Israel e defesa cibernética: estudo da vinculação Estado, setor privado e academia

Israeli cyberdefense: State, private sector and academy sector

Rev. Bras. Est. Def. v. 7, nº 2, jul./dez. 2020, p. 81-101
DOI: 10.26792/RBED.v7n2.2020.75206
ISSN 2358-3932

JÚLIA LOOSE
GRACIELA DE CONTI PAGLIARI

INTRODUÇÃO[1]

O avanço de tecnologias de informação e comunicação (TICs) e a popularização do acesso à Internet criaram processos inseridos em um ambiente complexo nas discussões das Relações Internacionais: o espaço cibernético. Sua complexidade se dá pelo exercício de se pensar em uma dimensão que não existe materialmente, mas que permeia todos os espaços físicos que se compreende por reais. Trata-se de uma dimensão virtual que se sustenta em primeiro lugar pela ação humana, portanto, é primordial pensá-la como um recurso de poder de quem a prioriza.

Em face deste cenário de transformação tecnológica, o presente artigo propõe analisar o tema a partir do seu estudo em um Estado relevante em matéria de defesa cibernética, o Estado de Israel. Sua capacidade tecnológica e a importância da cibernética do ponto de vista militar, bem como as regulamentações condutoras das políticas na área, justificam um estudo mais aprofundado sobre o tema. O objetivo do artigo é apresentar quais são os elementos que compõem a infraestrutura de defesa cibernética do Estado de Israel bem como sua evolução, e para este feito, busca-se analisar os documentos e marcos de referência em matéria cibernética, incluindo o atual documento de defesa nacional divulgado em 2015, *The Israel Defense Forces Strategy*, quanto à interpretação do Estado em relação ao ciberespaço e construção de capacidades tecnológicas militares.

Júlia Loose — Doutoranda do Programa de Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina (UFSC). Mestra em Relações Internacionais pela Universidade Federal de Santa Catarina.
Graciela De Conti Pagliari — Professora Associada da Universidade Federal de Santa Catarina. Doutora em Relações Internacionais pela Universidade de Brasília.

O artigo está dividido em duas partes devido à quantidade de informações do tema. O período temporal adotado para esta análise, 2010 a 2015, justifica-se por duas características: i) surgimento do *worm* Stuxnet (2010) e ii) criação do *National Cyber Boureau* (NCB), que ao serem exploradas demonstram a relevância da implementação da prioridade cibernética por Israel. Inicialmente aborda-se, como uma forma de apresentar o estado da arte no tema, o ciberespaço no seu espectro de novas ameaças, demonstrando os ataques cibernéticos a Israel que permearam o período temporal abordado. Na segunda parte será apresentado o mapeamento da infraestrutura de defesa cibernética do país quanto a seus organismos, e legislações de referência nas três esferas: estatal, privada e acadêmica-científica. Contata-se que Israel atribui prioridade para o setor cibernético em seu plano de defesa multidimensional, a partir do elemento de cooperação tripartite, tendo sua infraestrutura de defesa composta por Estado, setor privado e academia. Prioridade a qual, se condiciona devido à sua específica dinâmica securitária regional representada pela presença efetiva de atividades cibernéticas realizadas majoritariamente por fontes não tradicionais provenientes de grupos militares armados e sociedade civil.

Ademais, salienta-se que se desconhecem publicações em português com o mapeamento aqui realizado, cuja temática se torna relevante para o planejamento de defesa cibernética no Brasil, tanto no âmbito institucional das Forças Armadas, quanto nos âmbitos privado e acadêmico-científico. Tanto Israel quanto Brasil se constituem como duas potências regionais inseridas em sistemas regionais periféricos, dotados de particularidades próprias, e, portanto, capazes de exercer poder regionalmente, inclusive na esfera cibernética. Israel demonstra-se como um exemplo robusto de articulação de cooperação tripartite interagências, o que favorece a inserção do debate acerca do desenvolvimento deste tipo de cooperação, em nível doméstico, já existente no Brasil que pode ser aprimorada.

