ESCOLA DE GUERRA NAVAL

CC (FN) FERNANDO JOSÉ SIMÃO BAPTISTA

ISRAEL E HAMAS:
As implicações da batalha invisível.

Rio de Janeiro

2024

CC (FN) FERNANDO JOSÉ SIMÃO BAPTISTA

ISRAEL E HAMAS:
As implicações da batalha invisível.

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

Orientador: CF (FN) Rafael Alves Rodrigues Ferreira

Rio de Janeiro

Escola de Guerra Naval

2024

DECLARAÇÃO DA NÃO EXISTÊNCIA DE APROPRIAÇÃO INTELECTUAL IRREGULAR

Declaro que este trabalho acadêmico: a) corresponde ao resultado de investigação por mim desenvolvida, enquanto discente da Escola de Guerra Naval (EGN); b) é um trabalho original, ou seja, que não foi por mim anteriormente utilizado para fins acadêmicos ou quaisquer outros; c) é inédito, isto é, não foi ainda objeto de publicação; e d) é de minha integral e exclusiva autoria.

Declaro também que tenho ciência de que a utilização de ideias ou palavras de autoria de outrem, sem a devida identificação da fonte, e o uso de recursos de inteligência artificial no processo de escrita constituem grave falta ética, moral, legal e disciplinar. Ademais, assumo o compromisso de que este trabalho possa, a qualquer tempo, ser analisado para verificação de sua originalidade e ineditismo, por meio de ferramentas de detecção de similaridades ou por profissionais qualificados.

Documento assinado digitalmente
gov.br
FERNANDO JOSE SIMAO BAPTISTA
Data: 12/11/2024 19:48:23-0300
Verifique em https://validar.iti.gov.br

AGRADECIMENTOS

Gostaria de expressar minha sincera gratidão ao CF (FN) Rafael Alves Rodrigues Ferreira, que não apenas serviu como meu orientador, mas também forneceu apoio e inspiração inestimáveis ao longo deste percurso acadêmico. Sua dedicação e abordagem pragmática foram fundamentais para o desenvolvimento e a conclusão deste trabalho. Agradeço imensamente por sua paciência, estímulo e pela crença nas minhas capacidades, que foram essenciais para superar os desafios encontrados.

Além disso, estendo meus agradecimentos à turma Dodsworth, cuja camaradagem, suporte mútuo e colaboração enriqueceram significativamente minha experiência de aprendizado. A união e o espírito de equipe demonstrados por todos foram verdadeiramente inspiradores e contribuíram de maneira significativa para o meu desenvolvimento pessoal e acadêmico.

Este trabalho não seria o mesmo sem a orientação esclarecida do CF(FN) Rafael Ferreira, o suporte e o ambiente estimulante proporcionado pela turma Dodsworth. Estou profundamente grato por ter tido a oportunidade de aprender e crescer ao lado de pessoas tão excepcionais.

RESUMO

Este estudo investigou o amplo espectro do combate entre Israel e o grupo Hamas, com foco nas operações cibernéticas realizadas por ambos os lados. A análise abordou a evolução da estratégia de Israel, que se consolidou como líder global em cibersegurança, integrando operações no campo virtual e militar, através de unidades especializadas como a Unidade 8200 e hubs tecnológicos como o CyberSpark. Por outro lado, explorou-se a estrutura organizacional e as capacidades cibernéticas do Hamas, que incluem espionagem, campanhas de mídia social e ataques de negação de serviço (DDoS). Foram examinados eventos recentes do conflito, incluindo ataques relevantes no espectro virtual de autoria de grupos como Killnet e Anonymous Sudan, demonstrando a complexidade e sofisticação das ameaças modernas. O trabalho destacou a importância de uma infraestrutura cibernética robusta, a colaboração público-privada e o apoio da inteligência artificial para fortalecer a defesa de Israel. Além disso, foram fornecidas recomendações para melhorar a defesa cibernética, considerando o desenvolvimento tecnológico, a proteção de infraestruturas críticas, a cooperação interagências e a adaptação a desafios geopolíticos. Concluiu-se que a análise do conflito entre Israel e Hamas fornece importantes lições para a construção de uma defesa cibernética eficaz, aplicável a outros estados e organizações.

Palavras-chave: Cibersegurança; Estratégia Cibernética; Guerra Cibernética; Desenvolvimento Tecnológico; Infraestruturas Críticas; Inteligência Artificial

ABSTRAT

Israel and Hamas: the broad spectrum of combat.

This study investigated the broad spectrum of combat between Israel and the Hamas group, focusing on the cyber operations conducted by both sides. The analysis addressed the evolution of Israel's strategy, which has established itself as a global leader in cybersecurity, integrating virtual and military operations through specialized units such as Unit 8200 and technological hubs like CyberSpark. On the other hand, the organizational structure and cyber capabilities of Hamas were explored, including espionage, social media campaigns, and denial-of-service (DDoS) attacks. Recent events of the conflict were examined, including relevant virtual spectrum attacks by groups such as Killnet and Anonymous Sudan, demonstrating the complexity and sophistication of modern threats. The study highlighted the importance of robust cyber infrastructure, public-private collaboration, and the support of artificial intelligence to strengthen Israel's defense. Additionally, recommendations were provided to improve cyber defense, considering technological development, critical infrastructure protection, inter-agency cooperation, and adaptation to geopolitical challenges. It was concluded that the analysis of the conflict between Israel and Hamas offers important lessons for building effective cyber defense, applicable to other states and organizations.

Keywords: Cybersecurity; Israel; Hamas; Cyber Strategy; Cyber Warfare; Critical Infrastructures; Artificial Intelligence.

LISTA DE ABREVIATURAS E SIGLAS

BID	-	Base Industrial de Defesa
C^2	-	Comando e Controle
DDoS	-	*Distributed Denial of Service* (Negação de serviço distribuída)
IDF	-	*Israel Defense Forces* (Forças de Defesa de Israel)
IIA	-	*Israel Innovation Authority* (Autoridade de Inovação de Israel)
IL-CERT	-	*Israel Cyber Alliance* (Aliança Cibernética de Israel)
INCB	-	*Israel National Cyber Bureau* (Escritório Cibernético Nacional de Israel)
INCD	-	*Israel National Cyber Directorate* (Diretoria Nacional Cibernética de Israel)
ISF	-	*Internal Security Force* (Força de Segurança Interna)
NCSA	-	*National Cyber Security Authority* (Autoridade Nacional de Segurança Cibernética)
NSA	-	*National Security Agency* (Agência de Segurança Nacional)
$STIC^2$	-	Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle
TI	-	Tecnologia da Informação
TIC	-	Tecnologia da Informação e Comunicações

SUMÁRIO

1 INTRODUÇÃO....8
2 DEFESA CIBERNÉTICA DE ISRAEL....11
2.1 FUNDAMENTOS HISTÓRICOS DA ESTRUTURA CIBERNÉTICA....12
2.2 CAPACIDADES DE DEFESA E ATAQUE CIBERNÉTICO....17
3 AS OPERAÇÕES CIBERNÉTICAS DO GRUPO HAMAS....21
3.1 ESTRUTURA ORGANIZACIONAL E CAPACIDADES....21
3.2 EVOLUÇÃO TÁTICA....24
3.3 IMPLICAÇÕES DAS OPERAÇÕES CIBERNÉTICAS DO HAMAS....26
4 EVENTOS RECENTES DO CONFLITO ISRAEL E GRUPO HAMAS....27
4.1 ATAQUES CIBERNÉTICOS....27
4.1.1 Grupo Killnet....27
4.1.2 Anonymous Sudan....28
4.1.3 Aplicativo de Alerta de Mísseis....29
4.1.4 DDoS Generalizados....30
4.1.5 Ataques listados pelo relatório da INCD de janeiro de 2024....30
4.2 AVALIAÇÃO PARCIAL DOS RESULTADOS....32
5 LIÇÕES APRENDIDAS....35
5.1 DESENVOLVIMENTO TECNOLÓGICO E INOVAÇÃO....35
5.2 ATAQUES CIBERNÉTICOS CONTRA INFRAESTRUTURAS CRÍTICAS....37
5.3 DESAFIOS GEOPOLÍTICOS E HOSTILIDADES CIBERNÉTICAS....39
6 CONSIDERAÇÕES FINAIS....41
REFERÊNCIAS....43

1 INTRODUÇÃO

A era digital transformou o campo de batalha moderno, onde bits e bytes são tão letais quanto balas e bombas. No epicentro desta revolução encontra-se Israel, um país que, desde sua fundação, tem enfrentado desafios que exigem soluções arrojadas. O pequeno Estado do Oriente Médio não só se tornou uma potência militar convencional, mas também se estabeleceu como um dos líderes globais em segurança cibernética[1]. Sua capacidade de integrar operações no ciberespaço e militares é um testemunho de sua dedicação à inovação tecnológica e à defesa nacional.

Israel, um país nascido em meio a adversidades, reconheceu muito cedo a importância do domínio cibernético para a segurança nacional. Enfrentando uma série de desafios geopolíticos e securitários únicos. A evolução da estratégia de Israel está intrinsecamente relacionada a esses desafios, integrando capacidades ofensivas e defensivas e sustentando-se fortemente na pesquisa e no desenvolvimento tecnológico.

No entanto, o campo de batalha digital não é unidimensional. Diversas organizações têm se apresentado como adversários formidáveis no ciberespaço. Com esse intuito, este estudo explora a defesa cibernética de Israel e as operações no ciberespaço do Hamas, destacando as estratégias, táticas e tecnologias empregadas por ambos, detalhando as capacidades e desafios no domínio cibernético.

Logo, o estudo do conflito recente entre Israel e o Grupo Hamas tem como objetivo analisar as formas mais recentes de guerra cibernética de um país que se posiciona na vanguarda dos atores cibernéticos globais durante conflito entre Israel e Hamas no intervalo de um mês anterior ao dia sete de outubro de 2023 até cinco meses posteriores. As conclusões possibilitarão que a Marinha do Brasil tenha parâmetros para manter sua doutrina atualizada.

Dessa forma a dissertação analisará, de forma abrangente, a eficácia e

[1] [...] arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas. (Ministário da Defesa, 2014, p.19)

aplicabilidade do sistema de defesa cibernética de Israel. O estudo abordará a estrutura atual de defesa cibernética israelense, com foco na descrição das características de um modelo de defesa cibernética que tenha logrado sucesso diante das ameaças contemporâneas. Para alcançar esse objetivo, serão respondidas questões secundárias, tais como: o atual sistema de Guerra Cibernética de Israel obteve sucesso frente a novas tecnologias? Após os momentos iniciais do conflito, verificou-se a existência de algum novo método de ataque cibernético? Houve aumento de ações no campo cibernético no mês anterior ao ataque que possam indicar uma ação terrestre futura? As formas de ataques cibernéticos tiveram alguma mudança significativa? As estruturas críticas foram atacadas? Essas questões permitirão uma avaliação detalhada das capacidades cibernéticas e do potencial para servir como modelo internacional de defesa cibernética. O estudo está estruturado em seis capítulos, utilizando o método do estudo de caso para atingir uma conclusão.

