A Tríplice Hélice israelense no cenário de cibersegurança

The Israeli triple helix in the cybersecurity scenario

Rev. Bras. Est. Def. v. 9, n. 2, jul./dez. 2022, p. 197–225
DOI: 10.26792/RBED.v9n2.2022.75284
ISSN 2358-3932

ELIEZER DE SOUZA BATISTA JUNIOR
FREDERICO EMANUEL SOUSA NUNES
RÔBER YAMASHITA

INTRODUÇÃO

A formação e a evolução de Israel tornaram esse Estado cercado por inimigos, entre os quais os vizinhos não são os únicos, pois também se somam as hostilidades extrarregionais e principalmente as internas (Israel 2016). Alinhado a essa histórica geopolítica de desafio-resposta (Toynbee 1987, 164–241), o país tem vivenciado variadas ameaças nos domínios aéreo, terrestre, marítimo, espacial e, recentemente, o cibernético.

No início do século XXI, Israel colocou o ciberespaço como foco para desenvolvimento nacional, por meio da resolução 84/b, almejando ser uma das nações mais aprimoradas nesta área. Essa mudança estratégica teve um grande peso para com o atingimento dos objetivos políticos. Com isso, todas as estruturas que pudessem trabalhar com o novo ambiente tiveram a necessidade de se adequar para produzir resultados necessários (Israel 2002). Nesse contexto, a parte de segurança e defesa israelense evoluiu aos patamares de países considerados com tecnologia de ponta.

A Tríplice Hélice possui papel relevante no desenvolvimento de soluções tecnológicas para a segurança cibernética israelense. Portanto, o problema a ser respondido nesse artigo é: diante dos ciberataques às in-

Eliezer de Souza Batista Junior — Doutorando em Ciências Militares (CM) pelo Instituto Meira Mattos. Graduado em CM e Sistemas de Informações. Pós-graduado em Operações Eletrônicas, Operações Cibernéticas e Big Data. Possui mestrado profissional em CM. junhor82@gmail.com.
Frederico Emanuel Sousa Nunes — Mestre em Ciências Militares (CM) pelo Instituto Meira Mattos. Graduado em CM. Pós-graduado em Gestão da Administração Pública. freldsn@gmail.com.
Rôber Yamashita — Doutor (PhD) pela Asia e University (Kuala Lumpur/Malásia). Mestre em Operações Militares. Graduado em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN). Graduado em Administração. Pós-graduado em Guerra Eletrônica. rober_yamashita@yahoo.com.br.

fraestruturas críticas israelenses,[1] as ações de agentes da Tríplice Hélice[2] contribuem para a eficácia da segurança cibernética israelense?[3]

A pesquisa foi limitada à análise de documentos e pesquisas bibliográficas em revistas especializadas sobre esse tema. Nessa área, há limitações para comprovação de autoria de ataques, por conta da existência de robustas estruturas anonimizantes.[4] Assim, foram entendidas como válidas as acusações realizadas pelo Estado israelense.

Ao se estudar variados eventos de ataques cibernéticos a Israel, buscou-se concentrar o trabalho nos ataques direcionados às infraestruturas críticas do país, de modo a melhor delimitar a superfície de análise. Além disso, utilizou-se a técnica da realidade aparente, voltada aos eventos que foram estudados ou divulgados na academia ou na imprensa internacional, ao invés de todos os eventos que ocorreram realmente (incluindo os desconhecidos) (Singer and Friedman 2014). O marco temporal utilizado se inicia em 2009, momento em que, supostamente, houve o primeiro ciberataque manifestado contra uma infraestrutura governamental de Israel (Trend 2012).

O desenvolvimento trouxe como referencial teórico: (1) a teoria dos ataques cibernéticos, a fim de construir base para análise de ciberataques; (2) resposta a incidentes e Tríplice Hélice, a fim de trazer informações que possam subsidiar análises das ações da Tríplice Hélice no cenário de resposta a incidentes. Utilizou-se como base de dados os sites do CSIS e do Hackmageddon para se analisar os eventos ocorridos desde 2009. A análise dos resultados permitiu estabelecer que a Tríplice Hélice israelense apoia sua segurança cibernética.

TEORIA DO ATAQUE CIBERNÉTICO

A maior parte dos incidentes são relacionados a ataques cibernéticos, de forma geral. Os ataques cibernéticos podem ser definidos segundo o conceito a seguir.

> Um ataque de tecnologia da informação no espaço cibernético direcionado contra um ou vários outros sistemas de tecnologia da informação que objetivam dano na segurança da informação (confidencialidade, integridade e disponibilidade) que podem ser comprometidos individual ou coletivamente (FAGA 2017, 5).

Zhuang (2015) elaborou a teoria do ataque cibernético aumentando o escopo de parâmetros que existem no *Moving Target Defense* (MTD). O modelo distingue um ataque cibernético em vários subconjuntos: alvo,

atacante, ataque e exploração. As seções a seguir definirão os três primeiros subconjuntos. A exploração será descrita na seção da base de dados.

POSSÍVEIS ATACANTES

Atualmente, Israel não é reconhecido como Estado por 36 países (Israel 2016). A Tabela 1 mostra todos os países que não possuem ou romperam relações com Israel em algum momento.

Tabela 1
Rompimento de Relações Exteriores

País	Ano de rompimento
Afeganistão	(1)
Arábia Saudita	(1)
Argélia	(1)
Barein	(1)
Bangladesh	(1)
Butão	(1)
Brunei	(1)
Cuba	1973
Comores	(1)
Coreia do Norte	(1)
Djibouti	(1)
Etiópia	(1)
Iêmen	(1)
Indonésia	(1)
Irã	1979
Iraque	(1)
Kuwait	(1)
Líbano	(1)
Líbia	(1)
Malásia	(1)
Mali	1973
Mauritânia	2010
Níger	1973
Omã	2000
Paquistão	(1)
Catar	2000
Síria	(1)
Somália	(1)
Sudão	(1)
Tunísia	2000
Venezuela	2009

Obs (1): Países que nunca reconheceram Israel.
Fonte: Israel 2016.

A implantação do Estado de Israel fez a Palestina perder grande parte do seu território e legou aos israelenses um país com várias instabilidades relacionadas aos palestinos. Fruto desses tensionamentos, várias reuniões foram realizadas com a intenção de apaziguar o conflito, culminando com os acordos de paz de Oslo em 1993 e 1995. Há dois territórios administrados pela Autoridade Palestina com graus diferenciados: Cisjordânia e Faixa de Gaza (ONU 1995). Sob tal situação, verificou-se o surgimento de grupos terroristas internamente, com o Al-Fatah, Jihad Islâmica e Hamas, bem como inimigos terroristas extraterritoriais, como Estado Islâmico (ISIS ou Daesh), Hizbollah e Al-Qaeda (Marteu 2018).

Verificam-se variados inimigos de Israel, com o intuito de mostrar quais grupos podem ser considerados ameaças no espaço cibernético.

Alvo

As Infraestruturas críticas são instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, interrompidos ou destruídos, provocarão sérios impactos socioeconômicos (EUA 2013). As infraestruturas críticas informacionais utilizam o mesmo conceito, mas adaptado à utilização no espaço cibernético. São alvos potenciais para ameaças cibernéticas, pois causam grandes problemas para nações, trazendo efeitos necessários à conquista de objetivos previamente definidos.

A resolução 3.611 do governo israelense adotou recomendações na intenção de melhorar a proteção das infraestruturas críticas nacionais para a vida cotidiana em Israel e fortalecê-las tanto quanto possível, podendo valer-se de contra-ataques cibernéticos. Enquanto isso, promove o *status* de Israel como um centro para o desenvolvimento de Tecnologia da Informação e Comunicação, por meio da cooperação entre academia, indústria, ministérios e organizações de segurança (Israel 2011).

Ambiente do ataque (ciberespaço)

O ciberespaço[5] se tornou um domínio do poder (NYE 2010, 2) e passou a ser mais que assunto técnico nas relações interestatais. Carr (1981) abordou que relações corriqueiras entre Estados (como serviços postais ou transportes) são classificadas como "não políticas" ou "técnicas". Entretanto, caso impliquem relações de poder, a questão rapidamente se torna "assunto político", somando-se ainda à atuação de ONGs, crime organizado e terroristas, com capacidade de interferir no campo de forças geopolítico.