CIBERESPAÇO: BREVE APRESENTAÇÃO

Ciberespaço no espectro das novas ameaças

A literatura apresenta diferentes definições do ciberespaço não havendo consenso. Para Kuhel (2009, 29), o ciberespaço trata-se de um domínio operacional marcado "pelo uso da eletroeletrônica e do espectro eletromagnético com a finalidade de criação, armazenamento, modificação e/ou troca de informações através de redes interconectadas e interdependentes". O ciberespaço precede o surgimento da Internet, a qual por sua vez, é um elemento que compõe este espaço, sendo um condicionante para os

processos que nele ocorrem — espionagem, hacktivismo, guerra cibernética, entre outros. Observa-se, nesse sentido, que se trata de um domínio já existente dependente do desenvolvimento tecnológico, utilizado tanto nas relações domésticas para comunicação entre pares quanto no âmbito estatal para coleta de informações de inteligência.

Uma das definições é a proposta por Ventre (2011, 34), que critica a ideia de que o ciberespaço é sinônimo de Internet, mas sim argumenta que se trata de um escopo muito mais amplo que envolve diferentes camadas. Em suas palavras: "o ciberespaço é representado em três camadas: camada inferior: infraestrutura (*hardware*); camada intermediária (*software*) e a camada superior cognitiva". A essência da definição de Ventre (2011) é a característica de transversalidade do ciberespaço entre os espaços virtual e real. Todas as dimensões que são compreendidas como convencionais: terra, ar, mar e espaço sideral fazem parte do espaço real e são compostas pela existência de sistemas de telecomunicações, internet, infraestrutura, ordenadores, IPs, etc. Na dimensão virtual encontra-se o ciberespaço — e é quando essas duas dimensões se entrelaçam e interagem que ocorrem os ataques cibernéticos.

Os ataques cibernéticos, portanto, são atos agressivos que partem da dimensão real, e por meio da dimensão virtual alcançam determinado objetivo cujo impacto não se limita apenas ao ciberespaço. Podem ocorrer nas três camadas: hardware, quando direcionado a redes; software quando direcionado a espionagem e na camada humana cognitiva quando o objetivo é transmitir uma mensagem, comunicar ou informar. Já a Guerra cibernética é definida "como a dimensão cibernética de um conflito armado" (Ventre 2011, 37), fator o qual alavancou aos Estados o investimento de infraestrutura e estratégias de ciberdefesa e cibersegurança, o que também ocorreu aos atores não estatais conforme explorado por Barker (2019).

Para Barker (2019, 4) os mesmos conceitos trabalhados na Guerra, como ataque, defesa, privacidade, segurança foram transpostos para o "mundo cibernético". Nesse processo, além do engajamento dos Estados, os grupos não estatais expandiram seu escopo da guerra tradicional para a esfera cibernética, o que gera uma relação de igualdade perante a capacidade dos Estados Nações. Ou seja, o ponto de Barker (2019) é salientar que as atividades cibernéticas podem ser avançadas de forma equiparada tanto por Estados quanto por atores não estatais, tendo os últimos menos riscos do que os Estados, devido sua baixa infraestrutura para ataque (Barker 2019, 4). Embora os atores não-estatais demonstrem baixa capacidade cibernética, esse elemento na configuração da guerra cibernética interessa a este artigo, dado que Israel pertence a um entorno regional com alta presença relativa de atores não estatais, bem como considera o ciberespaço como uma quarta dimensão na estratégia de defesa e proteção, conforme

destacado em sua política declaratória de defesa "[...] Defense in all four dimensions (land, sea, air and cyber)." (IDF 2016, 18).

ISRAEL: ATAQUES E RESPOSTAS CIBERNÉTICAS NO PERÍODO DE 2010 — 2015

Autodeclarado como um Estado judeu, em meio a um "núcleo árabe fragmentado em múltiplos territórios" (Hinnebusch 2003, 3), o investimento de Israel em inovação tecnológica para defesa é uma prioridade. Não obstante, essa prioridade foi impulsionada pelos recorrentes ataques cibernéticos que o Estado enfrentou a partir dos anos 2000, especialmente após a acusação do seu suposto envolvimento — nunca autodeclarado — no *Worm Stuxnet*.

O entorno regional israelense caracteriza-se por uma configuração com correlação de forças estatais e não estatais que investem em medidas de infraestrutura cibernética[2]. Quanto à primeira ameaça de cunho estatal, Israel enfrentou ataques em sua maioria protagonizados pelo Irã, mas também por Turquia, África do Sul, Rússia e China (Cohen, Freilch, and Siboni 2015), como se verá no desenvolvimento dessa seção. Os atores não estatais apresentam duas categorias: os grupos armados e a sociedade civil. Aqueles compreendem como principais, Hezbollah e Hamas, o primeiro com sede no Líbano e o segundo com sede na Palestina. Já a atuação da sociedade civil, inclui-se nesse processo por meio da atuação de hackers ativistas.