Após essa introdução, o capítulo dois examina a robusta estratégia cibernética de Israel, detalhando suas capacidades, bem como as colaborações público-privadas que impulsionam sua eficácia. Este revela como Israel, através de uma combinação de inovação tecnológica, colaboração intersetorial e um forte compromisso com a pesquisa e desenvolvimento, conseguiu construir uma infraestrutura cibernética resiliente. A análise inclui a criação de unidades especializadas, como a Unidade 8200, e *hubs* tecnológicos, como o CyberSpark, que são fundamentais para a segurança nacional.

O terceiro capítulo foca nas operações cibernéticas do Hamas, revelando sua estrutura organizacional, táticas de espionagem e impactos internacionais. Desde a utilização de ataques simples, campanhas de mídia social até desenvolvimento de novas técnicas, o Hamas demonstra uma capacidade notável de adaptação e sofisticação em suas operações no ciberespaço. Este capítulo também aborda a colaboração internacional, destacando o apoio de Estados como Irã e Catar.

O quarto capítulo analisa os eventos recentes do conflito Israel-Hamas em 2023, destacando a intensificação dos ataques cibernéticos e as respostas inovadoras de ambos os lados. Os ataques de grupos como Killnet, Anonymous Sudan e AnonGhost ilustram a complexidade e a sofisticação das ameaças

modernas.

Já o quinto capítulo sintetiza os achados e oferta recomendações para fortalecer a defesa cibernética, considerando o desenvolvimento tecnológico, a proteção de infraestruturas críticas, a cooperação interagências e a adaptação a desafios geopolíticos. Este capítulo busca fornecer um conjunto de diretrizes e práticas recomendadas que possam ser adotadas por outros estados e organizações para garantir suas defesas cibernéticas em face de ameaças crescentes e em constante evolução.

Finalmente, o capítulo seis sintetiza o capítulo anterior, permitindo responder as questões da pesquisa e listando as principais características de um sistema de defesa cibernético contemporâneo e viável.

Este texto não se limita a um estudo sobre cibersegurança; constitui um convite para compreender como a guerra moderna é conduzida no silêncio do ciberespaço, onde os combatentes operam de maneira dissimulada, suas armas permanecem invisíveis, mas seus impactos revelam-se profundamente reais.

2 DEFESA CIBERNÉTICA DE ISRAEL

Este capítulo abordará Israel como uma potência que desenvolve uma estratégia robusta combinando capacidades avançadas. Citaremos os fundamentos históricos da estrutura cibernética que moldaram a abordagem do assunto, explorando desde suas raízes até as iniciativas mais recentes.

Desde a sua fundação, Israel enfrentou uma gama de desafios, o que levou à necessidade de soluções inovadoras e adaptativas. A evolução de sua estratégia cibernética está intrinsecamente ligada a esses revezes, refletindo uma fusão de pesquisa, desenvolvimento tecnológico e uma colaboração intensa entre o governo, academia e setor privado. A análise aprofundada dos marcos históricos e das estratégias adotadas proporcionam uma compreensão ampla de como Israel construiu uma infraestrutura antifrágil[2], destacando sua posição de liderança no cenário global de cibersegurança.

Também será abordada as operações cibernéticas significativas, tanto defensivas quanto ofensivas, que ilustram a capacidade de Israel de integrar suas operações cibernéticas com as militares convencionais. A constituição de unidades especializadas, como a Unidade 8200, e o desenvolvimento de centros tecnológicos, como o CyberSpark, são exemplos do compromisso contínuo de Israel com a inovação e a segurança. Além disso, são discutidas as colaborações público-privadas que têm sido fundamentais para o sucesso da estratégia de segurança do país, destacando como a sinergia entre diferentes setores impulsiona a eficácia das respostas a ameaças do campo virtual.

A análise do conflito entre Israel e Hamas oferece valiosos ensinamentos para a melhoria da estrutura de defesa cibernética[3]. Ao mergulhar nas intricadas redes de espionagem e no espectro virtual, ilustramos as complexidades de um campo de batalha invisível, mas extremamente poderoso.

Todavia antes de darmos novos passos, devemos ter em mente alguns conceitos que vão ajudar a entender esse novo campo dos conflitos modernos.

[2] Algumas coisas se beneficiam dos choques; elas prosperam e crescem quando expostas à volatilidade, ao acaso, à desordem e aos estressores, e amam a aventura, o risco e a incerteza. (Taleb, 2020).

[3] [...] conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente. (Ministério da Defesa, 2014, p.18).

Inicialmente devemos partir da definição de guerra cibernética:

> [...]corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C^2 do adversário, no contexto de um planejamento militar de nível operacional ou tático, ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle ($STIC^2$) do oponente e defender os próprios $STIC^2$. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC. (Ministério da Defesa, 2014, p.19).

Também necessitaremos conhecer o conceito de Operações Multidomínios:

> "são o emprego de armas combinadas de capacidades conjuntas e do Exército para criar e explorar vantagens relativas que alcancem objetivos, derrotem forças inimigas e consolidem ganhos em nome dos comandantes das forças conjuntas." (Departamento do Exército dos Estados Unidos, 2022, p. 16, tradução nossa)[4].

Já o poder cibernético é definido como "a capacidade de usar o ciberespaço para criar vantagens e influenciar eventos em outros ambientes operacionais e através dos instrumentos de poder" (Kuehl, 2009, p. 184, tradução nossa)[5] e Artefatos Cibernéticos "são equipamentos ou sistema empregado no espaço cibernético para execução de ações de proteção, exploração e ataque cibernéticos." (Ministério da Defesa, 2014, p.18). Os tipos e nomes dos artefatos serão apresentados e explicados durante o estudo de forma a facilitar o entendimento.

2.1 FUNDAMENTOS HISTÓRICOS DA ESTRUTURA CIBERNÉTICA

Desde o princípio, Israel compreendeu a importância crucial do domínio digital para a segurança nacional, com suas estratégias sendo moldadas por desafios geográficos e políticos singulares. O país tem enfrentado ameaças que necessitam de respostas inovadoras e adaptativas. A sobrevivência nacional em um ambiente hostil estimulou o desenvolvimento de uma estratégia de defesa cibernética robusta,

4 No original: "*Multidomain operations are the combined arms employment of joint and Army capabilities to create and exploit relative advantages that achieve objectives, defeat enemy forces, and consolidate gains on behalf of joint force commanders*."

5 No original: "*The ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power."*

refletindo uma fusão de capacidades ofensivas e defensivas com um forte pilar em pesquisa e desenvolvimento tecnológico (Cristiano, 2020).

No alvorecer da era digital, líderes israelenses e instituições de defesa perceberam o potencial transformador da tecnologia para a segurança nacional. Em 1997, foi estabelecida a unidade Tehila, uma infraestrutura para a era da internet, com o objetivo de fornecer às agências governamentais serviços essenciais para uma base estrutural de tecnologia da informação (TI) segura e unificada em todo o governo. As atividades oferecidas incluem acesso à internet para serviços em apoio a administração e hospedagem segura de sites, além de uma infraestrutura para apoiar futuros projetos governamentais (Tabansky, 2015).

Conquistou como seu primeiro marco o desenvolvimento da rede cibernética nacional de Israel ocorrida em 2002, quando o governo autorizou a Autoridade Nacional de Segurança da Informação (NISA) a orientar e proteger sistemas informatizados vitais de organizações civis públicas e privadas selecionadas (INCD, 2017).

Outro ponto significativo subsequente foi a criação, em janeiro de 2012, do Gabinete Cibernético Nacional de Israel (INCB), que se reportava diretamente ao Primeiro-Ministro, em consequência de uma resolução governamental de agosto de 2011. A INCB foi incumbida de conceber a política e a estratégia cibernética nacional do Estado, promover processos nacionais, desenvolver capacidades cibernéticas e fortalecer a liderança de Israel neste campo (INCD, 2017).

Em 15 de fevereiro de 2015, o governo de Israel adotou duas resoluções pioneiras que refletiam as principais recomendações da estratégia nacional de segurança cibernética desenvolvida pelo Gabinete. Essas resoluções incluíram a criação da Autoridade Nacional de Segurança Cibernética (NCSA), uma entidade governamental dedicada a liderar os esforços operacionais de segurança no campo digital do Estado de Israel. Segundo INCD (2017), a INCB e a NCSA constituem a Diretoria Nacional Cibernética de Israel (INCD), que passou a criar uma abordagem centralizada e coordenada para a segurança, sublinhando o compromisso de Israel com a defesa do espectro digital como uma base estratégica (Gori, 2022). Ela tem a responsabilidade integral pela defesa cibernética no âmbito civil. Suas atribuições incluem desde a formulação de políticas e o desenvolvimento de capacidades

tecnológicas até a operacionalização da defesa no ciberespaço. A INCD oferece serviços de gerenciamento de incidentes e diretrizes para todas as entidades civis, além de ser encarregada da proteção das infraestruturas críticas da economia israelense. Seu objetivo principal é fortalecer a resiliência do ciberespaço civil (Shamah, 2014).

Este movimento estratégico visava posicionar Israel como um líder em segurança cibernética, promovendo inovação tecnológica e estabelecendo uma infraestrutura resiliente para se proteger contra ameaças. Segundo Allison et al. (2016), "Em agosto de 2015, as Forças de Defesa de Israel (IDF) publicaram a sua primeira doutrina de defesa pública. De autoria do novo Chefe do Estado-Maior Geral das FDI, Tenente-General Gadi Eizenkot."[6], essa estratégia baseia-se em **princípios imutáveis**, como a **dissuasão**, **alerta antecipado**, **defesa**, **derrota do inimigo** e **vitória** (Allison et al., 2016).

Documentos subsequentes e a formação do INCD em 2016 reforçaram a estrutura operacional e a visão estratégica de Israel para o domínio cibernético. (Blessing; Austin, 2022). Essa estrutura da defesa é baseada em um conceito de operações genérico que define três camadas operacionais: **robustez cibernética agregada, resiliência cibernética**[7] **sistêmica** e **defesa cibernética nacional**. A abordagem oferece uma solução holística, tendo em conta as diferenças no nível de risco, a natureza da ameaça e o grau da sua clareza. Cada camada de resistência permite uma primeira resposta a incidentes que não representam uma ameaça imediata e grave, mas que podem causar danos cumulativos ao longo do tempo, ou que podem causar uma resposta grave da defesa nacional à medida que a compreensão da ameaça evolui (INCD, 2017).

A colaboração entre o setor público e privado é uma pedra angular da estratégia cibernética de Israel. Empresas privadas desempenham um papel de destaque no desenvolvimento de tecnologias avançadas e na proteção das redes do país. Muitas das inovações em cibersegurança emergem de empresas apoiadas por

[6] No original: "*In August 2015, the Israel Defense Forces (IDF) published its first-ever public defense doctrine. Authored by new IDF Chief of General Staff Lt. Gen. Gadi Eizenkot, the doctrine outlines the military's strategic and operational responses to the main threats facing Israel*."

[7] Capacidade de manter as infraestruturas críticas de tecnologia da informação e comunicações operando sob condições de ataque cibernético ou de restabelecê-las após uma ação adversa. (Ministério da Defesa, 2014; p. 19)

incubadoras e aceleradoras, frequentemente em parceria com instituições governamentais e militares (Tabansky,2015).