O poder cibernético é caracterizado como "capacidade de usar o ciberespaço para criar vantagens e influenciar eventos em outros ambientes operacionais e nos instrumentos do poder" (NYE 2010, 4). Segundo Segal (2016), para que essas vantagens e influências sejam atingidas, necessita-se do controle de certas formas de ação por parte do Estado. Tais ações são denominadas de "fontes do poder cibernético", sendo quatro seus principais componentes:

- Economias tecnologicamente avançadas: necessidade de as empresas nacionais dominarem as Tecnologias da Informação e Comunicações (TIC);
- Capacidade do governo trabalhar com o setor privado: o domínio sobre o tema cibernética ultrapassa o setor público;
- Ganância necessária: agências militares e de inteligência têm que ser aventureiras e inventivas para atuar com liberdade no ciberespaço; e
- Narrativa atraente: embasada em situações de influência (Segal 2016, 18–23).

Para Segal (2016), Israel é uma potência cibernética, não podendo ser considerado superpotência por não possuir volume adequado de tecnologias próprias (Segal 2016, 20).

RESPOSTA A INCIDENTES

A fim de dar base teórica às ações de agentes da Tríplice Hélice, a presente seção focará na resposta a incidentes. A resposta a incidentes de cibersegurança pode ser conceituada como o processo de resposta a eventos que ameaçam a segurança de ativos informatizados (Ahmad et al. 2019). Para tanto, existem fases para se responder a um incidente: preparação, detecção, identificação, contenção, erradicação, recuperação, investigação (forense), melhoria e acompanhamento (Thompson 2010, 87–135).

A primeira camada de proteção está dentro da própria empresa ou órgão afetado. Por meio de ferramentas informatizadas, as equipes de tratamento de incidentes tentam realizar a resiliência cibernética frente aos ataques perpetrados. Em alguns países, como Israel, agentes governamentais serão considerados uma outra camada de proteção para serem utilizados em momentos em que as outras camadas não conseguirem a eficácia necessária (Clarck and Knake 2011, 131–45). Em Israel, a Tríplice Hélice faz parte dessa camada.

A Tríplice Hélice é um conceito desenvolvido para uma dinâmica de inovação, havendo colaboração constante entre as esferas públicas, privadas e acadê-

micas. O modelo vincula as três partes, necessitando de recursos necessários para formação e operacionalização a partir das condições locais (Etzokowitz et al. 2008). Dessa forma, serão resumidas as três hélices de Israel.

Governo

O governo atua como condução da inovação, em termos de facilitá-la, principalmente patrocinando iniciativas. Além disso, possui o papel regulatório do mercado, tendo o cuidado para não sufocar pesquisas por meio de tributação (Driori et al. 2013, 12).

No caso da cibernética, o governo atua com suas unidades operacionais para fazer frente às ameaças que surgem. Os principais órgãos que possuem unidades de cibernética em Israel são: o Ministério da Defesa, o Ministério da Segurança Pública e o Escritório do Primeiro Ministro.

No Ministério da Defesa, há duas vertentes: (1) as IDF,[6] que são as Forças Armadas Israelenses; e (2) o braço industrial. Dentro das IDF, há duas divisões: (1) o C4I[7] Corps é uma unidade do Exército Israelense responsável pelas operações defensivas cibernéticas, que abarcam teleprocessamento e comunicações; e (2) o AMAN[8] que é responsável pelas operações de inteligência cibernética. O braço operacional do AMAN é a unidade 8200, responsável pela condução de ações militares no ciberespaço. No braço industrial, a Base Industrial de Israel possui dois segmentos: (1) a Sibat, que é o órgão que trata sobre produtos de defesa israelenses; e (2) a Mafat que trata sobre produtos de defesa com alto grau de sigilo (Baezner and Cordey 2019, 27).

O Escritório do Primeiro-Ministro se subdivide: (1) no ISA,[9] que é responsável pela parte de contraterrorismo e contraespionagem cibernética; e (2) no NCD,[10] que responde por todos os aspectos de defesa cibernética na esfera civil. O NCD possui o CERT-IL que é responsável pelo tratamento de incidentes (Baezner and Cordey 2019, 27).

No Ministério da Segurança Pública, há a unidade Lahave 433 da Polícia de Israel, que é responsável pelos crimes cibernéticos contra a população. Esta também trabalha com forense (Baezner and Cordey 2019, 27).

Academia

A academia (ou universidade) foi incumbida de criar conhecimento, por meio da aprendizagem e investigação. Com a Era da Informação, o conhecimento aumentou o seu valor agregado. Dessa forma, no cenário israelense, a busca por inovação foi aumentada por meio de disponibilização de pessoas capacitadas, resultados de pesquisas e repasse de conhecimento

para a indústria. A universidade israelense se envolveu cada vez mais na formação de empresas, já que muitas tecnologias são baseadas em pesquisas acadêmicas (Driori et al. 2013).

Alguns dados colaboram para a boa performance acadêmica israelense: 46% da população adulta possui ensino universitário; grandes taxas de publicações científicas, posições das universidades em *ranking* mundial e patentes de produções universitárias (Driori et al, 2013).

Há de se ressaltar a importância com a qual o governo percebe a academia. Para tanto, incentiva programas como o de transferência de tecnologia para empresas, propriedade intelectual, colaboração com indústrias e orientação de pesquisa e inovação (*Magnet Program*) (Berger 2013, 84–8). Segundo o *Global Innovation Index* (2021), Israel está posicionado na 15ª posição, sendo considerado líder na região do norte da África e oeste da Ásia (Wipo 2021, 4).

As universidades israelenses possuem papel fundamental em termos de defesa e securitização. Para tanto, são capazes de desenvolver sistemas que auxiliem as IDF em combate. Alguns exemplos são a Universidade de Tel Aviv, Universidade de Haifa e Universidade Hebraica de Jerusalém (Berger 2013, 79–81).

A academia Israelense, dentro da Teoria da Tripla Hélice, contribui com a indústria de defesa nacional, particularmente no setor cibernético. O bom posicionamento no *ranking* mundial de produção científica, bem como das patentes de produção universitária, são indicativos que transbordam para a indústria e beneficiam o governo.

Assim, a capacidade de Israel de integrar pesquisas universitárias às necessidades reais da indústria maximizam os resultados. O território geográfico limitado e grandes concentrações urbanas favorecem a aproximação entre indústria e academia, que trabalham com maior sinergia. O enfrentamento de ameaças cibernéticas com maior frequência cria em ambos (indústria e academia) a demanda por pesquisa e desenvolvimento tecnológico nessa área (Berger 2013).

Base industrial de defesa israelense

A BID[11] israelense já detinha, no início do século XXI, peso de 7,5% nas exportações nacionais (Markownski, Hall, and Wylie 2010). O país busca uma inserção internacional com forte participação de produtos de alta tecnologia, sendo um dos líderes globais em *startups*[12] tecnológicas. Tal situação concentra na BID um complexo de empresas cujos ativos se baseiam em conhecimento e inovação, compartilhando alta dependência de proteção da propriedade intelectual, com destaque para o ciberespaço (Argaman and Siboni 2015).

A especialização da BID israelense e a melhoria dos Prode[13] colocou vários destes no estado da arte de suas categorias (Sadeh 2004). Em paralelo, para promoção da produção industrial de defesa, Israel (2020a) incorporou à estrutura de seu Ministério da Defesa a Diretoria Internacional de Cooperação em Defesa (Sibat),[14] a Diretoria de Pesquisa e Desenvolvimento em Defesa (DDR & D[15]) e o Departamento de Produção e Compras (DOPP[16]) (Israel 2020b), agências que buscam a cooperação global e a prospecção de novos mercados para os Prode como os listados na Figura 1:

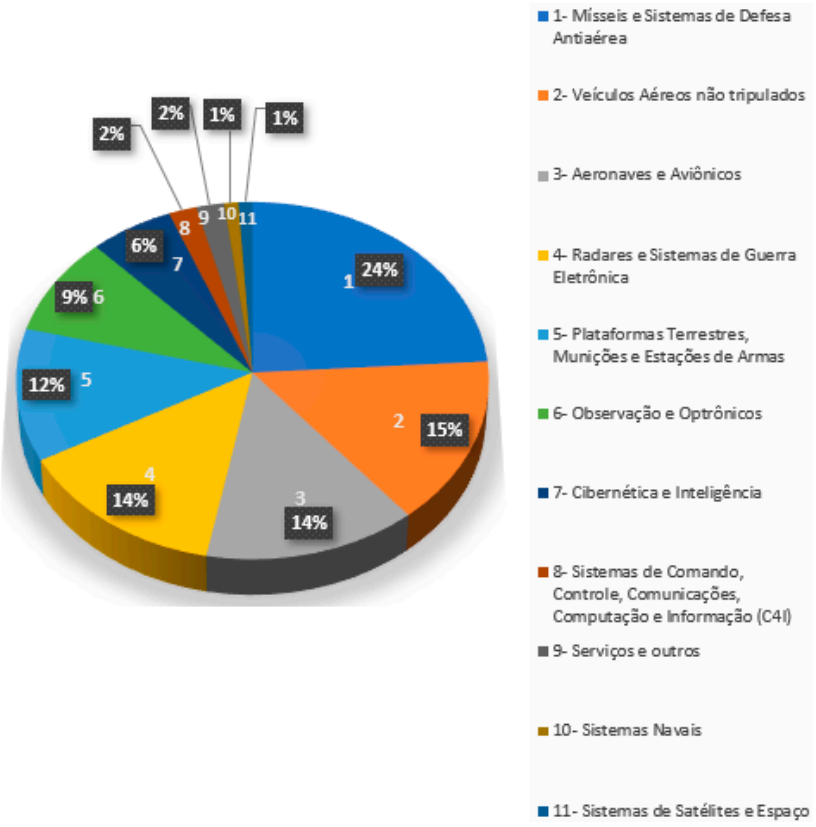


Figura 1 — Principais Prode israelenses para exportação em 2018.
Fonte: dos autores, adaptado de Sibat/Ministério da Defesa (Israel 2020a).

No campo militar, Israel aumentou, no início do século XXI, os gastos com segurança interna, contraterrorismo e guerra assimétrica, assimilando que as ameaças indefinidas e sem fronteiras não seriam derrotadas com

doutrina militar intensiva em mão de obra, plataformas militares pesadas e previsíveis (Sadeh 2004).

O maior financiador das indústrias de defesa israelenses é o próprio governo, que estimula a produção por meio da ciência e incentivos financeiros. Sabe-se que existe uma aproximação histórica entre EUA e Israel para desenvolvimento militar (EUA 2021) e que tem representado papel importante no desenvolvimento de Prode. Com os bons resultados, Israel tem conseguido exportar grande parte dos produtos de defesa a países no mundo inteiro. Em 2019, o país exportou 7,2 bilhões de dólares em equipamentos militares, o que o credenciou a estar entre os dez maiores exportadores. Os principais mercados são, respectivamente: Ásia-Pacífico (41%), Europa (26%), América do Norte (25%), África e América Latina (ambos com cerca de 4%) (Israel 2020).

A efetividade desse perfil de financiamento é questionada internamente, o que fica materializado na tensão surgida entre os papéis econômico e estratégico dessa indústria de defesa. Na Figura 2, pode-se observar a participação do gasto de defesa no PIB, deixando nítido o esforço relativo de cada país, sendo as demais reconhecidas potências militares.

Apesar das pressões por privatizações e maximização dos lucros e da concorrência internacional, as principais empresas ainda são públicas, caso de Elbit e Rafael. Como principais justificativas para esse equilíbrio pesar mais em prol da segurança do Estado, citam-se os boicotes internacionais e a performance do setor civil do país estar mais vocacionada como motor de inovação do que ao financiamento (Faglin 2018).

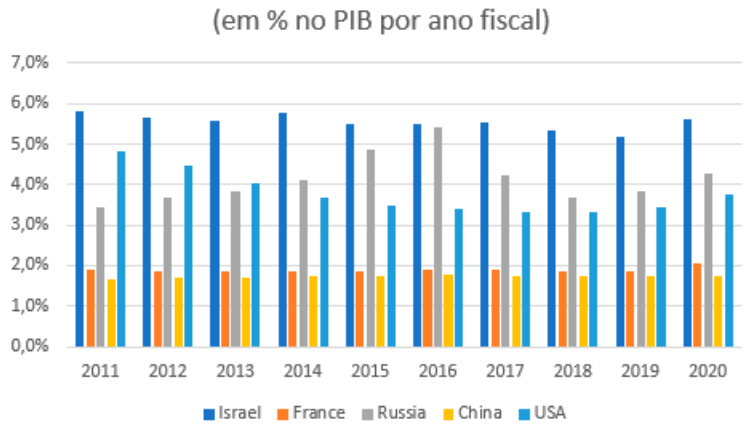


Figura 2 — Porcentagem de participação do gasto em defesa no PIB.
Fonte: dos autores, adaptado de Sipri (2021).

Os desafios à segurança que circundam Israel naturalmente pressionam a demanda para sua BID. As IDF têm se utilizado de soluções tecnológicas para o combate convencional e no amplo espectro (Sadeh 2004) e é justamente na interação entre estas e o sistema de inovação em defesa que o país vem obtendo vantagens competitivas: a estruturação do serviço militar, por exemplo, otimiza os recursos humanos especializados, permitindo que, muitas vezes, o desenvolvedor preste ou tenha prestado serviço em uma unidade combatente (Moran 2008). Observa-se tal prática em unidades de elite como a 8200, componente operacional do sistema de segurança cibernética (Argaman and Siboni 2015).

BASE DE DADOS

A base de dados deste projeto utilizou as informações contidas no sítio do CSIS (2021) e do Hackmageddon (2021).[17] Há de se destacar o enfoque que o CSIS dá aos eventos, classificando-os como "significativos". A metodologia obedeceu aos seguintes passos:

1) Realizou-se o *download* da base de dados do CSIS (2021);
2) Realizou-se o *download* da base de dados do Hackmageddon (2021);
3) Dados repetidos foram eliminados;
4) Dados referentes a ataques ofensivos de Israel foram desconsiderados;
5) Completou-se os dados da Tabela 2 com periódicos especializados no tema cibernética ou reportagens jornalísticas, nesta ordem de prioridade.

A Tabela 2 mostra o resultado da aplicação dos passos acima e relaciona os eventos cibernéticos significativos, informando o ano da ocorrência; os supostos responsáveis pelo ataque (atacante); a estrutura direcionada (alvo); a descrição sumária (ataque); a posição de Israel (exploração); e se houve retaliação. Tais domínios caracterizam os ataques cibernéticos às infraestruturas críticas de Israel e pode-se verificar que caracterizam os quatro subconjuntos da teoria do ataque cibernético.

Tabela 2
Ciberataques desde 2009

Evento	Ano	Descrição	Alvo	Responsável	Posição	Retaliação
01	Jan. 2009	Hackers atacaram a infraestrutura de Internet de Israel durante a ofensiva militar de janeiro de 2009 na Faixa de Gaza.	Infraestruturas de Internet	Supostamente, Hamas ou Hezbollah e outras instituições árabes	Confirmou	Sim. Ataque a *websites* palestinos (1)
02	2011	Grupo Anonimous indisponibilizou sítios de estruturas de defesa israelenses por 48 horas.	Sítio do Ministério da Defesa	Grupo Anonimous	Não se posicionou	Não (2)
03	Entre 2011 e 2012	Hackers chineses conseguiram acesso ao sistema antimísseis israelense.	Sistema de defesa antimísseis e anti-foguetes	Grupo ligado ao Exército de Libertação Popular da China	Confirmado	Não (3)
04	2012	Bolsa de Valores israelense e companhia aérea El Al ficaram indisponíveis.	Bolsa de Valores de Israel	Grupo 0xOmar e grupo Nightmare (árabes)	Não se posicionou	Ameaças governamentais e o grupo IDF Team (não estatal) indisponibilizou a bolsa de valores da Arábia Saudita e dos Emirados Árabes Unidos (4)

Evento	Ano	Descrição	Alvo	Responsável	Posição	Retaliação
05	Jul. 2012	Um *trojan* "Mahdi" realizou a coleta de dados em vários setores em todo o Oriente Médio e além, predominantemente em Israel e no Irã.	Agências do governo e academia	Supostamente grupo iraniano	Não se posicionou	Não (5)
06	Maio 2013	As autoridades israelenses relatam uma tentativa fracassada de comprometer o sistema hídrico.	Abastecimento de água para a cidade de Haifa	Grupo Exército Eletrônico Sírio	Confirmado, mas o Presidente do Conselho Nacional de P&D negou o sucesso do ataque	Não (6)
07	2016	Hacker (em colaboração à Jihad Islâmica) coletou dados sobre sistema de defesa israelense.	Movimentação de *drones* e policiais	Majd Oweida	Confirmado pela corte de Beershaba	Prisão e condenação do hacker a 9 anos de prisão (7)
08	2016	Um *ransomware* atacou o setor elétrico de Israel, usando *e-mail* malicioso (*phishing*).	Autoridade Elétrica de Israel	Provável de origem da Síria	Confirmado pelo ministro da infraestrutura, energia e água	Não (8)
09	Jan. 2016	Snowden revelou uma operação de aliados para obter acesso às imagens dos *drones* de vigilância de Israel.	Sistemas de defesa	Estados Unidos e Reino Unido	Não se posicionou	Não (9)