A disseminação do Stuxnet (2010) foi um fator importante regionalmente, para o estudo da relevância dos ataques cibernéticos realizados contra Israel posteriormente. O Stuxnet é um sofisticado *worm* de computador criado especificamente para se infiltrar em sistemas de controle industrial. O ataque mais significativo foi o ataque ao sistema desenvolvido pela Siemens, para girar as centrífugas de enriquecimento de urânio do Irã, na usina de Bushehr (Tabansky 2016, 61). O *worm* foi detectado em junho de 2010 pela Microsoft — que também foi atacada em todos os sistemas Windows — e pela companhia Symantec Norton Security (Fildes 2010). Estimou-se que o *W32.Stuxnet*, seu nome técnico, atingiu em um período de 48 horas cerca de 14.000 endereços de IP de instalações de diversos países conforme mostra a Figura 1.

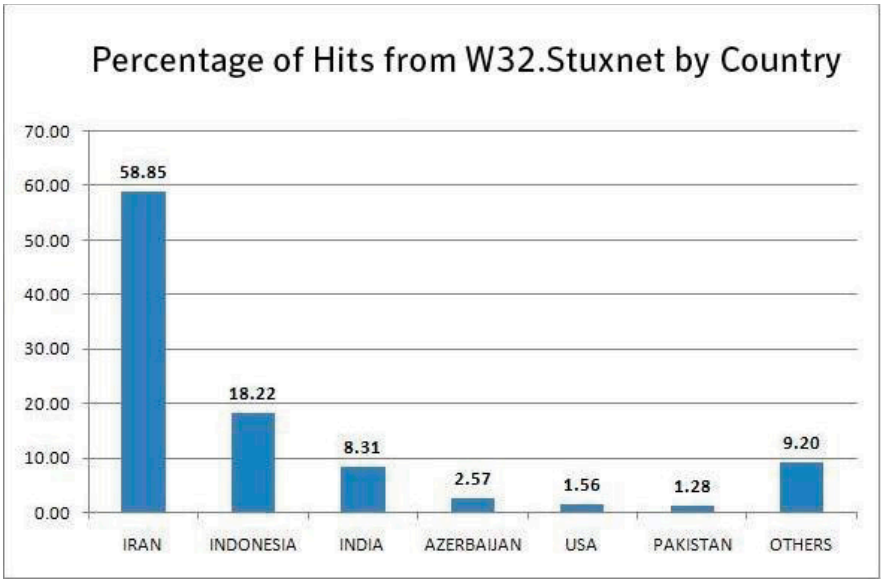

Figura 1 — Porcentagem de ataques do Stuxnet por país
Fonte: Retirado do Relatório "*W32.Stuxnet — Network Information*", elaborado pela Symantec Corporation (2010).

A partir do Stuxnet, compreendeu-se que um ataque realizado no ciberespaço poderia criar danos extremos no espaço físico com dano nuclear, embora esse objetivo não tenha sido concretizado[3]. Conforme aponta Milevski (2011, 65. Tradução nossa), pela primeira vez no "submundo do ciberespaço que um pacote abrangente foi capaz de se espalhar por si mesmo e ser empregado contra uma meta específica para alcançar ou facilitar um objetivo político", em sua duração de 48 horas. O autor destaca a importância que deve ser dada ao caso do Stuxnet, mesmo que não tenha atingido seu fim, dado sua complexidade e possibilidade de sucesso:

> O Stuxnet (*Malware*), no contexto internacional, em última análise, não afetou a vontade política iraniana de obtenção de um programa nuclear soberano. Então como o Stuxnet poderia ser bem sucedido? Esse tipo de ataque teria que ser destrutivo o suficiente, ao impactar as capacidades iranianas de fato ao acabar com o material disponível para seus programas nucleares. Além disso, também deveria ser capaz de superar o aumento da eficiência nuclear iraniana. Esse sucesso poderia ser possível, visto que o Stuxnet tem uma vantagem significativa sobre as operações físicas: ao contrário das pessoas reais, um malware pode estar em múltiplos lugares ao mesmo tempo, centenas de milhares, milhões ou mais. (Mileviksy 2011, 69, Tradução Nossa).[4]