O modelo de colaboração de Israel é frequentemente citado como um exemplo de sucesso, onde a rápida troca de informações e recursos entre entidades públicas e privadas permite uma resposta ágil e eficaz às ameaças digitais. Esta abordagem colaborativa também facilita a criação de normas e melhores práticas de segurança que são adotadas em todo o setor. As empresas de cibersegurança em Israel beneficiam-se de uma estreita cooperação com as forças armadas, especialmente com a Unidade 8200, conhecida por sua perícia em cibersegurança e inteligência (Murphy; Borghard, 2020).

Percebemos, a infraestrutura cibernética de Israel é avançada e altamente resiliente. O país possui uma rede vigorosa de instituições de ensino e pesquisa dedicadas à cibersegurança, como o Technion e a Universidade de Tel Aviv, que fornecem uma base sólida de conhecimento e inovação. Em 1969, Israel estabeleceu o CyberSpark, um parque cibernético, denominado Beer Sheva, que serve como um *hub* para empresas de tecnologia*,* startups*,* e entidades governamentais. “executa esses programas militares com suporte de IA. Quase 14.000 homens e mulheres em uniformes militares lutam contra inimigos do Irã, Hamas, Hezbollah e outros atores estatais e não estatais.” (Ahuja, 2023, p. 1, tradução nossa)[8]. Este centro é um exemplo emblemático da estratégia de Israel, por ser o ecossistema de cibersegurança daquele país, conectando a academia, a indústria e o governo. O parque abriga a Unidade Nacional de Cibersegurança, vários empreendimentos, grandes empresas multinacionais e centros de pesquisa universitários. Esta concentração de recursos e talentos em um único local facilita a inovação rápida e soluções eficazes às ameaças (INCD, 2017; Embaixada do Brasil em Tel Aviv, 2022). Esse ambiente colaborativo é essencial para a troca de conhecimento e desenvolvimento de novas tecnologias cibernéticas (Cristiano, 2020; Embaixada do Brasil em Tel Aviv, 2022).

Além disso, a infraestrutura cibernética de Israel inclui uma rede de centros de comando e controle que operam sem interrupções, garantindo a prontidão para

[8] No original: “*The Beer Sheva complex runs these AI-supported military programmes. Nearly 14,000 men and women in military fatigues fight enemies from Iran, Hamas, Hezbollah and other state and non-state actors from China and Russia*” (Ahuja, 2023, p. 2)

detectar e mitigar ameaças em tempo real. Estas instalações são indispensáveis para a proteção das redes críticas do país e para a coordenação de respostas a incidentes cibernéticos (Tabansky, 2015).

A integração de tecnologias avançadas, como a inteligência artificial e o aprendizado da máquina, permite a Israel identificar padrões anômalos e responder de forma proativa a potenciais ataques. "Em 2018, o Prêmio do Primeiro-Ministro para Segurança foi concedido aos desenvolvedores de projeto baseado em *machine learning*[9] que teria contribuído na prevenção de centenas de ataques terroristas." (Embaixada do Brasil em Tel Aviv, 2022, p. 20). As universidades desempenham um papel essencial, não apenas na educação e treinamento de novos profissionais, mas também na pesquisa e desenvolvimento de novas tecnologias. Instituições como o Technion e a Universidade Hebraica de Jerusalém estão na vanguarda da pesquisa em cibersegurança, frequentemente colaborando com o setor privado e o governo para desenvolver soluções arrojadas para desafios cibernéticos emergentes (Tabansky, 2015; Embaixada do Brasil em Tel Aviv, 2022).

A Unidade 8200 é uma das mais renomadas unidades de inteligência do mundo, desempenha um papel de destaque na estratégia de Israel. Os veteranos dessa unidade frequentemente fundam ou se juntam a startups de cibersegurança, trazendo consigo uma vasta experiência e conhecimento técnico. “Em cerca de meia década, este ciclo deu origem a um ecossistema cibernético que conta com alguns dos melhores funcionários e tecnologia do mundo.” (Ahuja, 2023, p. 2, tradução nossa)[10].

A transferência de conhecimento do setor militar para o setor privado gera uma sinergia que promove o aperfeiçoamento e reforça a segurança nacional. Além disso, o governo israelense implementou várias iniciativas para fomentar a colaboração público-privada. O Israel Cyber Alliance (IL-CERT) é um exemplo de parceria entre o setor público e privado que facilita a troca de informações sobre ameaças cibernéticas e promove a cooperação na resposta a incidentes. Essa

[9] O Machine Learning and Intelligent Systems promove pesquisa, criação de conhecimento e colaboração em IA entre pesquisadores do Technion e entre o Technion e instituições externas. (Embaixada do Brasil em Tel Aviv, 2022)

[10] No original: “*In about half a decade, this cycle has given rise to a cyber ecosystem that has some of the best personnel and technology in the world*.” (Ahuja, 2023, p. 2)

colaboração garante que as melhores práticas e tecnologias de cibersegurança sejam compartilhadas e implementadas em todo o setor (Tabansky, 2015).

Outra iniciativa importante é a Israel Innovation Authority (IIA), que oferece suporte financeiro e recursos para startups de cibersegurança. A IIA ajuda a obter financiamento, desenvolver seus produtos e entrar no mercado global. Este apoio é fulcral para o desenvolvimento de novas tecnologias e a criação de empregos no setor de cibersegurança (Tabansky, 2015). Estas instituições oferecem suporte técnico e financeiro para startups em estágio inicial, ajudando-as a desenvolver suas tecnologias e expandir seus negócios.

A colaboração entre o setor público e privado também é facilitada por eventos e conferências de cibersegurança, como a conferência anual Cyber Week, realizada em Tel Aviv. Este evento atrai especialistas de todo o mundo, promovendo a troca de conhecimentos e a formação de parcerias entre empresas, governos e instituições acadêmicas (Murphy; Borghard, 2020).

2.2 CAPACIDADES DE DEFESA E ATAQUE CIBERNÉTICO

Israel é conhecido por seu poder cibernético tanto de defesa quanto de ataque cibernético. As capacidades de defesa de Israel são complementadas por uma abordagem proativa à segurança. Em vez de apenas reagir a incidentes, adota uma postura preventiva, utilizando inteligência artificial e análise preditiva para identificar e neutralizar ameaças antes que elas se materializem. Além disso, a integração de tecnologias avançadas de criptografia e autenticação fortalece a segurança das redes críticas conforme descreve Cristiano (2020). O país investiu pesadamente em suas forças de defesa cibernética, particularmente na Unidade 8200. Esta unidade é responsável por muitas das inovações e operações de cibersegurança do país, desde a coleta de inteligência até a execução de ataques cibernéticos ofensivos (Blessing e Austin, 2022).

A Unidade 8200 tem sido fundamental no desenvolvimento das capacidades cibernéticas do país. Esta unidade, muitas vezes comparada à Agência de Segurança Nacional (NSA) dos Estados Unidos, é responsável por uma ampla gama de operações, incluindo espionagem, coleta de inteligência, e ataques cibernéticos

ofensivos. As atividades são frequentemente citadas como exemplos de cibersegurança avançada, e a unidade é reconhecida internacionalmente por sua sofisticação e eficácia (Cristiano, 2020).

Um exemplo notável das capacidades cibernéticas de Israel é a operação Orchard em 2007, onde um ataque precedeu uma investida aérea a uma instalação nuclear na Síria. Mesmo essa investindo milhões de dólares em sistemas de defesa aérea, não havia nada fora do comum nos radares. “Os céus sobre a Síria pareciam seguros e totalmente vazios quando passava da meia-noite. Entretanto, formações de Eagles e Falcons penetram o espaço aéreo sírio a partir da Turquia” (Clarke; Knake, 2015). Esta ação demonstrou a habilidade de Israel de integrar operações cibernéticas com militares convencionais, criando uma sinergia que amplifica a eficácia das suas operações de defesa e ataque (Blessing e Austin, 2022)

Nos conflitos na Faixa de Gaza, durante a Operação Chumbo Fundido (2008-2009), Israel enfrentou uma série de ataques cibernéticos que tentaram derrubar ou desfigurar sites governamentais e militares.

Além da operação Orchard, Israel tem conduzido várias outras operações cibernéticas ofensivas que destacam suas capacidades avançadas. Em 2010, a descoberta do *malware* Stuxnet, amplamente atribuído a uma colaboração entre Israel e os Estados Unidos, demonstrou a capacidade de Israel de desenvolver e implantar artefatos sofisticados. O Stuxnet foi projetado para sabotar as centrífugas nucleares do Irã, retardando significativamente o programa nuclear do país (Cristiano, 2020). Embora nunca oficialmente confirmado, Israel é amplamente acreditado como coautor, com os Estados Unidos, do *worm* Stuxnet. Este foi um ataque cibernético sofisticado que visou sabotar o programa nuclear iraniano. Além de Stuxnet, Israel foi tanto alvo quanto perpetrador de várias campanhas de espionagem e ataques de negação de serviço (DDoS) [11]. Estes têm sido

[11] Os chamados “ataques de negação de serviço” são exatamente aqueles que visam indisponibilizar um sistema de informação, que deixa de oferecer o serviço para o qual foi concebido – ou, ainda, passa a oferecê-lo de maneira precária. A partir do final da década de 1990 percebeu-se que a indisponibilidade de sistemas poderia ser forçada a partir da sobrecarga de requisições causada pela atuação coordenada de um grande número de máquinas executando solicitações rotineiras a um sistema de informação. Devido à ação de diversas unidades computacionais atuando como um sistema distribuído, tais ataques passaram a ser denominados Ataques Distribuídos de Negação de Serviço, ou ataques DDoS. (Clarke; Knake, 2015, p. 271).

particularmente intensos em momentos de tensão política ou militar elevada. (Gori, 2022).

Na Operação Pilar de Defesa (2012) e Operação Margem Protetora (2014), ambas marcadas por intensas em guerra cibernética contra grupos palestinos, com ataques DDoS e campanhas de hacking sendo os mais comuns (Handler, 2022).

Em 2021 na faixa de Gaza, além dos combates físicos, houve relatos de uma série de ciberataques contra infraestruturas israelenses e palestinas, incluindo tentativas de interrupção de serviços de comunicação e dados (Embaixada do Brasil em Tel Aviv, 2022).

Israel também tem se destacado na defesa contra investidas cibernéticas. Durante os conflitos com Hamas e outros grupos, Israel conseguiu repelir ataques coordenados destinados a desestabilizar suas infraestruturas críticas. As unidades de defesa cibernética colaboram de maneira próxima com outras agências de segurança para vigiar, identificar e eliminar ameaças digitais em tempo real segundo Cristiano (2020). O surgimento do Cyber Dome, um sistema avançado de defesa cibernética, utiliza *big data*, inteligência artificial e outras tecnologias digitais para proteger as infraestruturas críticas de Israel. Este sistema é composto por um conjunto de unidades, incluindo a Unidade 8200, Mossad, Shin Bet e a Diretoria de Defesa Cibernética do IDF. O Cyber Dome foi projetado para combater guerras virtuais de maneira similar ao Iron Dome, mas focado no ciberespaço (Ahuja, 2023).