Evento	Ano	Descrição	Alvo	Responsável	Posição	Retaliação
10	Abr. 2017	Israel anunciou que havia se defendido de uma campanha de ataque cibernético iraniano contra 120 alvos.	Empresas do governo, alta tecnologia, hospitais e escolas	Possivelmente grupos palestinos	Confirmado pela autoridade israelense de Defesa Cibernética	Não (10)
11	Maio 2017	Campanha de *hackers* tendo como alvos várias empresas.	Fornecedores de TI israelenses, instituições financeiras e correios nacionais	Hackers ligados ao Irã (Grupo OilRig APT)	Confirmado	Não (11)
12	Jul. 2017	Pesquisadores de segurança revelaram uso de ataques de *phishing* para atingir instituições governamentais, empresas de defesa, empresas de TI e muito mais em Israel, Arábia Saudita, EUA, Alemanha, Jordânia e Turquia.	Infraestruturas de defesa, governo e empresas de TI	Grupo de espionagem cibernética ligado ao Irã, ativo desde 2013	Confirmado, mas negou a efetividade	Não (12)
13	2018	Hamas realiza campanha contra militares das IDF, fazendo-os instalar softwares maliciosos.	Ministério da Defesa	Hamas	Confirmado pelas IDF e ISA	Não (13)
14	Mar. 2019	Irã invadiu o celular do ex-chefe das IDF (Benny Gantz) antes das eleições de abril de Israel.	Líder da oposição israelense	Serviço de inteligência do Irã	Confirmado por Benny Gantz	Não (14)
15	Mar. 2019	*Hackers* chineses tinham como alvo empresas de defesa israelenses que tinham conexões com os militares dos EUA.	Setor de Defesa	Hackers chineses (Naikon Group)	Confirmado	Não (15)

Evento	Ano	Descrição	Alvo	Responsável	Posição	Retaliação
16	Maio 2019	Hamas tenta, sem sucesso, hackear alvos israelenses.	Não informado	Hamas	Confirmado pelo Comandante da Divisão de Cibernética das IDF	As Forças de Defesa israelenses lançaram um ataque aéreo (16)
17	Abr. 2020	Hackers tentaram hackear o sistema hídrico, sem sucesso.	Sistemas de comando e controle de estações de tratamento de água, estações de bombeamento e esgoto em Israel	Suspeitas de relação com o Irã	Confirmado pelo chefe de cibernética israelense	Ataque ao porto de Shahid Rajee do Irã, indisponibilizando parte do sistema informatizado
18	Jul. 2020	Israel anunciou que dois ataques cibernéticos foram realizados contra a infraestrutura hídrica israelense, embora nenhum deles tenha sido bem sucedido.	Sistema de tubulações de água agrícola da Galileia e do centro do país	Não conhecido	Confirmado pela autoridade hídrica, mas sem danos	Não (17)
19	Ago. 2020	O Ministério da Defesa israelense anunciou que defendeu-se com sucesso um ataque cibernético contra fabricantes de defesa israelenses, lançado por um suposto grupo de hackers norte-coreano.	Indústrias de Defesa	Grupo Lazarus (supostamente da inteligência da Coreia do Norte)	Confirmado pelas IDF	Não (18)

Fonte: dos autores, baseado em CSIS (2021) e Hackmageddon (2021). Em complemento: 1. ProjectGoose (2009); 2. Kalman (2011); 3. Cohen (2015) e Mitigate Cyber (2014); 4. Williamson (2012); 5. Seculert (2012); 6. Ralph (2013); 7. Reuters (2016); 8. Storm (2016); 9. *The Intercept* (2016); 10. Israel (2017); 11. Paganini (2017a); 12. Paganini (2017b); 13. Gross (2018); 14. Horovitz (2019); 15. *Times of Israel* (2020a); 16. Chopsey (2019); 17. *Times of Israel* (2020b); 18. Ayyub (2020).

A Tabela 3 relaciona os eventos com participação da Tríplice Hélice, elencando o número do evento descrito na Tabela 2; o participante da Tríplice Hélice; e a descrição da ação de resposta ao incidente. Verifica-se que esse quadro caracteriza a "ação dos agentes da Tríplice Hélice", com os subsídios elencados por meio da teoria da resposta a incidentes e da Tríplice Hélice.

Tabela 3
Relacionamento com a Tríplice Hélice

Evento	Participante da Tríplice Hélice	Ação
01	Estudantes de várias faculdades recrutados pelo IDF	Criaram uma "*botnet* voluntária" para responder ao ataque
02	6Scan	A *startup* realizou auditoria (análise forense) e constatou que o problema estava no nível hardware e não software
03	Israel Aerospace Industries (IAI) e Rafael Advanced Defense Systems com a colaboração da CyberESI	Empresa CyberESI (parceira da IAI e Rafael) descobriu sobre o escape de dados por meio de logs
04	Não há registros de participação da Tríplice Hélice israelense de cibernética neste evento	
05	Seculert (Israelense) em conjunto com a Karpersky	Descoberta da atividade maliciosa
06	Faculdade Technion-Israel Institute of Technology	Melhoria de medidas protetivas
	Grupo Mekorot	Recuperação
07	Shin Bet e empresas relacionadas (Mafat)	Identificação do ataque
08	Secretaria Nacional de Cibernética Israelense	Identificação do ataque massivo
09	Não há registros de participação da Tríplice Hélice israelense de cibernética neste evento	
10	Autoridade Israelense de Defesa Cibernética	Tratamento de incidentes
11	Clearsky	Tratamento de incidentes
12	Clearsky	Identificação da ameaça
13	IDF e Clearsky	Tratamento de incidentes
14	Shin Bet	Descoberta
15	Check Point Software Technologies	Descoberta e recuperação

Evento	Participante da Tríplice Hélice	Ação
16	Esforço conjunto de empresas civis e militares	Localização do alvo
17	Diretório de Cibernética Nacional e empresas parceiras (como Claroty)	Tratamento de incidente e análise forense
18	Autoridade hídrica e empresas parceiras	Tratamento de incidentes
19	IDF	Tratamento de incidentes

Fonte: dos autores, baseado nos mesmos autores da Tabela 2.

ANÁLISE DOS RESULTADOS

A base de dados se baseou em 19 eventos significativos que foram direcionados às infraestruturas críticas. Os ataques mostrados corroboram o cenário neorrealista apresentado por Carr (1981), que enfatiza os Estados, mas não exclui os atores não estatais.

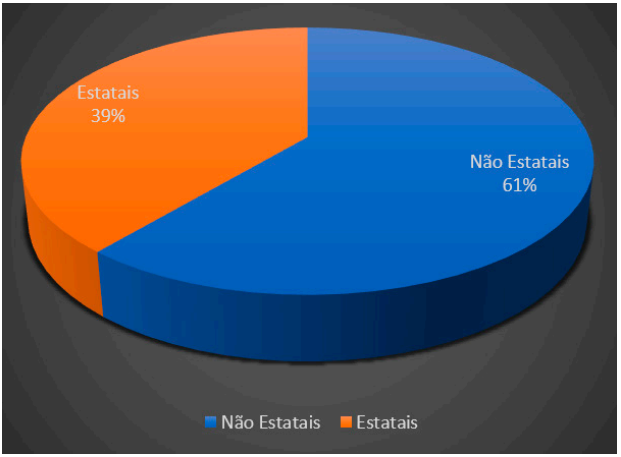


Figura 3 — Ataques estatais e não estatais direcionados a Israel.
Fonte: dos autores, baseado na Tabela 2.

Em termos de inimigos terroristas, verifica-se que a maior ameaça não estatal a Israel é o Hamas. Sob o aspecto estatal, destaca-se o Irã, conforme mostrado na Figura 4, a seguir.