Por ser criado com o objetivo de atingir sistemas industriais de infraestruturas críticas do espaço físico (centrais elétricas, usinas hidrelétricas e unidades industriais nucleares), o Stuxnet foi apontado como o mais sofisticado ataque cibernético já realizado e por esse motivo associa-se sua criação com algum Estado (Fildes 2010). Nunca houve autoria declarada, no entanto o governo iraniano apontou que sua criação teve motivação governamental, acusando Estados Unidos e Israel. Segundo Barker (2019), nos casos em que armas cibernéticas parecem ter sido usadas por atores estatais, dificilmente algum Estado aceitou a responsabilidade de usá-las e o caso do Stuxnet é um exemplo, pois se acusa o envolvimento de Israel e Estados Unidos, mas nunca houve uma declaração por parte de ambos (Barker 2019, 8). Aqui salienta-se a dificuldade da pesquisa em classificar a autoria dos ataques, devido a particular característica de anonimato que o ciberespaço proporciona.

No cenário israelense, nesse mesmo contexto, foi criado em 2011 o NCB, já mencionado, uma agência governamental que atua em parceria tanto com o setor privado, quanto com o setor acadêmico para o desenvolvimento de políticas de cibersegurança e liderança global. O NCB é um órgão fundamental para a pesquisa e mapeamento dos ataques cibernéticos ao país e no fomento do desenvolvimento de tecnologia para combatê-los (Cohen, Freilch, and Siboni 2015, 4).[5]

Conforme apontam Cohen, Freilch e Siboni (2015), estima-se que Israel sofra ataques com origem de grupos estatais e não-estatais, Hezbollah e Hamas, os quais, segundo o governo israelense, são liderados pelo Irã. Em 2011, Israel acusou o Irã de liderar a Operação *newscaster* contra si mesmo e Estados Unidos. A Operação consistiu na criação de falsas identidades virtuais com laços de funcionários do governo e repórteres. O ataque comprometeu mais de dois mil computadores e foi descoberto somente em 2014. Dois anos antes (2012), Israel havia acusado novamente o Irã, Hamas e Hezbollah como responsáveis por uma série de ataques que se sucederam aos sistemas nacionais vitais do país, como água, energia e bancos (Cohen, Freilch, and Siboni 2015, 4).

No período aqui abordado, um dos ataques mais significativos foi a Operação *#OpIsrael*, coordenada pelo grupo *Anonymous* e demais hacktivistas pró-Palestina. A Operação iniciou em 2013 e consistiu em um ataque programado para que fossem retirados do ar todos os sites do governo no dia do *Holocaust Remembrance Day* (27 de janeiro). Foi retirada do ar uma gama de sites governamentais, incluindo sites de bancos e agências financeiras e do Museu Nacional do Holocausto. Durante grande parte do dia, Tel Aviv ficou sem conexão de Internet. Estimou-se que o dano causado foi de três bilhões de dólares de prejuízo para o país. Os sites eram retirados

com a utilização da *hashtag #Opisrael*, que também estava sendo disseminada nas redes sociais como o Twitter (Pitts 2017).

Durante a Operação Margem Protetora (2014), ofensiva contra o Hamas que durou mais de um mês, outro ataque cibernético retirou do ar o site das FDI por diversas vezes. Aqui cabe mencionar o contexto da operação, que gerou uma comoção internacional, dado que acarretou a baixa de palestinos mortos — civis confome caracterização do conflito israelo-palestino — em sua maioria, jovens[6]. Um aspecto curioso desta operação que corrobora o propósito deste artigo foi sua narração direta feita no Twitter, pelo perfil das FDI, que oscilava entre estar disponível ou fora do ar (Cohen, Freilch, and Siboni 2015, 4).

Os eventos acima mencionados representam um contexto regional que além de altamente militarizado, dispõe de ameaças cibernéticas, o qual justifica o investimento em infraestrutura aprimorada. Israel é um exemplo que priorizou em seu projeto de grande estratégia nacional o desenvolvimento de capacidades tanto ofensivas quanto defensivas em matéria cibernética. Essas capacidades resultaram em sua estrutura em defesa cibernética, desenvolvida a partir do investimento em inovação em ciência e tecnologia com a cooperação tripartite entre Estado, setor privado e academia, conforme trabalhado a seguir.