Além das capacidades de defesa e ataque, Israel tem desenvolvido técnicas para garantir a resiliência cibernética de suas infraestruturas vitais. Estas estratégias incluem a implementação de redundâncias, a realização de testes de penetração regulares e o desenvolvimento de planos de resposta a incidentes detalhados. “Queremos ser atacados. Envie-nos os trojans e malware. Isso nos ajuda a nos preparar melhor. Não apenas nos prepararemos, mas também diremos ao resto do mundo como fazê-lo.” (Ahuja, 2023, p. 1, tradução nossa).[12]

[12] No original: “*We want to be attacked. Send us the trojans and malware. It helps us prepare better. Not only will we prepare ourselves, we will tell the rest of the world how to do it.”* (Ahuja, 2023, p. 1).

Israel também investe em programas de educação e treinamento para garantir que todos os operadores de infraestruturas críticas estejam bem-preparados para lidar com ataques cibernéticos (Blessing e Austin, 2022).

Para Israel, é notável que o enfrentamento de um cenário global em constante evolução requer uma estratégia de defesa cibernética que se adapte continuamente a novos desafios e tecnologias emergentes. O compromisso com a pesquisa e desenvolvimento, a colaboração internacional e a educação continuarão a ser crucial para aprimorar a capacidade defensiva de Israel. A adaptação as ameaças emergentes e a promoção de um ecossistema cibernético seguro e resiliente permanecem no cerne da estratégia nacional de Israel. Este posicionamento reflete uma abordagem integrada e contemporânea para garantir a segurança nacional no domínio digital. Através de uma combinação de capacidades, parcerias estratégicas e um compromisso com a inovação, Israel estabelece-se como um dos líderes globais em guerra cibernética. À medida que o país enfrenta desafios futuros, sua estratégia cibernética continuará a evoluir, reafirmando seu compromisso com a proteção do ciberespaço nacional e internacional.

3 AS OPERAÇÕES CIBERNÉTICAS DO GRUPO HAMAS

A transformação digital e o avanço das tecnologias de informação têm impactado significativamente o cenário geopolítico global, introduzindo novas dimensões nos conflitos. O grupo Hamas, uma organização política e militar palestina que, além de suas operações militares convencionais, tem desenvolvido capacidades cibernéticas sofisticadas.

Desde que assumiu realmente o controle da Faixa de Gaza em 2007, o Hamas tem enfrentado incontáveis adversidades, o que incentivou a adoção de estratégias audaciosas no campo digital. A análise detalhada da estrutura organizacional e das capacidades cibernéticas do Hamas revela como a organização integra espionagem e operações de influência informacional em suas táticas. A evolução dessas táticas vem se destacando em operações recentes que utilizam engenharia social e aplicativos móveis maliciosos, demonstra a adaptabilidade e a sofisticação crescente do grupo.

Este capítulo também aborda a colaboração internacional que tem sido determinante para o desenvolvimento das capacidades cibernéticas do Hamas. O suporte de aliados, proporcionando financiamento e recursos tecnológicos, tem sido fundamental para o aprimoramento contínuo das operações. A análise destas dinâmicas oferece uma compreensão abrangente de como o Hamas utiliza o ciberespaço para complementar suas ações militares convencionais e influenciar o ambiente de informação global.

Por fim, destacamos as implicações globais dessas operações, enfatizando a necessidade de uma vigilância contínua e de estratégias de defesa cibernética para mitigar os riscos associados a essas atividades. Compreender as capacidades e as táticas no campo digital do Hamas é essencial para desenvolver respostas eficazes a esses riscos despontantes no cenário global de segurança.

3.1 ESTRUTURA ORGANIZACIONAL E CAPACIDADES

O Hamas, conhecido formalmente como Harakat al-Muqawama al-Islamiyya (Movimento Islâmico de Resistência), é uma organização política e militar palestina que governa a Faixa de Gaza. Embora amplamente reconhecido por suas

operações militares convencionais e ataques terroristas, o Hamas também desenvolveu capacidades cibernéticas significativas, que evoluem em sofisticação e impacto ao longo dos anos (Gori, 2022).

A estrutura cibernética do Hamas está intrinsecamente ligada ao seu braço militar, as Brigadas Izz al-Din al-Qassam. Dentro deste corpo, destaca-se a Internal Security Force (ISF), composta por membros da força de segurança al-Majd. A ISF é responsável por operações de espionagem e por suprimir a oposição política e dissidências dentro do partido e do aparato de segurança. A diversidade das missões da ISF manifesta-se nas operações cibernéticas do Hamas, que abrangem uma ampla. gama de atividades, incluindo as operações de influência informacional. Contudo, "operações cibernéticas do Hamas são majoritariamente focadas em espionagem, buscando obter inteligência valiosa para fornecer vantagens decisórias a seus líderes e comandantes em arenas políticas e militares" (Handler, 2022, p. 13). Dessa forma, “A propaganda desempenha um papel crítico para o Hamas, pois busca fortalecer sua popularidade. Os temas mais comuns da propaganda do Hamas envolvem justificar o lugar do grupo dentro da comunidade palestina e legitimar seu governo em Gaza.” (Byman; McCaleb, 2023, p. 2, tradução nossa).[13]

Usam normalmente como táticas o *spear phishing*[14], ataques DDoS, vazamentos de dados e exploração de vulnerabilidades em sistemas de TI. Essas atividades são frequentemente apoiadas por atores estatais como Irã, Coreia do Norte, Rússia e China (Centro Simon Wiesenthal, 2023).

Segundo Handler (2022), umas das técnicas iniciais do Hamas envolvia a distribuição de anexos maliciosos. Este tipo de artefato cibernético demorou cerca de 3 anos para ser descoberto.

> As táticas iniciais do grupo centraram-se numa abordagem de “spray and pray”, distribuindo correios eletrônicos impessoais com anexos maliciosos a um grande número de alvos, na esperança de que um subconjunto os atacasse. Por exemplo, uma operação que começou em meados de 2013 e

[13] No original: “*Propaganda plays a critical role for Hamas as it seeks to shore up its popularity. The most common Hamas propaganda themes concern justifying the group’s place within the Palestinian community and legitimizing its rule in Gaza*.” (Ahuja, 2023, p. 2).

[14] Os ataques de phishing geralmente envolvem correios eletrônicos genéricos que tentam forçar o destinatário a compartilhar dados pessoais, como senhas e detalhes de cartão de crédito. O phisher então usa essas informações para fins mal-intencionados, como roubo de identidade ou fraude financeira. (Kaspersky, 2024).

> foi descoberta em fevereiro de 2015 envolveu operadores do Hamas que atraíam alvos com a promessa de vídeos pornográficos que eram, na verdade, aplicações de malware. Os operadores dependiam de suas vítimas – que incluíam alvos nos setores governamentais, militar, acadêmico, de transporte e de infraestrutura – retendo informações sobre os incidentes dos departamentos de tecnologia da informação no local de trabalho, por vergonha de clicarem em pornografia no trabalho, maximizando assim o acesso e tempo no alvo. (Handler, 2022, p. 7, tradução nossa).[15]

Além da espionagem, um subconjunto das operações cibernéticas do Hamas envolve o uso de informações coletadas para influenciar o público. Essas operações de informação incluem desde *hack-and-leaks*, quando hackers adquirem informações secretas e as tornam públicas, até campanhas de mídia social que promovem narrativas favoráveis ao Hamas. Em dezembro de 2014, o Hamas reivindicou o crédito por hackear a rede classificada das IDF e divulgar vários vídeos detalhando operações militares israelenses (Byman; McCaleb, 2023).

Outro método empregado pelo Hamas é a desfiguração de sites, uma forma de vandalismo online que envolve a invasão de sites para postar propaganda. Durante a Operação Protective Edge em 2014, o Hamas conseguiu acesso à transmissão via satélite do canal de televisão israelense Channel 10, transmitindo imagens de palestinos feridos supostamente por ataques aéreos (Handler, 2022). De acordo com Byman e McCaleb (2023), "essas táticas demonstram a capacidade do Hamas de integrar operações cibernéticas em sua estratégia de guerra, ampliando seu impacto e alcance.".

Ademais, a infraestrutura do Hamas inclui uma rede de centros de comando e controle, responsáveis por coordenar e executar ataques cibernéticos. Estes centros são fundamentais para garantir que as operações do Hamas sejam bem coordenadas e eficazes, permitindo uma resposta rápida e adaptativa às ações dos seus adversários (Tabansky, 2015). Também integrou sistemas de rede avançados

[15] No original: "*Naturally, Israel is a primary target of Hamas's cyber espionage. These operations have become commonplace over the last several years, gradually evolving from broad, blunt tactics into more tailored, sophisticated approaches. The group's initial tactics focused on a 'spray and pray' approach, distributing impersonal emails with malicious attachments to a large number of targets, hoping that a subset would bite. For example, an operation that began in mid-2013 and was discovered in February 2015 entailed Hamas operators luring targets with the promise of pornographic videos that were really malware apps. The operators relied on their victims—which included targets across the government, military, academic, transportation, and infrastructure sectors—withholding information about the incidents from their workplace information technology departments, out of shame for clicking on pornography at work, thereby maximizing access and time on the target."* (Handler, 2022, p. 7).

dentro de seus túneis de terror, permitindo que os agentes nos centros de comando e controle supervisionem eventos em qualquer um dos túneis (Shamah, 2014).

O Hamas se engajou em ataques digitais mais refinados, visando não apenas coletar informações, mas também causar danos diretos a infraestruturas críticas. Em 2016, o grupo estava desenvolvendo malware capaz de desativar redes elétricas e sistemas de água. Essa categoria de ataque demonstra uma escalada na ambição e capacidade do Hamas em utilizar a guerra cibernética como uma ferramenta de combate e desestabilização (Leon, 2023).

3.2 EVOLUÇÃO TÁTICA

A evolução das táticas é evidente em suas campanhas mais recentes. Em 2017, o Hamas adotou uma abordagem mais personalizada usando técnicas de engenharia social[16] para direcionar *malware* a partir de perfis falsos no Facebook, visando o pessoal das IDF. Essa evolução continuou com o desenvolvimento de vários aplicativos para smartphone que instalavam *trojans*[17] de acesso remoto em dispositivos. Em 2018, o Hamas disfarçou *spyware*[18] em um aplicativo de alerta de foguetes chamado Red Alert, direcionado a israelenses (Handler, 2022).

Outro exemplo notável foi a operação de 2020, onde o Hamas utilizou aplicativos de namoro como “Catch&See e GrixyApp” para implantar *spyware* nos celulares dos alvos. Estes aplicativos permitiram ao Hamas coletar informações sobre diversas instalações militares e equipamentos das IDF, incluindo veículos blindados (Handler, 2022).

De acordo com a firma de inteligência de ameaças Cybereason, as operações do Hamas indicam um novo nível de sofisticação. Em abril de 2022, uma campanha de espionagem cibernética visando indivíduos das forças militares, policiais e de

[16] A engenharia social é um método usado para enganar, manipular ou explorar a confiança das pessoas. É uma forma de ataque sem violência física que busca fazer com que a vítima realize voluntariamente ações prejudiciais a si mesma, como divulgar informações sensíveis ou transferir dinheiro para desconhecidos. (ABIN, 2021, p. 7)

[17] Trata-se de um programa que tem um pacote de vírus e na maioria das vezes é utilizado para se conseguir informações de outros computadores ou executar operações indevidas em diversos dispositivos. (CanalTech, 2014)

[18] Spyware é um software instalado sem que você saiba, seja em um computador tradicional, um aplicativo no navegador da Web ou um aplicativo que reside em seu dispositivo móvel. Ou seja, o spyware transmite suas informações pessoais confidenciais para um invasor. (Kaspersky, 2024).

serviços de emergência israelenses utilizou *malware* previamente não documentado, destacando um avanço significativo nas capacidades operacionais do grupo (Buckley; Connor, 2023; Leon, 2023).