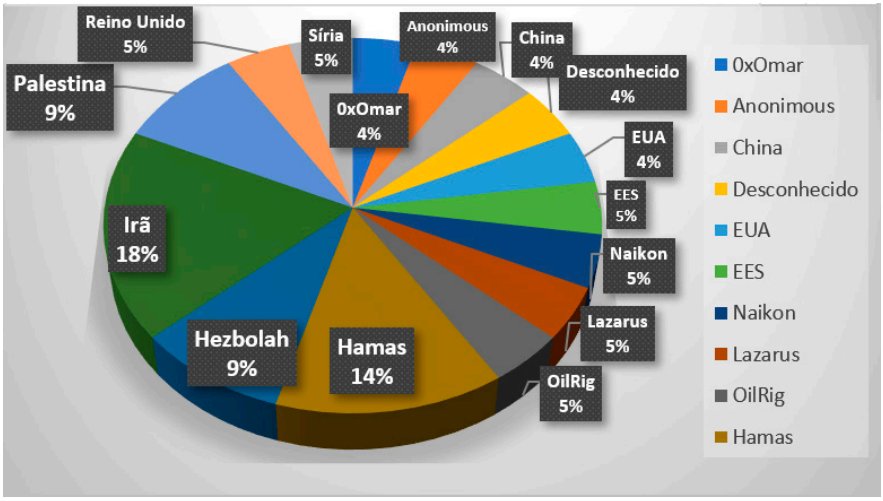


Figura 4 — Principais fontes de ataques cibernéticos.
Fonte: dos autores, baseado na Tabela 2.

As principais origens de ataques cibernético a Israel provêm da Palestina e do Irã, conforme mostra a Figura 5.

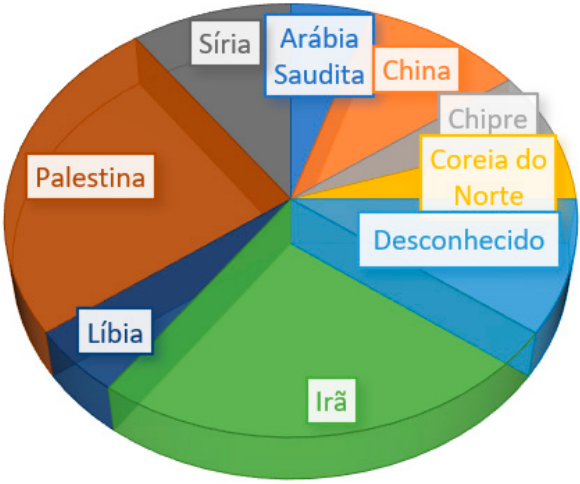
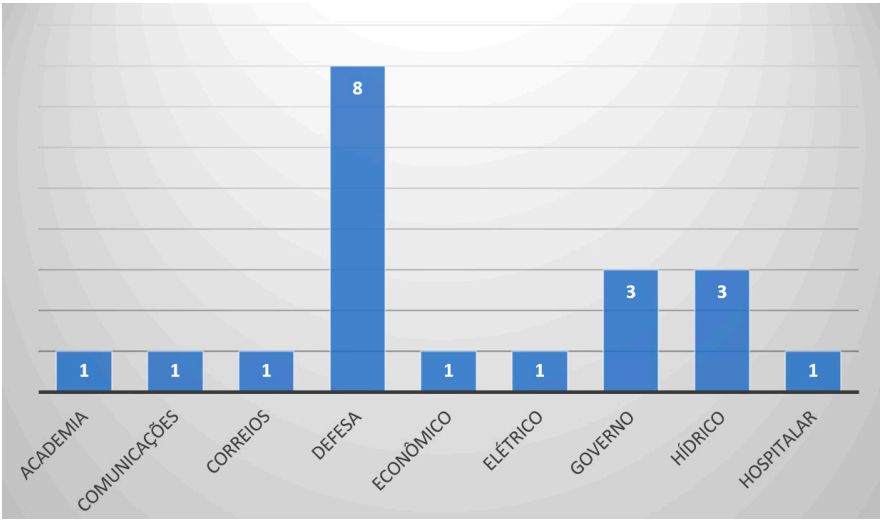


Figura 5 — Principais origens de ataques cibernéticos.
Fonte: dos autores, baseado na Tabela 2.

Tais apontamentos corroboram a análise dos possíveis atacantes, apontada na Seção "Possíveis atacantes".

O nível de complexidade utilizado nos ataques pelas ameaças anteriormente explanadas mostra que os *malwares* utilizados tendem a se tornar mais perigosos. Verificou-se que, no início, utilizavam-se táticas de indisponibilização de sítios, passando por desconfiguração dos mesmos, até atingir o controle (mesmo que temporário) de sistemas (Tabela 2).

Os principais alvos dos ataques direcionados às infraestruturas são abordadas conforme mostrado na Figura 6, a seguir.



Obs: O evento 5 possui atuação em "governo" e "academia" e, com isso, houve a contagem de um para cada, totalizando 20 eventos para esse gráfico, em específico.
Figura 6 — Principais alvos dos ataques cibernéticos.
Fonte: dos autores, baseado na Tabela 2.

De acordo com a Figura 6, as infraestruturas de defesa são os principais alvos, seguidos da distribuição de água, pois o atingimento deste alvo impacta consideravelmente a população. Governo também está no mesmo patamar de importância, o que justifica a campanha de operações de informação. Em menor grau de ataques, na parte hospitalar, Israel vivenciou ameaça atual recorrente no mundo: ataques de *ramsonware*[18] e tentativa de roubos de dados de pesquisas relacionadas ao coronavírus (Press 2018). Alvos relacionados à energia justificam-se pelos reflexos para a defesa nacional e, por fim, no campo econômico, os *hackers* tentaram invadir estruturas que poderiam causar grande impacto, como a Bolsa de Valores.

Quanto ao tempo, verificaram-se comportamentos estatais distintos. A Figura 7, a seguir, mostra as respostas dadas aos eventos, classificando-as em: ausência, ameaça e retaliação.

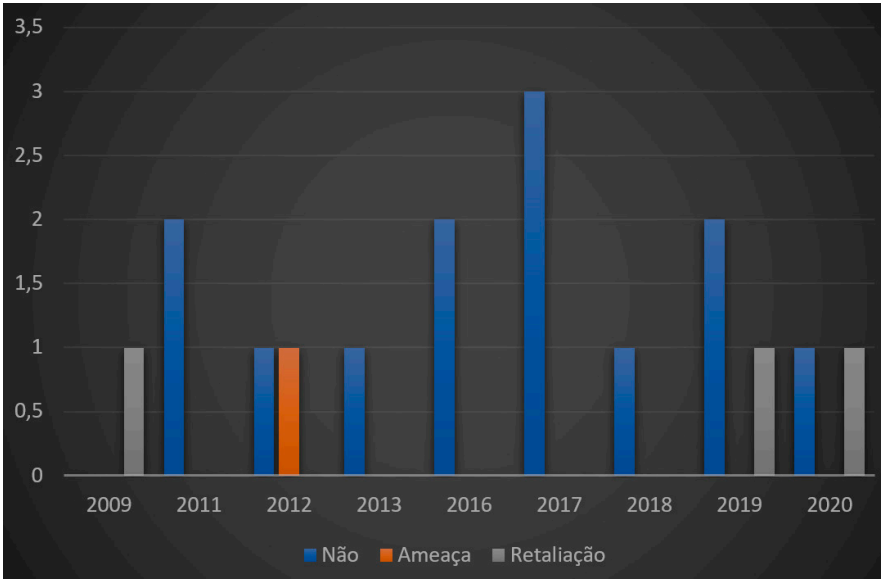


Figura 7 — Comportamento de Israel perante os ataques cibernéticos sofridos.
Fonte: dos autores, baseado na Tabela 3.

A Figura 7 mostra que a postura prioritária de Israel foi o de não responder publicamente aos ataques recebidos. Verificou-se uma postura defensiva no tocante aos ataques proveniente de *hackers* e de estruturas nacionalistas. Há de se ressaltar que essa postura foi evidenciada no momento da descoberta do ataque. Há muita dificuldade de se afirmar que um ataque cibernético realizado por Israel próximo na linha do tempo teve relação com um ataque recebido, se a narrativa implementada pela autoridade que publicitou o evento não deixou claro a sua intenção de ameaçar ou realizar uma contraofensiva.