ISRAEL: INFRAESTRUTURA EM DEFESA CIBERNÉTICA

Israel é reconhecido mundialmente pelo seu envolvimento com tecnologias de inovação, fomento à pesquisa cientifica e desenvolvimento de startups. Segundo dados do centro israelense *Central Bureau of Statistics*, em 2014, dentro do escopo de países da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) o Estado de Israel, considerando a porcentagem do PIB nacional, ocupou o segundo lugar de liderança dos gastos em pesquisa e inovação tecnológica, conforme aponta o relatório desenvolvido no NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Estão incluídos nesse processo de desenvolvimento, a instalação de tecnologias avançadas de infraestrutura de comunicação, que incluem cabos fixos e a construção de fibra ótica (CCDCOE, 2017 6).

Conforme aponta Tabanksy (2016), o alto investimento em tecnologia sob iniciativa do Estado, fez com que o país se utilizasse do ciber poder[7] na aplicação do *hard power* e dissuasão da sua política defesa, especialmente frente ao Irã nuclear. No que tange ao investimento de ciber tecnologia para defesa nacional, Tabansky (2016, 51) aponta que a tecnologia cibernética oferece ferramentas novas e acessíveis para o alcance mais rápido de seus interesses no conflito, isso inclui arquitetura de rede e de sistema,

criptografia, amostras de malware, comandos militares e indicadores de defensores cibernéticos. Para que se possa dimensionar o investimento na esfera do Estado, do setor privado e da academia, apresenta-se a seguir um rigoroso levantamento destes investimentos[8].

Estado

Nesta subseção, serão apreciadas três iniciativas do Estado, que cresceram em importância conforme a política de prioridade do tema foi sendo implementada. Essas iniciativas dividem-se em dois grandes momentos: fim da década de 1990, com criação da plataforma *Tehila*, e a partir de 2010 com a criação de dois órgãos: o NCB, já mencionado, e o *National Cyber Secutiry Authority*.

No fim da década de 1990, Israel criou a plataforma eletrônica *Tehila*, *Government Infrastructure for the Internet Age*. A plataforma consistia em uma ferramenta de proteção destinada à garantia de conexões seguras de acesso à Internet dos escritórios governamentais e aos sites do governo. A criação da *Tehila* foi a primeira iniciativa do país para proteção das redes nacionais, que, posteriormente e de maneira mais sofisticada tecnologicamente, tornou-se a National Information Security Authority (NISA), criada para a proteção da infraestrutura nacional em matéria de informação (Cohen, Freilch, and Siboni 2015, 5). Atualmente a *Tehila* evoluiu para a o portal do governo (gov.il) de acesso ao público, que contém uma ampla gama de orientações das políticas promovidas pelo Estado em saúde, emprego, educação, investimento estrangeiro, além do fornecimento de serviços eletrônicos utilizados pela população como o portal de atividade fiscal e o sistema jurídico. O portal do governo é disponível em hebraico, árabe e inglês.

Em 2010, a segurança cibernética se tornou publicamente um objetivo prioritário. O Primeiro Ministro, Benjamin Netanyahu, lançou a Iniciativa Cibernética Nacional sob os cuidados do Ministério da Ciência, no conselho Nacional de Pesquisa e Desenvolvimento. Essa atividade foi uma força tarefa composta por mais de oitenta funcionários das FDI, setor privado e academia. O objetivo era a promoção da liderança israelense na segurança cibernética em nível global e resultou na Resolução 3611 (2011) do Governo intitulada de "Promoção das Capacidades Nacionais do Ciberespaço" (CCDCOE 2017, 8).

A Resolução 3611 foi o prelúdio para a criação do já mencionado NCB: primeiro órgão nacional de consultoria e consolidação para segurança cibernética. Conforme aponta o relatório da CDCOE, a Resolução 3611 indica quatro prioridades de domínio do ciberespaço para Israel. São elas:

(1) o avanço das capacidades nacionais e a melhoria da gestão dos atuais e futuros desafios do ciberespaço.
(2) melhorar a defesa das infraestruturas nacionais essenciais para a manutenção de uma vida estável e produtiva no Estado de Israel.
(3) avançar o status do país como um centro global para o desenvolvimento de tecnologias de informação.
(4) incentivar a cooperação interdisciplinar entre a academia, setor privado e ministérios. (CCDCOE 2017, 8).