O suporte internacional tem sido decisivo para as atividades cibernéticas do Hamas. A Turquia, por exemplo, foi reportada como um local de operações do Hamas, proporcionando um refúgio seguro e recursos tecnológicos. Além disso, estados patrocinadores têm oferecido financiamento, santuários e tecnologia de armas, permitindo ao Hamas continuar desenvolvendo suas potencialidades ofensivas (Shamah, 2014). Handler (2022) afirma que "a colaboração entre o Hamas e estados como Irã e Catar é fundamental para o aprimoramento contínuo de suas capacidades cibernéticas".

> Embora Doha permita que o Hamas utilize a sua tecnologia para combater Israel, é com a sua própria segurança cibernética que os líderes do Catar estão preocupados. Para eles, a guerra entre Israel e o Hamas é um campo de provas para ver como os seus investimentos em sistemas cibernéticos valeram a pena. (Shamah, 2014, p. 1, tradução nossa)[19].

O relacionamento com o Irã é particularmente significativo, pois este país tem fornecido expressivo financiamento, treinamento e suporte técnico ao Hamas, permitindo ao grupo acessar tecnologias avançadas e desenvolver suas próprias capacidades cibernéticas internamente. Esta relação de suporte estratégico e técnico tem sido um fator impulsionador para a evolução das habilidades digitais do Hamas, permitindo que o grupo implemente ataques mais sofisticados e direcionados. A colaboração entre o Hamas e especialistas iranianos tem resultado em uma troca constante de informações e tecnologias, fortalecendo a capacidade do Hamas de conduzir operações complexas e de alto impacto (Byman; McCaleb, 2023).

Nesse contexto o Hamas tem utilizado criptoativos para financiar suas operações. Desde 2019, seu braço militar, Brigadas *Izz al-Din al-Qassam*, tenta usar criptomoedas como método alternativo de arrecadação de fundos. Plataformas como PayPal, Wise e várias criptomoedas têm sido efetivas para facilitar doações e transferências de valor (Centro Simon Wiesenthal, 2023).

[19] No original: ‘*While Doha is allowing Hamas to use its technology to fight Israel, it’s their own cyber-security the leaders of Qatar are worried about. “For them, the war between Israel and Hamas is a proving ground to see how their investments in cyber systems have paid off””* (Shamah, 2014, p. 1).

As operações cibernéticas do Hamas refletem uma adaptação contínua e aprimoramento de suas estratégias de resistência e influência. Com táticas cada vez mais sofisticadas e suporte de estados aliados, o grupo se posiciona como um ator com prestígio digital emergente e capaz. As suas operações demonstram uma capacidade de influenciar o ambiente informacional de maneira significativa, subsidiando suas ações militares convencionais (Leon, 2023; Byman, 2023).

Além das operações clássicas, o Hamas tem utilizado suas capacidades cibernéticas para operações psicológicas e de propaganda. Por meio de campanhas nas redes sociais e outros meios digitais, busca desestabilizar o moral dos seus adversários e ganhar apoio da opinião pública. Durante conflitos intensos, como a Operação Margem Protetora em 2014, essas campanhas se intensificaram, com o Hamas divulgando vídeos e mensagens que pretendiam mostrar sua força e a suposta fraqueza do inimigo (Handler, 2022).

Uma parte significativa das operações cibernéticas do Hamas envolve a coleta e utilização de inteligência para planejar e executar ataques. As informações coletadas através de espionagem do campo digital são frequentemente utilizadas para identificar alvos vulneráveis e planejar operações de sabotagem ou ataques coordenados. Este ciclo contínuo de coleta de inteligência e ação reflete a complexidade e rendimento das operações do Hamas (Byman, 2023).

3.3 IMPLICAÇÕES DAS OPERAÇÕES CIBERNÉTICAS DO HAMAS

As operações cibernéticas do Hamas representam uma evolução significativa na sua estratégia, realizando operações de influência informacional e ataques diretos a infraestruturas críticas. A versatilidade e a eficácia das suas operações no ciberespaço são evidentes nas táticas sofisticadas e no suporte internacional que a organização recebe. Estes apoios proporcionam os recursos e a expertise para perpetrarem suas ações, eminentemente ideológicas.

A análise detalhada das táticas e operações revela uma organização que se adapta continuamente às mudanças tecnológicas e aos desafios geopolíticos, utilizando o ciberespaço como uma extensão de suas operações militares convencionais. As implicações globais dessas atividades destacam a necessidade

de vigilância contínua e de estratégias robustas de defesa para mitigar os riscos associados a segurança global.

4 EVENTOS RECENTES DO CONFLITO ISRAEL E GRUPO HAMAS

O conflito entre Israel e Hamas em 2023 marcou um novo capítulo na guerra cibernética, destacando a importância das operações multidomínios no contexto de conflitos armados modernos. Logo, em 7 de outubro, o Hamas realizou uma série de ataques coordenados contra comunidades judaicas em Israel, resultando na morte de mais de 1.200 pessoas, o dia mais mortal para os judeus desde o Holocausto (Sands; Suliman, 2023). Em resposta, Israel intensificou suas operações defensivas e ofensivas. O Cyber Dome e outras iniciativas cibernéticas foram mobilizadas para combater as ameaças digitais e proteger todas as infraestruturas de Israel (Ahuja, 2023). Dessa forma, este capítulo examina as principais ocorrências no campo digital durante este conflito.

4.1 ATAQUES CIBERNÉTICOS

Aqui serão listados os ataques que foram noticiados e os mencionados por instituições israelenses. Ressaltamos que, inevitavelmente, haverá ataques que não foram divulgados e outros, muito provavelmente, nem identificados. Dessa forma, os casos apresentados servirão para ampliar nossa análise sobre o tema.

4.1.1 Grupo Killnet

O grupo Killnet, uma coletividade de hackers pró-Rússia, que é conhecido por realizar ataques de negação de serviço distribuído (DDoS), fez declarações públicas de apoio ao Hamas e anunciou intenções de continuar atacando o governo israelense. Essas ações destacam a natureza complexa do ciberespaço como um campo de batalha onde atores estatais e não estatais podem exercer influência significativa (Centro Simon Wiesenthal, 2023).

O Killnet visou diversos alvos nos sistemas de Israel, incluindo sites do governo e da agência de segurança Shin Bet, agência do campo da contrainteligência focada em possíveis sabotagens, atividades terroristas e questões de segurança de natureza fortemente política, sobrecarregando os servidores com solicitações excessivas e comprometendo suas funcionalidades (Security Leaders,

2023a). Esses ataques certificam a capacidade técnica e a intenção de usar ciberataques como ferramenta de influência política em meio a tensões geopolíticas. Além disso, o impacto desses ataques não se limitou à interrupção dos serviços online. Eles obrigaram Israel a implementar medidas de segurança avançadas e a fortalecer a cooperação com aliados internacionais para compartilhar inteligência sobre ameaças cibernéticas e estratégias de defesa.

Os ataques do Killnet foram caracterizados por uma sofisticação técnica que envolveu o uso de *botnets*[20] distribuídas, dificultando as defesas israelenses a distinguir entre tráfego legítimo e malicioso. Ademais, o grupo utilizou técnicas de camuflagem para evitar a detecção, desafiando as capacidades de resposta rápida das defesas cibernéticas israelenses (Security Leaders, 2023a).

A escalada desses ataques reflete uma tendência crescente de grupos hacktivistas que operam em sincronia com interesses geopolíticos maiores, demonstrando que a cibersegurança não é apenas uma questão técnica, mas também um componente estratégico de defesa nacional.

4.1.2 Anonymous Sudan

O grupo Anonymous Sudan também se destacou no cenário digital durante o conflito. Este declarou apoio à resistência Palestina e assumiu a responsabilidade por ataques cibernéticos contra alvos israelenses, incluindo o website do *The Jerusalem Post* (Security Leaders, 2023a). A suspeita de que eles possam ser uma frente russa sugere uma possível manipulação ou apoio oculto por parte da Rússia, com intuito de influenciar conflitos no Oriente Médio (Centro Simon Wiesenthal, 2023).

Os ataques DDoS realizados pelo Anonymous Sudan e Team_insane_Pakistan, como o que visou o The Jerusalem Post, envolvem a inundação de servidores com tráfego excessivo, sobrecarregando-os e interrompendo os serviços (Security Leaders, 2023b). Os ataques não apenas causaram interrupções, mas também tiveram um efeito psicológico, amplificando o

[20] Os computadores atacantes são chamados de botnet, uma rede robótica de computadores “zumbis” controlados remotamente. (Clarke; Knake, 2015, p. 26)

caos e a desinformação. Isso ilustra como a guerra cibernética pode ser usada para desestabilizar não apenas a infraestrutura crítica, mas também a confiança pública e a coesão social (Centro Simon Wiesenthal, 2023). Esses ataques têm um impacto significativo na comunicação e na disseminação de informações, especialmente durante períodos de elevada tensão.

4.1.3 Aplicativo de Alerta de Mísseis

O grupo de hackers AnonGhost realizou um ataque significativo ao explorar uma vulnerabilidade em um aplicativo de alerta de mísseis amplamente usado por cidadãos israelenses. Este ataque destaca a importância de proteger aplicativos que desempenham funções críticas em segurança nacional e a necessidade de uma vigilância contínua contra artefatos cibernéticos em um mundo cada vez mais digital e conectado (Centro Simon Wiesenthal, 2023).

O AnonGhost conseguiu explorar uma falha de segurança específica no aplicativo de alerta de mísseis, permitindo a inserção de notificações falsas. Os principais impactos desse ataque foram psicológicos e sociais, induzindo pânico e desorientação. Além disso, alertas falsos podem levar a uma mobilização desnecessária de serviços de emergência, desviando recursos críticos de situações reais de emergência (Centro Simon Wiesenthal, 2023). A longo prazo, tais ataques podem danificar a reputação dos sistemas de alerta, levando a dúvidas sobre sua confiabilidade.

Em resposta aos ataques cibernéticos contra Israel, grupos de hackers que apoiam Israel, como o Indian Cyber Force, conduziram contra-ataques visando entidades associadas com a Palestina. Esses grupos derrubaram importantes sites palestinos, incluindo o do Banco Nacional Palestino e o site do Hamas (Mozelli, 2023).

Os contra-ataques visaram minar a operacionalidade e a eficácia organizacional dos grupos palestinos. Esses eventos destacam a natureza interconectada dos conflitos modernos, onde o ciberespaço se torna um teatro de operações estratégico e tático (Centro Simon Wiesenthal, 2023). Outrossim, há de se avaliar as questões legais e éticas, especialmente quando envolvem

infraestruturas civis como bancos, potencialmente colocando em risco dados e serviços essenciais para a população civil (Gori, 2022).

4.1.4 DDoS Generalizados

Durante o conflito, foram identificados o uso extensivo de ataques DDoS ao nível da aplicação e ao nível da comunicação, bem como desfiguração de websites (INCD, 2024). Israel foi alvo de uma série de ataques generalizados, visando sua infraestrutura crítica, incluindo plantas energéticas e sistemas de alerta. Esses ataques são comuns por sua relativa facilidade de execução e pelo impacto significativo que podem causar (Security Leaders, 2023a).