A partir de 2019, Israel adotou nítida postura contraofensiva. Os ataques recebidos foram respondidos com outros ataques no espaço cibernético ou físico. O país foi, inclusive, o pioneiro ao adotar postura de ataque cinético para contrapor ataque cibernético, atingindo um centro de controle de operações cibernéticas do Hamas. Da bibliografia pesquisada, não há relatos anteriores de tal situação. Em outro evento, o país indisponibilizou a operacionalidade de um porto no Irã, gerando nítidos impactos econômicos.

Quanto ao tópico participação da Tríplice Hélice frente aos ataques cibernéticos, verificou-se que a grande disponibilidade de órgãos governamentais, universidades e empresas de tecnologia possibilita a utilização de diversos produtos e/ou serviços voltados à atividade de segurança cibernética. A Tríplice Hélice ajudou Israel a diversificar seu comportamento, conforme mostrado na Figura 8.

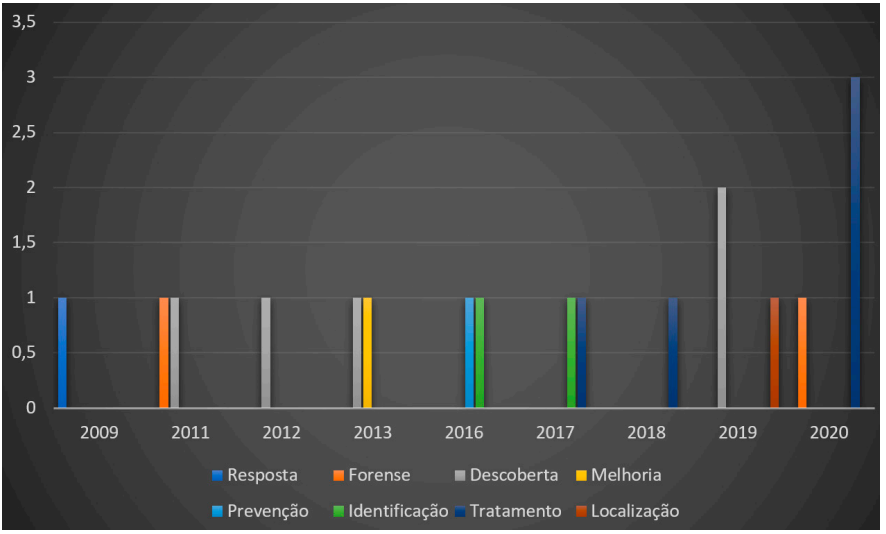


Figura 8 — Comportamento de Israel perante os ataques cibernéticos sofridos.
Fonte: dos autores, baseados nas Tabelas 2 e 3.

O auxílio proporcionado pela Tríplice Hélice no tratamento de incidentes foi notório. Em quase todos os eventos, houve ente governamental, universidade, empresa ou Prode auxiliando as infraestruturas israelenses a mitigar os efeitos negativos das ameaças. Essa situação caracteriza a interação civil-militar na defesa cibernética de Israel, corroborando o que já é verificável na própria estrutura de seu Ministério da Defesa.

Outro ponto é relacionado à prevenção. Apenas um dos eventos necessitou de medidas drásticas, no caso do emprego de atuador cinético (míssil) para destruir um centro cibernético do Hamas. Na maioria das outras situações, os ataques foram defendidos pelos sistemas protetivos, neutralizando as ameaças ou mitigando seus efeitos.

Mesmo sendo uma potência cibernética (Segal 2016), sistemas israelenses foram focos de espionagem de fontes estatais, como China (evento 2 da Tabela 2), EUA e Reino Unido (evento 9 da Tabela 2), sendo esses

dois últimos reconhecidos como aliados. Tal situação mostra que, mesmo havendo os melhores recursos tecnológicos, ainda assim o ambiente é permissivo a intrusões.

Os dados mostram eficácia israelense frente aos ataques recebidos, bem como participação da Tríplice Hélice em eventos relevantes no ciberespaço. Dos 19 eventos mostrados, somente em dois não se encontraram relacionamentos com a Tríplice Hélice.

Uma limitação da pesquisa se referiu à não obtenção de dados das operações de inteligência, o que já foi anteriormente mapeado como restrição, conforme mostrado nas Seções "Governo", "Academia" e "Base industrial de defesa israelense". Dados de ramos sigilosos da DDR&D (Mafat) não possibilitaram ser detalhados, embora seja previsível que ela participe conjuntamente das operações de inteligência.

Há de se destacar também a participação acadêmica em pesquisas do tipo "*problem-solving*", auxiliando na melhoria e implementação de sistemas de segurança informatizados.

CONCLUSÃO

O problema apresentado no estudo foi: diante dos ciberataques às infraestruturas críticas israelenses, as ações de agentes da Tríplice Hélice contribuem para a eficácia da segurança cibernética israelense? Embora não fosse objetivo dessa pesquisa mensurar a contribuição, a percepção baseada nas fontes consultadas indica que a Tríplice Hélice de Israel contribui para a melhoria da segurança cibernética de seu país.

Para responder ao problema geral do estudo, inicialmente foi apresentada teoria dos ataques cibernéticos, da resposta a incidentes e da Tríplice Hélice. Após, uma base de dados foi utilizada, mostrando os ataques cibernéticos sofridos pelo país a partir de 2009. Finalmente, foi verificada a participação da Tríplice Hélice frente aos ataques cibernéticos sofridos pelo país em suas infraestruturas críticas.

Da análise das informações coletadas, verificou-se que, diante das ameaças às infraestruturas críticas israelenses, ficou perceptível a contribuição da Tríplice Hélice para a eficácia da segurança cibernética, visto que ela está envolvida em 17 dos 19 principais eventos de ataques cibernéticos, conforme mostrado na Tabela 3. Ou seja, há a eficácia de percepção na porcentagem 89,47% das ações de agentes da Tríplice Hélice em relação aos ataques cibernéticos às infraestruturas críticas.

A Tríplice Hélice também contribuiu diretamente para a efetividade das operações de segurança, das quais em apenas um evento foi necessário utilizar forma cinética (ataque de míssil) para destruir um centro de ci-

bernética inimigo. Em outras palavras, esse foi o único momento em que, após a identificação da ameaça, as defesas cibernéticas não foram capazes de prover a segurança necessária para o país, mostrando uma eficácia de tratamento de incidentes de 94,11% (16 eventos tratados dos 17 totais).

As indústrias, em sua maioria *startups*, auxiliaram o Estado israelense em várias atividades. Sua atuação frente às ameaças foi destacada, pois o país continuou funcionando, mostrando resiliência e sem que a sociedade fosse forçada a mudar sua rotina.

A participação acadêmica está inserida em um ciclo impulsionado por políticas de Estado alinhadas, proporcionando a sinergia entre formação de recursos humanos de qualidade, sua certificação e amadurecimento por meio do serviço militar obrigatório e seu posterior aproveitamento nas indústrias de defesa. O governo é o grande patrocinador da sinergia das pás da Tríplice Hélice, principalmente pelas destacadas ações de promoção do fomento necessário ao desenvolvimento, consubstanciados por demandas dos órgãos que trabalham com defesa cibernética ou das infraestruturas críticas.

Quando a Tríplice Hélice envolve a Base Industrial de Defesa, aumenta o protagonismo do governo, pois o cliente principal das indústrias de defesa são justamente órgãos governamentais nacionais. A maioria dos produtos de defesa não podem ser comercializados senão para governos. Nesse sentido, Israel está num contexto regional onde os incentivos do Estado favorecem o desenvolvimento da BID, particularmente na área cibernética.

Incentivos públicos na área de pesquisa diminuem a incerteza do retorno financeiro que as empresas precisam dedicar em pesquisa e desenvolvimento. A área cibernética exige recursos humanos altamente capacitados, aumentando a importância de estreita ligação com a Academia e Instituições de Ensino para prospecção de talentos e especialização dos profissionais.

Os efeitos proporcionados pela Tríplice Hélice destacam Israel no cenário mundial cibernético. Verifica-se a presença de todos os quatro elementos do poder cibernético (Segal 2016). Israel possui a capacidade de interoperar com eficácia os setores civis e militares, conforme apontado. Tal situação pode ser decorrente da conciliação do serviço militar obrigatório com seu aproveitamento como mão de obra especializada na iniciativa privada, gerando confiança e *expertise* de ambas as partes. Outra característica é a atuação (ganância necessária). Verifica-se que o setor de inteligência atacou de forma preventiva ou por retaliação os adversários, especialmente a partir de 2018. O único ponto em que Israel ainda não detém dominância se refere aos meios de TIC. O país ainda possui dependência dos EUA no setor cibernético, especialmente no tocante aos equipamentos. Suas empre-

sas não dominam o mercado, estando grande parte delas ainda na condição de *startup*. Dessa forma, Israel se caracteriza como potência cibernética em desenvolvimento e com uma Tríplice Hélice que vem contribuindo para o *status* de tal poder.