Com o avanço do debate sobre o desenvolvimento cibernético no país, em 2015 o NCB estabeleceu um segundo órgão nacional de segurança cibernética, a *National Cyber Secutiry Authority*. Ambos os órgãos são os pilares institucionais da Direção Nacional de Defesa Cibernética (*Ma'arach)* que incluiu outras Resoluções para além da 3611. A atual estrutura governamental em matéria cibernética está sintetizada no organograma a seguir:

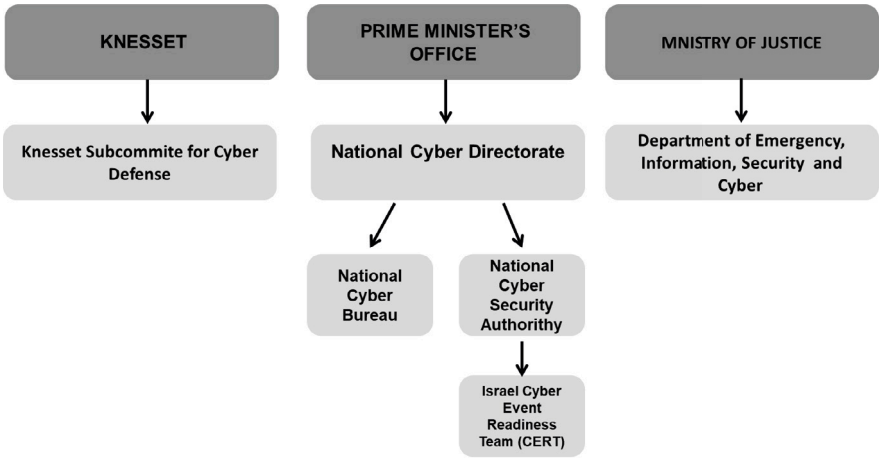

Figura 2: Estrutura de Defesa Cibernética de Israel
Fonte: Elaboração própria baseada em informações coletadas no site do governo israelense e documento da Política Declaratória de Defesa (2016).

Mencionado no relatório, a Mossad, Agência de Inteligência israelense supostamente desenvolve em cooperação com o *National Cyber Directorate*, capacidades cibernéticas defensivas para abordar uma ampla gama de ameaças. No entanto, ressalta-se que as informações não estão disponíveis

por se tratar de uma agência de inteligência da magnitude da Mossad. A seguir apresentaremos as agências em matéria cibernética ainda pertencentes a esfera estatal, no âmbito das FDI.

Forças de Defesa Israelenses

Apresenta-se as FDIs como subtópico à parte, pois as mesmas não se confundem com as demais iniciativas políticas dos governos, exceto pela dinâmica prioritária que é estabelecida para a área cibernética. As FDI, compostas pelo Chefe do Estado Maior Geral, Alto Comando e efetivos do exército, força aérea e marinha (IDF, online), representam uma das estruturas mais importantes do Estado israelense em face de seu entorno conflitivo e das ameaças e relações de desconfiança regionais. As mesmas estão incluídas no *National Cyber Directorad*, ao desenvolver capacidade cibernética na defesa de redes de comunicação, sistemas de armamento e coleta de informações sobre o inimigo que possui tecnologia e capacidade de ataque as suas redes de Defesa (Cohen, Freilch, and Siboni 2015, 6).

Em 2012, as FDI implementaram o *IDF Cyber Defender Training Course*, um amplo programa de treinamento militar para segurança cibernética. O treinamento consiste no recrutamento de militares por meio de exames técnicos em parceira com o Centro de Computação e Informação de Sistemas (*Computing and Information System*) e a Escola de Profissionais de Computação (*School for Computer Professions*) — outras duas agências do escopo das FDI. A partir deste sistema organizacional criaram-se diversas unidades militares especializadas em defesa cibernética. Em sua maioria, as unidades não são divulgadas pelo Estado e não aparecem nos sites oficiais, o que torna um tema difícil de ser explorado. No entanto, as duas unidades divulgadas, embora com defasagem de dados, são a Unidade 8200 e a Unidade C4I.

A Unidade 8200 consiste em uma unidade de inteligência composta por um grupo militar de elite que desenvolve tecnologias de defesa. Em muitos aspectos, conforme apontam Coheh, Freilch e Siboni (2015) a unidade se equipara à Agência de Segurança Nacional dos Estados Unidos (NSA), e, portanto, as informações também são classificadas. Contudo, segundo os relatórios da Oitava Conferência Internacional de Cyber Conflito em Israel (2016), a Unidade 8200 foi responsável pela resposta de Israel à ataques cibernéticos mencionados na seção anterior, tal qual o ataque às facilidades nucleares da Síria, conhecido como a *Operação Orchard* em setembro de 2007 (Tabansky 2016).