> Grupos ciberterroristas juntaram-se à briga, lançando os seus próprios ataques a websites israelitas. Notadamente, foram identificados atores específicos de ameaças cibernéticas, incluindo: um ator baseado em Gaza conhecido como Storm-1133 que tem como alvo os sectores israelitas de energia, defesa e telecomunicações; um grupo ligado ao Irã, Imperial Kitten, que visa o sector tecnológico do Oriente Médio, incluindo Israel; e The Returnees, um grupo de hackers que tem como alvo tanto a infraestrutura israelense quanto cidadãos individuais." (Centro Simon Wiesenthal, 2023, p.3, tradução nossa).[21]

Muitos desses ataques reivindicados por grupos hacktivistas não puderam ser verificados de forma independente, levantando questões sobre a autenticidade e a escala real das operações reportadas (Centro Simon Wiesenthal, 2023). Em cenários de conflito, a desinformação pode ser usada como uma tática para exagerar a eficácia de um ataque e manipular a percepção pública (Security Leaders, 2023a).

4.1.5 Ataques listados pelo relatório da INCD de janeiro de 2024

[21] No original: "*Cyberterrorist groups have joined the fray, launching their own attacks on Israeli websites. Notably, specific cyber threat actors have been identified, including: a Gaza-based actor known as Storm-1133 who has targeted Israeli energy, defense, and telecommunications sectors; an Iran-linked group, Imperial Kitten, targeting the Middle East's tech sector, including Israel; and The Returnees, a hacker collective that has targeted both Israeli infrastructure and individual citizens.*" (Centro Simon Wiesenthal, 2023, p.3).

Houve uma ampla atividade de ações por pulverização, onde diversas tentativas foram realizadas para explorar vulnerabilidades e erros humanos na aplicação de configurações, como uso de senhas fracas e ausência de limites para tentativas de autenticação malsucedidas. Tentativas Múltiplas de Penetração em vários ativos foram feitas para obter acesso e provocar vazamento ou exclusão de informações (INCD, 2024). Foi percebido um aumento de cerca de 20% nos ataques cibernéticos contra Israel durante a guerra em 2023, com um aumento de mais de 50% especificamente direcionado ao setor governamental (CISO Advisor, 2023b; Security Leaders, 2023b).

Diversos grupos, como o Imperial Kitten, lançaram operações cibernéticas contra organizações israelenses, principalmente entidades públicas e governamentais. Esses artefatos incluem *malware*[22], ransomware[23] e wipers[24]. Os ataques exploraram iscas de *phishing* com temas de recrutamento de emprego para infectar sistemas e obter persistência na rede (Kaur, 2023).

> "Um grupo pró-Hamas chamado Cyber Av3ngers teve como alvo a Noga – Israel Independent System Operator, empresa com sede em Heifa que opera rede elétrica, alegando ter comprometido sua rede e desligado seu site. O grupo também mirou a Israel Electric Corporation, a maior fornecedora de energia elétrica em Israel e nos territórios palestinos, bem como uma usina." (CISO Advisor, 2023a, p. 2).

Além das atuações comuns em sistemas Windows, foram detectadas ações contra sistemas Linux, incluindo a ativação de *wipers* como parte de ataques de destruição. Técnicas diversas para elevação de privilégios e persistência através de mecanismos de comando no Linux que permitem programar tarefas para serem executadas de maneira independente foram documentadas (Centro Simon Wiesenthal, 2023).

[22] Popularmente conhecidos como "vírus", os malwares são softwares maliciosos que contaminam dispositivos, sejam PCs, smartphones ou outros (CanalTech, 2024).

[23] Malware can do a lot of things including encrypting your files so that you don't have access to it, which leads you to pay the hackers so that you can access your files. This particular type of malware is called Ransomware, seeing that you have to pay ransom to be able to access your files. (Tindall, 2021, p. 12).

[24] Um limpador é um malware que exclui ou destrói o acesso de uma organização a arquivos e dados. Este tipo de malware é comumente usado como uma ferramenta de destruição e interrupção, uma vez que a perda de informações críticas pode impossibilitar uma organização de manter operações comerciais ou realizar determinadas ações (Check Point Software, 2024).

Conforme relatório da INCD (2024), as câmeras de segurança foram atacadas via internet com o objetivo de prejudicar ou impedir seu uso para monitoramento físico, além de utilizá-las como ferramentas de espionagem para coletar informações das áreas observadas. Diversos outros dispositivos conectados a internet foram alvos de ataques e operações de influência nas redes sociais para utilização de diversos canais e personificação de perfis, publicação de informações falsas ou informações tecnicamente corretas sem contexto relevante, com o intuito de enganar, prejudicar ou manipular a opinião pública. Em adição, ocorreram atuações com *phishing*, como uso de engenharia social por correios eletrônicos e mensagens de texto para aumentar a credibilidade dos ataques. Por fim, informações pessoais dos destinatários eram às vezes adicionadas para persuadi-los a clicar em links ou anexos. Este tipo de campanha aumentou significativamente durante a guerra.

Detectou-se atuações no campo digital contra organizações do setor de provedores de serviços gerenciados, que fornecem serviços essenciais para muitas outras. Isso inclui empresas de hospedagem web e prestadoras de serviços de integração e TI (Kaur, 2023). Quinze grupos principais, associados ao Irã, Hamas e Hezbollah, foram observados operando contra o ciberespaço israelense durante a guerra, colaborando e compartilhando informações, métodos e ferramentas para realizar diversas ações. Entre eles, destaca-se o grupo Cyber Toufan, que atacou empresas israelenses como Signature-IT e Ikea, vazando grandes bancos de dados com informações pessoais de milhões de usuários (INCD, 2024). O grupo também atuou contra a Max Security e a Radware, duas empresas de segurança cibernética e geointeligência em Israel (CISO Advisor, 2023b). Podemos mencionar também os Ghosts of Palestine e o AnonGhost, que lançaram campanhas de desfiguração de sites e DDoS contra alvos israelenses. Esses grupos utilizaram plataformas como o Telegram para coordenar ataques e compartilhar seus feitos publicamente (Mozelli, 2023).

4.2 AVALIAÇÃO PARCIAL DOS RESULTADOS

A resposta a essas atividades requer colaboração internacional e coordenação entre agências de segurança cibernética para rastrear, mitigar e

prevenir ataques. Essa colaboração permite a partilha de inteligência e melhores práticas para responder efetivamente a esses perigos. Ampliar a conscientização sobre segurança nesse campo virtual entre os stakeholders de infraestruturas críticas também podem ajudar a preparar e responder contra essas ações, minimizando o impacto de desinformações ou ataques reais. Somente dessa forma será possível fortalecer as infraestruturas críticas essenciais para proteção contra esses riscos (Gori, 2022).

Adicionalmente, iniciativas para estabelecer normas e protocolos que regulem a conduta em ciberespaço são fundamentais para enfrentar os desafios legais e éticos associados a esses ataques (Ahuja, 2023). Especificamente, é preciso analisar as questões éticas quando existir efeitos diretos aos civis, como instituições bancárias, que podem ameaçar dados e serviços essenciais para a população. Este aspecto ressalta a importância de uma regulamentação vigorosa e de medidas de proteção adequadas para garantir a segurança e a continuidade dos serviços essenciais.

Os eventos de 2023 esclarecem a constituição complexa da guerra cibernética no conflito entre Israel e Hamas, envolvendo uma mistura de hacktivismo, ataques direcionados e ações de contra-ataque. As operações nesse inusitado campo digital têm implicações significativas para a segurança nacional, exigindo uma vigilância contínua e estratégias de defesa robusta.

Para atenuar tais ataques e prevenir incidentes futuros, é essencial que sejam realizadas auditorias de segurança periódicas e testes de penetração para detectar e corrigir vulnerabilidades. Além disso, a implementação de uma validação rigorosa de mensagens e a comunicação clara com o público são vitais para gerenciar e corrigir a disseminação de informações falsas (Centro Simon Wiesenthal, 2023).

Os ataques podem danificar a reputação dos sistemas de alerta, levando a dúvidas sobre sua confiabilidade. Este ponto é crítico, pois a confiança pública e a coesão social são pilares importantes em momentos de adversidade, ficando flagrante que essas ações podem, se bem-sucedida, gerar vítimas fatais. Em cenários de conflito, a desinformação pode ser usada como uma tática para exagerar a eficácia de uma atividade e manipular a percepção pública. Esse uso estratégico torna-se uma ferramenta poderosa na guerra cibernética

contemporânea, reforçando a necessidade de uma resposta coordenada e eficaz para amenizar seus efeitos.

Este capítulo forneceu uma visão detalhada dos principais eventos de guerra cibernética no conflito Israel-Hamas em 2023, destacando a necessidade de uma abordagem integrada e colaborativa para a cibersegurança em tempos de conflito. As diversas táticas utilizadas pelos grupos hacktivistas e as respostas coordenadas demonstram a evolução contínua da guerra e a necessidade de estratégia de defesa integrada para proteger infraestruturas críticas e manter a segurança nacional (Mozelli, 2023). É essencial continuar esta análise para permitir uma compreensão mais ampla das implicações e das estratégias necessárias para enfrentar os desafios contemporâneos.

5 LIÇÕES APRENDIDAS

O estudo da guerra cibernética no contexto do conflito entre Israel e o grupo Hamas revelou uma série de lições e estratégias que podem ser aplicadas para aprimorar a doutrina e a estrutura de defesa cibernética de um Estado e aprimorar a doutrina da Marinha do Brasil. Este capítulo tem como objetivo sintetizar os principais pontos dos capítulos anteriores e oferecer recomendações para uma estrutura resiliente, levando em consideração o desenvolvimento tecnológico, a proteção de infraestruturas críticas, a cooperação interagências e a adaptação a desafios geopolíticos.

5.1 DESENVOLVIMENTO TECNOLÓGICO E INOVAÇÃO

A Base industrial de Defesa (BID) de Israel desempenha um papel de destaque na segurança cibernética do país, composta por startups e indústrias tecnológicas. Desde os anos 2000, Israel tem incentivado o desenvolvimento de tecnologias, posicionando suas empresas na vanguarda global, o que é essencial para a defesa contra investidas no campo digital. A cooperação entre governo, academia e setor privado é um dos fundamentos dessa estratégia, promovendo um ambiente de inovação contínua e adaptabilidade a perigos emergentes.

Além disso, Israel estabeleceu uma rede complexa de instituições de ensino e pesquisa dedicadas à cibersegurança, como o Technion e a Universidade de Tel Aviv, que fornecem uma base sólida de conhecimento e inovação. O estabelecimento do CyberSpark, integra as empresas de tecnologia, *startups* e entidades governamentais. Esse ambiente colaborativo é essencial para a troca de conhecimento e desenvolvimento de novas tecnologias (Embaixada do Brasil em Tel Aviv, 2022).

A infraestrutura de Israel é fundamental para a proteção das redes críticas do país e para a coordenação de respostas a incidentes no espectro digital. A integração de tecnologias avançadas como a inteligência artificial e o aprendizado de máquina permitem identificar padrões anômalos e responder de forma proativa a potenciais ataques (Tabansky, 2015). O modelo de colaboração de Israel é

frequentemente citado como um exemplo de sucesso, onde a rápida troca de informações e recursos entre entidades públicas e privadas permitem uma resposta ágil e eficaz às ameaças cibernéticas (Murphy, 2020).