Por fim, devido à contínua modernização dos sistemas informatizados, os assuntos relativos a ataques e defesas cibernéticas continuarão em voga. O país ou grupo que detém tecnologia e a aplica em alinhamento com seus objetivos estará à frente dos seus concorrentes. Nesse sentido, o domínio da tecnologia cibernética continuará sendo um requisito crítico para o Estado de Israel em relação à sua sobrevivência no Oriente Médio.

REFERÊNCIAS

Ahmad, A., K. C. Desouza, S. B. Maynard, H. Naseer, and R. L. Baskerville. 2019. "How Integration of cyber security management and incident response enables organizational learning". *Journal of the Association for Information Science and Technology*: 939–53.

Argaman, Shahar, and Gabi Siboni. 2015. "Commercial and Industrial Cyber Espionage in Israel". In *Cyberspace and National Security — Selected Articles III. The Institute for National Security Studies (INSS)*. Tel Aviv (Abr.).

Ayyub, Rami. 2020. *Israel says it thwarted foreign cyber attack on defence industry*. https://www.reuters.com/article/us-israel-cyber-attack-idUSKCN25825T.

Baezner, Marie, and Sean Cordey. 2019. *National Cybersecurity Strategies in Comparison — Challenges for Switzerland*. Zurich: Center for Security Studies. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-National%20Cybersecurity%20Strategies%20in%20Comparison.pdf.

Berger, Navah. 2013. "The Role of Academia in a Knowledge-Based Economy: Case Study of the Seven Research Universities' Technology Transfer Offices in Israel". In *Helix Model of Innovation in Israel*. Jerusalem: The Hebrew University of Jerusalem: 71–101.

Blumenthal, Neil. 2020. *O que é uma startup:* definição, características e seus tipos. https://www.the-itfactory.com/startup-knowledgebase/article/what-is-a-startup/.

Carr, Edward Hallett. 1981. *The Twenty Years Crisis: 1919-1939*. An Introduction to the Study of International Relations. London; New York: Macmillan & Co. Ltd.; St. Martin's Press Inc.

Clearskysec. 2019. *Hamas Attack — Impersonating "Red Alert" App, Cellcom TV and New Websites*. https://www.clearskysec.com/wp-content/uploads/2019/02/ClearSky-End_of_Year_Report-2018.pdf.

Cohen, M. S., C. D. Freilich, and G. Siboni. 2015. "Israel and Cyberspace: Unique Threat and Response". *International Studies Perspectives*: ekv023.

CPR. 2020. *Check Point Research. Hamas Andoid Malware on IDF Soldiers* — This is how it happened. https://research.checkpoint.com/2020/hamas-android-malware-on-idf-soldiers-this-is-how-it-happened/.

CSIS. 2021. Center for Strategic & International Studies. *Significant Cyber Incidents*. https://csis-website-prod.s3.amazonaws.com/s3fs-public/210430_Significant_Cyber_Events_List.pdf?B21zjJhsoO3qkgQNyGMmZN5IhAE80S_I.

Driori, G. S., O Barkai, A. Bem-Dor et al. 2013. *The Helix Model of Innovation in Israel:* The Institutional and Relational Landscape of Israel's Innovation Economy. Jerusalem: The Hebrew University of Jerusalem.

Estados Unidos da América (EUA). 2013. Departamento de Segurança Interna. Centro de Recursos em Infraestruturas Críticas. http://training.fema.gov/EMIWeb/IS/is860a/CIRC/defense1.htm.

Estados Unidos da América (EUA). 2021. *U. S. Security Cooperation with Israel:* fact sheet. https://www.state.gov/u-s-security-cooperation-with-israel/.

Etzkowitz, H. 2003. "Innovation in Innovation: The Triple Helix of University-Industry-Government Relations". *Social Science Information* 42, no. 3: 293–337.

Etzkowitz, H. et al. 2008. "Pathways to the enrrepreneurial university: towards a global convergence". *Science and Public Policy* 35, no. 9: 681–95.

Faga, Hemen Philip. 2017. "The Implications of transnational cyber threats in International Humanitarian Law: Analysing the distinction between cybercrime, cyberattack, and cyber warfare in the 21st century". *Baltic Journal of Law & Politics*. Ebonyi State University.

Faglin, Guy. 2018. *A corrida da inovação —Tecnologias comerciais e militares em armas*: o ponto de equilíbrio apropriado. x ed. Haifa-Israel.

Gross, Judah Ari. 2018. "After Facebook, Hamas turns to Instagram to lure IDF soldiers, army says". *The Times of Israel* (Ago.). https://www.timesofisrael.com/after-facebook-hamas-turns-to-instagram-to-lure-idf-soldiers-army-says/.

Hackmageddon. *Cyber attacks timeline.* 2021. https://www.hackmageddon.com/category/security/cyber-attacks-timeline/.

Israel. 2002. *Background for the Establishment of the Bureau.* Jerusalém: Escritório do Primeiro Ministro.

Israel. 2011. *Israel National Cyber Directorate.* https://www.gov.il/en/departments/units/israel_national_cyber_directorate_unit.

Israel. Ministério da Defesa. 1985. DDR&D — *Directorate of Defense Research & Development.* https://english.mod.gov.il/About/Innovative_Strength/Pages/Directorate-_of_Defense_Research_Development.aspx.

Israel. Ministério da Defesa. 2018. *Promoção das Exportações em Defesa.* https://english.mod.gov.il/About/Defense_Exports/Pages/default.aspx.

Israel. Ministry of Foreign Affairs. 2020b. *List of countries and status of diplomatic relations with Israel.* https://www.gov.il/en/Departments/General/israeli_relations.

Israel. 2017. *National Cyber Array.* https://www.gov.il/he/Departments/publications/reports/hospital_guidelines.

Israel. 2020. "Israeli defense exports pull in $7.2 billion in sales. *The Jerusalem Post* (Jun.). https://www.jpost.com/israel-news/israeli-defense-exports-pull-in--72-billion-in-sales-632356.

Kalman, Matthew. 2011. *Israel denies Anonymous cyber-attack to blame for websites failure.* https://www.theguardian.com/world/2011/nov/07/israel-anonymous--cyber-attack-websites.

Karspersky. 2020. *O que é ransomware?* https://www.kaspersky.com.br/resource--center/definitions/what-is-ransomware.

Clarke, R. A., and R. K. Knake. 2015. *Guerra Cibernética:* A próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro: Braspot.

Kuehl, Daniel T. 2009. *From Cyberspace to Cyberpower:* Defining the Problem em Cyberpower and National Security. Washington, D. C.: National Defense UP.

Markownski, S., P. Hall, and R. Wylie (Eds.). 2010. *Defence Procurement and Industry Policy:* A small country perspective. London; New York: Routledge.

Marteu, E. 2018. "Israel and the Jihad threat". *Survival — Global Politics and Strategy* 60: 85–106. Abingdon (Reino Unido): Routledge.

Mekorot. 2020. *General Information.* https://www.mekorot.co.il/Eng/newsite/AboutUs/Pages/GeneralInformation.aspx.

Mitigate Cyber. 2014. *Chinese hackers steal israeli military documents.* https://mitigatecyber.com/chinese-hackers-steal-israeli-military-documents/.

Moran, Dominic. 2008. "Israel: Defense Boom Seeks Wiggle Room". *ISN Security Watch.* Zurich.

Nye, J. S. 2010. *Cyber Power.* Cambridge: Havard Kennedy School.

ONU. 1995. *Israeli-Palestinian Interim Agreement on the West Bank and the Gaza Strip.* Washington, D. C. (Set.). https://peacemaker.un.org/sites/peacemaker.un.org/files/IL%20PS_950928_InterimAgreementWestBankGazaStrip%28OsloII%29.pdf.

Paganini, Pierluigi. 2017a. *Iranian Group OilRig is back and delivers digitally signed malware.* https://securityaffairs.co/wordpress/55145/apt/oilrig-apt-itan.html.

Paganini, Pierluigi. 2017b. *The massive attack against Israel alleged lauched by Iranian OilRig APT group.* https://securityaffairs.co/wordpress/58464/hacking/oilrig--apt-target-israel.html.