Cabe destaque a esta Operação pois se tratou de um exemplo da combinação de elementos militares tradicionais (enfoque para a Força Aérea)

e elementos de ciberataque que paralisaram a Força Aérea Síria. Segundo (Raska 2015, 6. Tradução Nossa): "a operação Orchard é o primeiro exemplo do tipo de capacidades que as nações terão de alavancar no futuro com a utilização do ciberespaço como multiplicador de força". Aqui se tangenciou a capacidade das FDI em atuar no campo de batalha com tecnologia cyber e obter êxito. Além dessa Operação, Israel utilizou suas capacidades tecnológicas em outras ações ofensivas: como na Operação Margem Protetora em Gaza (2014).

O segundo corpo, o C4I consiste na Unidade Tecnológica de elite da FDI. A unidade é responsável por toda a defesa cibernética das FDI, o que inclui a reponsabilidade de todas as formas de comunicação das FDI, onde atuam no fornecimento de tecnologia aos militares que estão em campo para o gerenciamento de situações de risco. Conforme mencionado pelo próprio corpo, seu objetivo é "iniciar, desenvolver, explorar e fortalecer o sistema de integração tecnológica da FDI" (IDF, online).

Dentro do plano multidimensional de defesa, o Documento de Defesa Nacional, *The Israel Defense Forces Strategy*, foi divulgado ao público em 2015. Na própria apresentação da doutrina dá-se proeminência às ameaças cibernéticas que são classificadas em "ciberterrorismo associado a grupos não-estatais e de espionagem" (IDF, 2016, p. 2). Outro ponto relevante é a inclusão do ciberespaço como uma quarta dimensão na estratégia de defesa e proteção junto às demais dimensões "reais". Nas palavras do documento: "(...) Defense in all four dimensions (land, sea, air and cyber)." (IDF 2016, 18). Segundo o documento a interpretação do Estado sobre o ciberespaço se define por:

> O ciberespaço se configura como um domínio de combate adicional. Este domínio deve apresentar ações defensivas, ofensivas e de coleta de informações. A capacidade da FDI neste domínio deve ser baseada nos seguintes termos: a) estabelecimento de um cyber arm, o qual servirá de Comando Principal, subordinado ao Chefe do Estado Maior, destinado a operações no ciberespaço; b) desenvolvimento de capacidades tecnológicas de defesa cibernética para as capacidades operacionais e de apoio (pessoal e logística de sistemas). (IDF 2016, 42, Tradução Nossa). [9]

Nesta afirmação retirada do documento, cabe destaque para o termo *cyber arm* — exército cibernético. No qual conforme aponta Barker (2019), se define por um exército que se utiliza de *cyberweapons* — algo difícil de ser definido dado sua atualidade. Para tanto, considera-se que se a guerra cibernética é a extensão de um conflito armado para o ciberespaço, as armas utilizadas também são particulares, tais quais: *malware*, *botnets* e qualquer outro meio que possibilite ataques cibernéticos. A existência de

cyberweapons pressupõe a existência de um ciberarsenal, responsável pela defesa das infraestruturas críticas cibernéticas do Estado (Barker 2019, 5).[10] Conforme demonstrado no documento (IDF 2016, 37), embora não havendo registros de uma divisão de "cyberarm" Israel publicita seu interesse no desenvolvimento de capacidades cibernéticas, que sinalizariam a criação de um *cyber arm*, a partir das suas FDI, sendo elas: utilização para inteligência, responsabilidade logística, investigação e influência cognitiva nas operações, entre outras.

A partir do compilado do setor público e das especificidades desenvolvidas para as Forças Armadas, a partir das quais demonstra-se a relevância que a cooperação tripartite na dimensão ciber assumiu no Estado israelense, cumpre desenvolver as iniciativas e construções responsivas à ciber dimensão que o setor privado desenvolveu.

Setor privado

O setor privado é um pilar fundamental para a cooperação tripartite. Segundo dados do World Economic Forum, Israel ocupa o segundo lugar no ranking dos dez maiores países inovadores do mundo (World Economic Forum Report 2015-2016). Conhecido como a "nação das startups", esse dado corrobora com a quantidade de empresas startups no país. Segundo relatório da CCDCOE existem aproximadamente 360 empresas de cibersegurança e o número de exportações de produtos desenvolvidos beira seis bilhões de dólares (CCDCOE 2017, 16).

A mais importante iniciativa tripartite, com forte presença do setor privado é o *Israel Inovation Cyber Arena*, o *Cyber Spark*. Uma arena de pesquisa em cyber tecnologia localizada no deserto de Bee-Sheva. Embora com investimento do setor privado, a organização é estatal e compõe a cooperação entre o NCB, indústria cibernética e as Universidades de Negev e Ben-Gurion University, especialmente com a implementação de incubadoras (Cyberspark, *online*).