A Unidade 8200, com um histórico positivo nas ações de inteligência, juntamente com seus veteranos, frequentemente fundam ou se juntam a startups, mantendo a experiência e conhecimento técnico no setor cibernético. Esta manutenção de conhecimento no setor militar e privado cria uma sinergia que impulsiona a inovação e fortalece a postura de segurança do país (Cristiano, 2020). Ficando evidente que essa sistemática se torna renovável e autossuficiente no tange o fomento da BID, gerando emprego e desenvolvendo tecnologia em proveito do país.

A criação INCD em 2016 sublinhou o compromisso de Israel com a defesa no campo digital como um fundamento estratégico. Documentos políticos e programas, como a Iniciativa Cibernética Nacional de 2010, delinearam a visão de Israel para o domínio cibernético, enfatizando a importância da inovação tecnológica e da infraestrutura resiliente para proteger contra ameaças (Allison et al., 2016). Essas mudanças de postura de Israel demonstram o entendimento do real perigo que o ciberespaço pode proporcionar. Tornando incontestável a necessidade da abordagem cibernética se tornar nacional, não se limitando a preocupação das Forças Armadas, uma vez que esse espectro pode atingir todos os indivíduos, seja diretamente ou indiretamente. A criação de um ecossistema de inovação, semelhante ao CyberSpark, pode fomentar a colaboração e o desenvolvimento de tecnologias avançadas para a defesa. “Entendeu que para obter êxito na defesa completa e impenetrável de suas redes, era necessário unir forças. A interdisciplinaridade é algo marcante ao analisar a maneira como esse país divide esforços e investimentos em defesa cibernética.” (Wanderley et al.,2020).

Essa abordagem holística assegura que Israel continue na vanguarda da segurança cibernética, adaptando-se continuamente às novas ameaças e mantendo sua posição de autoridade global no desenvolvimento tecnológico e na inovação. O que torna esse estudo uma parte importante para os Estados que desejam se preparar para os desafios que se avizinham nesse novo campo.

5.2 ATAQUES CIBERNÉTICOS CONTRA INFRAESTRUTURAS CRÍTICAS

Desde 2011, observou-se um aumento significativo no número de ataques digitais contra infraestruturas críticas israelenses e, muitas das vezes coordenados e sofisticados. O país vem otimizando seus recursos na defesa dessas infraestruturas, superando tecnologicamente seus adversários com o apoio da estrutura cibernética. A implementação de sistemas avançados de detecção, prevenção e resposta a incidentes, como o Cyber Dome, materializa a capacidade em manter uma postura defensiva potente.

A resposta de Israel a esses ataques tem sido fortalecer suas defesas cibernéticas através de parcerias público-privadas, programas de pesquisa e desenvolvimento, e iniciativas de cooperação internacional. Empresas privadas desempenham um papel destacado no desenvolvimento de tecnologias avançadas e na proteção das redes do país. Muitas das inovações em cibersegurança emergem de startups apoiadas por incubadoras e aceleradoras, frequentemente em parceria com instituições governamentais e militares (Tabansky, 2015).

Outra perspectiva para enfrentar os novos desafios é a visão de Richard Clarke e Robert Knake no livro Guerra Cibernética: A próxima ameaça à segurança e o que fazer a respeito, onde mencionam “A Estratégia da Tríade Defensiva” como solução para a defesa cibernética dos Estados Unidos.

O primeiro pilar é a proteção do backbone, ou "espinha dorsal" ou "rede de transporte", que é a rede principal responsável pelo tráfego de dados dos clientes na internet. Esta rede controla a infraestrutura central de um sistema mais amplo com alto desempenho. Entre as principais empresas que operam essas redes estão AT&T, Verizon, Level 3, Qwest e Sprint, que possuem extensos sistemas de cabos de fibra ótica que se estendem por todo o país e se conectam a cabos submarinos internacionais. Mais de 90% do tráfego de internet nos Estados Unidos passa por esses cabos, tornando quase impossível acessar qualquer local no país sem utilizar um desses provedores de *backbone*. Portanto, ao proteger esses provedores, está-se garantindo a segurança de grande parte da infraestrutura da internet nos Estados Unidos e em outras partes do ciberespaço. Há inicialmente pontos a serem destacados, como o risco no fato de haver a possibilidade de controle e restrição do

acesso a informações, o que, por exemplo, poderia beneficiar politicamente um governante. E outra análise seria técnica, pois o grande volume de dados que trafegam pela internet demandaria um atrasado na transmissão de dados para que houvesse uma verificação de segurança (Clarke; Knake, 2015).

O segundo pilar é a manutenção de uma rede elétrica segura. Sem energia elétrica, não há acesso ao ciberespaço e a maioria das outras coisas das quais dependemos para de funcionar, ou pelo menos não por muito tempo (Clarke; Knake, 2015). A solução proposta no livro Guerra Cibernética seria garantir que não haja conexão dos geradores às redes de internet. O primeiro passo nessa direção seria a implementação de regulamentos rigorosos exigindo que as companhias elétricas dificultem ao máximo o acesso à rede de controle. Isso significaria eliminar qualquer possibilidade de acesso ao sistema de controle via Internet. Para complicar ainda mais as atividades de um adversário cibernético, seria possível exigir que os sinais de controle enviados aos geradores, transformadores e outros componentes críticos fossem criptografados e autenticados. A criptografia dos sinais garantiria que, mesmo que alguém conseguisse acesso ao sinal para enviar uma instrução a um gerador, não teria o código secreto necessário. Dada a possibilidade de algumas partes da rede ainda serem comprometidas por um hacker de outro país, certas seções-chave deveriam possuir um sistema de comunicação de backup para o envio de sinais de comando e controle, permitindo a possível restauração do serviço. (Clarke; Knake, 2015).

O terceiro pilar da Tríade Defensiva é a própria defesa – o Departamento de Defesa. “Existe pouca chance que um estado-nação realize um grande ataque cibernético contra os Estados Unidos sem tentar paralisar o Departamento de Defesa no processo.” (Clarke; Knake, 2015, p.162).

Dessa forma, verificamos que os Estados em geral estão em alerta e em constante desenvolvimento para se contrapor a esses assombros, invisíveis e extremamente diversificados ataques. Podemos notar que a tríade defensiva sugerida por Clarke e Knake se alinha com os eventos cibernéticos recentes e com as preocupações Israelenses. Seja construindo uma defesa cibernética capaz de se adaptar rapidamente as inovações, estabelecendo um departamento de Defesa com poder suficientemente dissuasório, capacidade de realizar ataques contra Estados

agressores e, com maior destaque, promovendo a união de todas as esferas do Estado em prol da prosperidade de soluções para enfrentar as desafiadoras ameaças do espectro digital. Nesse contexto, podemos concluir que os Estados Unidos da América e Israel são destaques no combate nesse novo campo de batalha invisível e furtivo. E percebemos que, ressalvando as peculiaridades de cada Estado, ambos perseguem a capacidade cibernética adaptativa através de um esforço integrado nacional e claramente seus esforços seguem em evolução, com a fiel meta de integrar todas as esferas de poder do Estado nessa empreitada.

5.3 DESAFIOS GEOPOLÍTICOS E HOSTILIDADES CIBERNÉTICAS

O cenário geopolítico de Israel, cercado por inimigos e enfrentando hostilidades contínuas, incluindo ameaças cibernéticas de grupos como o Hamas, exige uma conduta firme em cibersegurança. A necessidade de se defender contra esses perigos é um fator chave na estratégia de segurança cada vez mais presente na realidade de todos os Estados.

O conflito Israel-Hamas também tem repercussões globais, afetando não apenas a região, mas também países que apoiam Israel. Os ataques cibernéticos têm visado não apenas Israel, mas também nações aliadas.

As forças adversárias, mesmo que sejam relativamente débeis ou constituídas por grupos não estatais, podem contar com apoios ideológicos e de outros estados interessados. Logo, com apenas uma declaração de apoio a um Estado, podemos nos colocar como alvos desses grupos no espectro cibernético. Assim, a guerra cibernética tende a atingir níveis máximos de intensidade. Portanto, é imperativo que estejamos preparados para confrontar os mais avançados e elaborados artefatos mesmo em períodos entre guerras.

Cabe ressaltarmos que as grandes empresas de tecnologia e os Estados tendem a não divulgar suas derrotas no domínio cibernético. Isso ocorre devido à necessidade das empresas não perderem clientes e prestígio, bem como colocar em risco sua existência, e os Estados jamais mencionariam perdas de dados sigilosos ou que foram afetados diretamente no desenvolvimento do país e de sua população, comprometendo, em última análise, sua soberania. Logo, essas preocupações

atingem economicamente os Estados, particularmente na proteção de segredos industriais ou de mercado. Dessa forma, um Estado que ainda não se envolveu em estudar tal área, já está perdendo tempo nessa corrida pela compreensão e influência desse domínio sem limites geográficos.

6 CONSIDERAÇÕES FINAIS

A análise do conflito cibernético entre Israel e Hamas oferece percepções valiosas para a melhoria das estruturas de defesas cibernéticas. Israel compreendeu que, para proteger suas redes com eficácia, era fundamental unir forças. A colaboração interdisciplinar é uma característica marcante na forma como o país organiza e investe na defesa cibernética. Verificamos durante o estudo, que mesmo Israel sendo um dos líderes da guerra cibernética no mundo, sofreu vários ataques cibernéticos, e alguns com relativo sucesso.

A defesa cibernética é uma prioridade para militares, governantes e civis, não apenas por proteger contra as ameaças modernas trazidas pela invenção da internet e sua fácil acessibilidade, mas também por se tornar uma ferramenta crucial para a manutenção da existência do Estado. Incluímos o exemplo dos Estados Unidos da América para reforçar a preocupação de outros Estados no desenvolvimento da guerra cibernética.

O fenômeno da guerra cibernética é envolto em um nível de sigilo governamental tão intenso que faz com que o período da Guerra Fria seja visto como mais claro e compreensível, devido à complexidade intrínseca de controlar artefatos cibernéticos. Armas cibernéticas não podem ser detectadas ou impedidas de maneira convencional, nem podem ser inspecionadas em bases militares. Atualmente, é altamente improvável que os Estados permitam que equipes internacionais de inspetores verifiquem os programas em suas redes de computadores, pois esses programas são projetados para proteger informações confidenciais.

Diante de todo o conteúdo pretérito, como resposta para o problema inicial da pesquisa, concluímos que a estrutura de defesa cibernética de Israel pode servir como arquétipo para outros Estados e de incentivo ao setor privado. A análise revelou que o sistema de Israel, alicerçado em inovação tecnológica, cooperação público-privada, um forte investimento em pesquisa e desenvolvimento e o alistamento da inteligência artificial, se mostra eficaz frente às novas ameaças tecnológicas e se mantendo atualizadas frente a rápida evolução tecnológica. O sucesso do sistema de Guerra Cibernética israelense é evidenciado pela capacidade

do país em adaptar-se rapidamente a riscos emergentes, utilizando tanto estratégias ofensivas quanto defensivas, conforme verificado nos momentos iniciais do conflito recente, onde novos métodos de ataques foram identificados.