Press, Viva Sarah. 2018. "Under Attack: Israeli Cyber Experts Warns Of Large-Scale Healthcare Hacks". *NoCamels* (Jul.). https://nocamels.com/2018/07/israeli-cyber-experts-healthcare-hacks/.

Project Grey Goose. 2009. "Project Grey Goose Phase II Report: The evolving state of cyber warfare". *Greylogic* (Mar.).

Ralph, Talia. 2015. *Syria's Electronic Army attempted attack on Haifa's water system.* https://www.pri.org/stories/2013-05-25/syrias-electronic-army-attempted-attack-haifas-water-system.

Reuters. 2016. *Israel acusa palestino de hackear drones e dados de aeroporto.* https://br.reuters.com/article/internetNews/idBRKCN0WP2II.

Sadeh. Sharon. 2004. "Israel's Defense Industry in the 21st Century: Challenges and Opportunities". *Strategic Assessment Quarterly* 7, no. 3 (Dez.). Tel Aviv: Jaffee Center for Strategic Studies.

Seculert. 2012. *Mahdi — The cyber savior?* https://web.archive.org/web/20121117052310/http:/blog.seculert.com/2012/07/mahdi-cyberwar-savior.html.

Segal, Adam. 2016. "The Hacked World Order: how nations fight, trade, maneuver, and manipulate in the digital age". *Public Affairs*. New York.

Singer, P. W., and A. 2014. Friedman, *Cybersecurity and Cyberwar:* what everyone needs to know. New York: Oxford University Press.

Stockolm International Peace Research Institute. 2021. *Sipri Military Expenditure Database*. https://www.sipri.org/databases/milex.

Storm, Darlene. 2016. *No, Israel's power grid wasn't hacked, but ransomware hit Israel's Electric Authority*. https://www.computerworld.com/article/3026609/no-israels--power-grid-wasnt-hacked-but-ransomware-hit-israels-electric-authority.html.

The Intercept. 2016. *ISUAV Video Descrambling*. https://www.documentcloud.org/documents/2699846-Anarchist-Training-mod5-Redacted-Compat.html.

Thompson, Eric C. 2018. *Cybersecurity Incident Response:* How to Contain, Eradicate, and Recover from Incidents. Lisle: Apress

Times of Israel. 2020b. *Cyber attacks again hit Israel's water system, shutting agricultural pumps*. https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/.

Times of Israel. 2020a. *Israeli firm says Chinese cyber-espionage tool used to spy on governments*. https://www.timesofisrael.com/israeli-firm-says-chinese-cyber-espionage-tool-used-to-spy-on-governments/.

Toynbee, Arnold. 1987. *A Study of History*. Oxford University Press.

Trend. 2012. *Israeli fire service site attacked by 'Gaza Hackers'*. https://en.trend.az/world/israel/1979610.html.

Williamson, Mark L. 2012. *The Cyber Military Revolution and the need for a new framework of war. Joint Forces Staff College:* https://apps.dtic.mil/dtic/tr/fulltext/u2/a562392.pdf.

Wipo. 2021. *Global Innovation Index 2021: Tracking Innovations through Covid-19 crisis*. Genebra: World International Property Organization.

Zhuang, R., A. G. Bardas, S. A. Deloach, and O. Zinming. 2015. *A Theory of Cyber Attacks: A step towards analyzing MTD Systems:* 11-20. Kansas University.

NOTAS

1. "Ciberataques às infraestruturas críticas" israelenses é a variável independente.
2. "Ações de agentes da Tríplice Hélice" é a variável interveniente.
3. "Eficácia da Segurança Cibernética israelense" é a variável dependente.
4. Anonimização é o efeito de se tornar anônimo.
5. "Domínio global dentro do ambiente informacional, cujo caráter distintivo e único é moldado pelo uso da eletrônica e do espectro magnético para criar, armazenar, modificar, trocar e explorar informações através de meios interdependentes e redes interconectadas usando Tecnologia de Informação e Comunicação" (Kuehl 2009, 28)
6. Acrônimo de *Israel Defense Forces*.
7. Acrônimo de *Command, Control, Computer, Communications and Inteligence*.
8. Acrônimo de *Agaf há-Modi'in* que significa inteligência militar.
9. Acrônimo de *Israel Security Agency*. Também conhecido como *Shin Bet*.
10. Acrônimo de *National Cyber Directorate*.
11. O Departamento de Segurança Interna do principal aliado israelense, os Estados Unidos da América (EUA), inclui na BID as entidades e subcontratadas nacionais e estrangeiras que atuam em sistemas, subsistemas, componentes ou peças de armas militares para as agências federais (EUA 2020). Utilizado conceito dos EUA por não haver descoberto o conceito israelense.
12. Uma *startup* é uma empresa que trabalha para resolver um problema onde a solução não é óbvia e o sucesso não é garantido (Blumenthal 2020).
13. Acrônimo para *Produto de Defesa*.
14. Acrônimo para *The International Defense Cooperation Directorate of the Israel Ministry of Defense*.
15. Acrônimo para *The Directorate of Defense Research and Development)*.
16. Acrônimo para *The Department of Production and Procurement (DOPP)*.
17. As bases de dados do CSIS e Hackmageddon foram utilizadas por conta da quantidade de citações em artigos acadêmicos. O CSIS é o Centro de Estudos Estratégicos Internacionais e possui viés acadêmico. Já o Hackmageddon possui característica técnica.
18. Software malicioso que criptografa dados do computador e exibe mensagens exigindo pagamento de uma taxa para fazer o sistema voltar a funcionar (Kaspersky 2020).

A TRÍPLICE HÉLICE ISRAELENSE NO CENÁRIO DE CIBERSEGURANÇA

RESUMO

Conflitos envolvendo Israel têm sido constantes na história do país. O século XX consolidou suas fronteiras com guerras nas quais a superioridade qualitativa lhe foi favorável, mas que também geraram uma realidade de infindáveis hostilidades que ultrapassam seu entorno estratégico. A Tríplice Hélice israelense é composta por governo, indústria e academia com foco que prioriza ativos de conhecimento e inovação, incluindo a área de cibernética. Nesse sentido, os resultados indicam que a Tríplice Hélice tem participado do esforço de segurança cibernética do país, notadamente nesse início do século. A partir de 2009, houve aumento importante do número de ataques cibernéticos contra infraestruturas críticas israelenses, objeto de estudo deste trabalho. A metodologia de investigação é qualitativa com abordagem exploratória, utilizando-se revisões bibliográficas. Baseando-se no banco de dados do CSIS e Hackmagedon e de relatórios de antivírus, os resultados apontaram que Israel vem otimizando seus recursos na defesa dessas infraestruturas, superando tecnologicamente seus adversários. A Tríplice Hélice tem auxiliado no desenvolvimento dessas soluções em produtos e serviços de defesa para que o Estado faça frente ao cenário desafiador, cooperando para sistemas responsivos, resilientes e dinâmicos. Tal interação em prol da segurança cibernética nacional tem sido eficaz, na medida em que o Estado tem explorado favoravelmente a sinergia de esforços entre suas forças de defesa e a inovação tecnológica da BID e academia.

Palavras-chave: Tríplice Hélice, Cibersegurança e Infraestruturas Críticas de Israel.

ABSTRACT

Conflicts involving Israel have been constant in the country's history. The 20th century consolidated its borders with wars in which qualitative superiority was favorable to it, but which also generated a reality of endless hostilities that went beyond its strategic surroundings. The Israeli triple helix is made up of government, industry and academia with a focus that prioritizes knowledge and innovation assets, including the area of cybernetics. In this sense, the results indicate that the triple helix has participated in the country's cybersecurity effort, notably at the beginning of the century. From 2009 onwards, there was a significant increase in the number of cyber-attacks against critical Israeli infrastructure, the object of study of this work. The research methodology is qualitative with an exploratory approach, using bibliographic reviews. Based on the CSIS and Hackmagedon database and antivirus reports, the results showed that Israel has been optimizing its resources in the defense of these infrastructures, technologically outperforming its adversaries. Triple Helix has helped in the development of these solutions in defense products and services for the State to face the challenging scenario, cooperating for responsive, resilient and dynamic systems. Such interaction in favor of national cybersecurity has been effective, insofar as the State has favorably exploited the synergy of efforts between its defense forces and the technological innovation of the IDB and academia.

Keywords: Triple Helix, Cybersecurity and Israel's Critical Infrastructure.

Recebido em 24/11/2021. Aceito para publicação em 17/12/2022.