJAD8aZNuA6aT-FRoCWvcQAvD_BwE. Acesso em: 05 set. 2022.

XMCYBER. **What is a Red Team?** 2022. Disponível em: https://www.xmcyber.com/glossary/what-is-a-red-team/. Acesso em: 27 dez. 2022.

YESHIVA WORLD NEWS - YWN. IDF High-Tech Defenders Complete Training. **The Yeshiva World.** 14 jun. 2013. Disponível em: https://www.theyeshivaworld.com/news/headlines-breaking-stories/174050/idf-high-tech-defenders-complete-training.html. Acesso em: 06 set. 2022.