Respondendo as demais questões secundárias, a pesquisa apontou a existência de um aumento nas atividades cibernéticas no mês anterior aos ataques, sugerindo uma possível preparação para ações futuras, porém não necessariamente indicando para movimentações terrestres ou qualquer outra ação específica. Após os momentos iniciais do conflito, não se verificou a existência novos métodos de ataque cibernético, ou pelo menos noticiado ou identificado, entretanto se notou que as formas de ataques cibernéticos sofreram mudanças significativas, com uma maior sofisticação e complexidade, refletindo a evolução das ameaças e dos grupos hackers. As estruturas críticas de Israel, por sua vez, foram alvos de maior e mais elaborados número de ataques, demonstrando a importância de uma defesa robusta, em camadas e integradas. Essas conclusões reforçam a premissa de que a abordagem de Israel, caracterizada pela interdisciplinaridade e sinergia entre setores, pode, de fato, ser um modelo a ser seguido por outros Estados em busca de uma defesa cibernética eficaz e resiliente.

Devemos, por fim, salientar que estamos vivenciando a quarta revolução industrial, que vai além de meras mudanças em sistemas e máquinas inteligentes. Com um alcance mais amplo e profundo, novas descobertas estão ocorrendo simultaneamente em diversas áreas do conhecimento. O que distingue este momento dos anteriores é a fusão dessas tecnologias e a interação entre os domínios físico, digital e biológico. A conectividade digital, combinada com a inteligência artificial, está transformando a sociedade de forma profunda. A escala do impacto e a velocidade das mudanças tornam essa transformação única na história.

Portanto, a realidade do campo cibernético exige imediatamente uma canalização de esforços contínua e inovadora. Devemos investir em tecnologias avançadas, formar parcerias estratégicas e desenvolver políticas estruturadas para enfrentar essas furtivas e poderosas ameaças invisíveis. Somente através de um compromisso coletivo e diligente poderemos garantir a segurança, prosperidade e a soberania do Estado.

REFERÊNCIAS

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Engenharia Social**. Guia para a proteção de conhecimentos sensíveis. 2021. Disponível em: <https://www.gov.br/abin/pt-br/institucional/acoes-e-programas/PNPC/boaspraticas/cartilha-engenharia-social-guia-para-protecao-de-conhecimentos-sensiveis>. Acesso em: 20 jun. 2024.

AHUJA, Namrata Biji. How Israel is Planning for Hybrid Wars of the Future with Cyber Dome. **The Week**, 2023. Disponível em: <https://theweek.com/cyber-dome-israel-hybrid-wars>. Acesso em: 20 jun. 2024.

ALLISON, Graham; et al. Deterring Terror: English Translation of the Official Strategy of the Israel Defense Forces. Cambridge, MA: **Belfer Center for Science and International Affairs**, Harvard Kennedy School, 2016. Disponível em: <https://www.belfercenter.org>. Acesso em: 18 jun. 2024.

BUCKLEY, Joseph; CONNOR, Stina. **Israel-Hamas Conflict to Heighten Cyber Espionage and Disruptive Cyber Threats**. Control Risks, 2023.

BYMAN, Daniel; McCALEB, Emma. **Understanding Hamas's and Hezbollah's Uses of Information Technology**. CSIS Briefs, 2023.

CANALTECH. **O que é Trojan?** Disponível em:<https://canaltech.com.br/produtos/O-que-e-trojan/>. Acesso em: 25 mai. 2024.

CHECK POINT SOFTWARE. **What is Wiper Malware?** Disponível em:<https://www.checkpoint.com/pt/cyber-hub/threat-prevention/what-is-malware/what-is-wiper-malware/>. Acesso em: 28 jul. 2024.

CENTRO SIMON WIESENTHAL. The Israel-Hamas War: Crypto Assets Financing Hamas. **ED Snider Social Action Institute**, 2023a. Disponível em: <https://www.wiesenthal.com/assets/pdf/israel-hamas-war_cryptoassetsfinancinghamas-2023.pdf>.Acesso em: 10 mai 2024.

CENTRO SIMON WIESENTHAL. The Use of CYBERTERRORISM in the Israel-Hamas War. **ED Snider Social Action Institute**, 2023b. Disponível em: <https://www.wiesenthal.com/assets/pdf/02_24_hamascyberterrorism_report.pdf>. Acesso em: 10 mai 2024.

CISO Advisor. **Hackers se aliam à guerra entre Israel e Hamas com ciberataques.** 2023a. Disponível em:<https://www.cisoadvisor.com.br/hackers-se-aliam-a-guerra-entre-israel-e-hamas-com-ciberataques/>. Acesso em: 15 fev. 2024.

CISO Advisor. **Ciberataques crescem com expansão da guerra Israel-Hamas. 2023b**. Disponível em:<https://www.cisoadvisor.com.br/ciberataques-crescem-com-intensificacao-da-guerra-israel-hamas/>. Acesso em: 15 fev. 2024.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética**: A próxima ameaça à segurança e o que fazer a respeito (Portuguese Edition). BRASPORT, 2015. Edição do Kindle.

CRISTIANO, Fabio. Israel: **Cyber defense and security as national trademarks of international legitimacy**. In: ROMANIUK, S. N.; MANJIKIAN, M. Routledge Companion to Global Cyber-Security Strategy. Basingstoke: Palgrave Macmillan, 2020.

DEPARTAMENTO DO EXÉRCITO DOS ESTADOS UNIDOS. **FM 3-0**: Operations. Washington, D.C.: Department of the Army, 2022.

DIRETORIA NACIONAL CIBERNÉTICA DE ISRAEL. "**Iron Swords" War in Cyber Sphere**: Insights, Recommendations and Mitigations. Israel, 2024.

DIRETORIA NACIONAL CIBERNÉTICA DE ISRAEL. **Israel National Cyber Security Strategy in Brief.** Israel, 2017.

GONÇALVES, Fernanda Cristina Nanci Izidro. **Ciberdefesa em Perspectiva Comparada: Brasil x Israel**. Unilasalle-RJ/IESP-UERJ, 2020. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xvi_cadn/ciberdefesaa_ema_perspectivaa_comparadaa_brasila_xa_israel.pdf>. Acesso em: 14 mai. 2024.

GORI, Beatrice. **From Kinetic to Cyber Attacks and Back**: the Israeli approach to deterrence in cyberspace and the multi-dimensional threat of Hamas. Center for cyber security and international relations studies, 2022.

HANDLER, S. P. The Cyber Strategy and Operations of Hamas: Green Flags and Green Hats. **Atlantic Council**, 2022. Disponível em: <https://www.bbc.com/portuguese/articles/cv203d23vnpo>. Acesso em: 20 jun. 2024.

HOFFMAN, B. **The Use of Cyberterrorism in the Israel-Hamas War**. CSIS, 2023. Disponível em: <https://www.csis.org/analysis/use-cyberterrorism-israel-hamas-war>. Acesso em: 20 jun. 2024.

KAUR, Gagandeep. Cyberattacks on Israel intensify as the war against Hamas rages. **Check Point**. Disponível em:< https://www.csoonline.com/article/1249135/cyberattacks-on-israel-intensify-as-the-war-against-hamas-rages-check-point.html>. Acesso em: 27 jun. 2024.

KASPERSKY. **Spear Phishing**. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/spear-phishing>. Acesso em: 01 jul. 2024.

KUEHL, D. T. **Cyberspace and cyberpower**. In: KRAMER, F. D.; STARR, S. H.; WENTZ, L. K. (eds). Cyberpower and national security. Washington, DC: National Defense University Press/Potomac Books, 2009.

LEON, Elad. The Israel-Hamas War's Impact on the Cyber Threat Landscape. **CYE Insights**, 2023.

MINISTÉRIO DA DEFESA. **Doutrina Militar de Defesa Cibernética**: MD31-M-07. Brasília: Ministério da Defesa, 2014. Disponível em: [link]. Acesso em: 29 jun. 2024.

MOZELLI, R. **Além de Enfrentar Hamas, Israel Sofre Ataques Cibernéticos**. Olhar Digital, 2023. Disponível em: <https://olhardigital.com.br/2023/10/09/seguranca/alem-de-enfrentar-o-hamas-israel-sofre-com-ataques-ciberneticos/>. Acesso em: 20 jun. 2024.

MUKHERJEE, Shashank. **How Israel plans for hybrid wars of the future with the Cyber Dome**. The Week, 14 out. 2023. Disponível em: <https://www.theweek.in/theweek/cover/2023/10/14/how-israel-plans-for-hybrid-wars-of-the-future-with-the-cyber-dome.html>. Acesso em: 21 jun. 2024.

NISSENBAUM, Dion; RASMUSSEN, Sune Engel; FAUCON, Benoit. With Iranian Help, Hamas Builds 'Made in Gaza' Rockets and Drones to Target Israel. **Wall Street Journal,** 20 maio 2021. Disponível em: <https://www.wsj.com/articles/with-iranian-help-hamas-builds-made-in-gaza-rockets-and-drones-to-target-israel-11621535346>. Acesso em: 20 jun. 2024.

SANDS, Leo; SULIMAN, Adela. **Why is Israel at war with Hamas in Gaza?** A basic explainer. The Washington Post, 2023. Disponível em: https://www.washingtonpost.-com/world/2023/10/17/israel-hamas-war-reason-explained-gaza/. Acesso em: 22 jul. 2024.

SECURITY LEADERS. **Ciberguerra se inicia entre Israel e Palestina com Ataques de Grupos Hacktivistas**, 2023a. Disponível em: <https://securityleaders.com.br/ciberguerra-se-inicia-entre-israel-e-palestina-com-ataques-de-grupos-hacktivistas/>. Acesso em: 20 jun. 2024.

SECURITY LEADERS. **Análise laboratorial indica alta nas atividades cibernéticas contra aliados de Israel,** 2023b. Disponível em: <https://securityleaders.com.br/analise-laboratorial-indica-alta-nas-atividades-ciberneticas-contra-aliados-de-israel/>. Acesso em: 20 jun. 2024.

SHAMAH, David. Qatari Tech Helps Hamas in Tunnels, Rockets: Expert. **The Times of Israel,** 31 jul. 2014. Disponível em: <https://www.timesofisrael.com/qatari-tech-helps-hamas-in-tunnels-rockets-expert/>. Acesso em: 27 jun. 2024.

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

TALEB, Nassim Nicholas. **Antifrágil:** Coisas que se beneficiam com o Caos. Nova edição. Rio de Janeiro: Objetiva, 2020.

TINDALL, **Mason. Beginner's Guide to Cybersecurity**: A Comprehensive Guide to Protecting Yourself from Cyberattacks and Identity Theft in 2021 (p. 12). Edição do Kindle.

WANDERLEY, Ana Beatriz Queiroz; SANTOS, Beatriz Silva Flores dos; BARRETO, Johanna Larrubia; PORTELA, Júlia Rodrigues Clemente; POLIZZO, Luisa Carvalho; OLIVEIRA, Natalia Gonçalves. **Ciberdefesa em Perspectiva Comparada**: Brasil x Israel. Unilasalle-RJ/IESP-UERJ, 2020. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xvi_cadn/ciberdefesaa_ema_perspectivaa_comparadaa_brasila_xa_israel.pdf>. Acesso em: 14 mai. 2024.