Outra iniciativa, dirigida por diferentes corporações multinacionais foi o estabelecimento de mais de vinte sedes em Israel. Empresas de tecnologias como PayPal, IBM, General Electric, McAfee fazem parte desse pacote. Além disso, a criação do *Israeli Companies Consortium* (IC3), liderado pela indústria aeroespacial israelense, consiste em um grupo composto somente por empresas de cibersegurança, criado em 2016 com apoio do Ministério da Economia (CCDCOE 2017, 16).

Observa-se que ambas as iniciativas são de caráter dual, mesclando os investimentos do setor público e privado. Diante deste vasto cenário de startups de cibersegurança no setor privado, privilegiou-se nessa seção a

apresentação de duas principais iniciativas desenvolvidas, as quais, a partir dos seus relatórios anuais, demonstram o papel que exercem na incorporação do tema ciber na agenda do governo israelense.[11]

Academia

A ligação de Israel com a educação como elemento aglutinador do Estado é presente desde sua autoproclamação. Já no projeto de unificação do exército de Ben-Gurion[12] a educação foi elemento fundamental para o processo de construção das FDI com o estabelecimento de ensino militar nas escolas (Cohen 2008, 31). A partir das décadas de 1950 e 1960 o apoio e investimento às Universidades foi crescente. Esse histórico de investimento estatal na esfera acadêmico-científica é transpassado para a cooperação tripartite na esfera cibernética, a partir da criação de institutos de pesquisa direcionados e incubadoras tecnológicas.

Israel possui atualmente nove Universidades públicas as quais possuem departamentos de computação. Destacam-se nesta seção, institutos com coordenação do NCB, como no caso da Universidade Hebraica de Jerusalém e o *Technion-Israel Institute of Tecnology*, localizado em Haifa. Em 2012 o Ministério de Ciência e Tecnologia priorizou o financiamento de estudos acadêmicos de segurança cibernética dentro do escopo de coordenação do NCB. A iniciativa resultou em acordos de cooperação entre Estado e Universidades para a criação de centros cibernéticos de excelência. O primeiro deles foi o Centro Interdisciplinar de Pesquisa Cibernética (ICRC), na Universidade de Tel Aviv. O ICRC se organiza em três pilares de pesquisa: era da informação; transformação digital e segurança cibernética, e opera na concessão de bolsas de estudos para pesquisadores locais e estrangeiros (IRCS, online).

Cabe ressaltar como elemento da cooperação tripartite que para além da esfera acadêmica universitária, o Estado criou Programas para o nível escolar de ensino: Programa *Magshimim* e *Nitzanei Magshimin*, que incluem na grade curricular a disciplina de segurança cibernética, além de informática como obrigatórias. Ambos os programas além do financiamento partir do Ministério da Educação, também parte das FDI, que vêm objetivando cada vez mais a busca de militares especializados em T.I para atuação em Inteligência.

CONSIDERAÇÕES FINAIS

Este trabalho se propôs a sinalizar os aspectos possíveis de serem mapeados, em virtude da escassez de fonte sobre o assunto anteriormente

justificada, da infraestrutura de defesa israelense em matéria cibernética. Na primeira parte do texto, destacamos que o ciberespaço se insere no espectro das novas ameaças, portanto, considerou-se que no âmbito da guerra, este espaço se caracteriza como um ambiente de combate propulsor ao conflito, que se intersecciona com os ambientes dados como reais nos termos de Ventre (2011), a lembrar: mar, terra, ar e espaço sideral. O que corrobora com o argumento de Barker (2019), ao afirmar que o avanço das atividades cibernéticas propicia uma nova configuração para o conflito, caracterizada pela presença de *ciberweapons* e *ciberarms*. Essa configuração por sua vez, gera uma relação de igualdade de capacidade dos Estados Nação e atores não estatais.

Ainda neste momento buscou-se apresentar os ataques e respostas cibernéticos a Israel no período de 2010 a 2015, tal qual escolhido a partir do ano de fundação do NCB e da influência conjuntural do *worm* Stuxnet. Constatou-se que o âmbito regional israelense se configura por uma correlação de forças estatais e não estatais que não somente operam no espaço real, mas transferem suas capacidades ao operar no ciberespaço. Dado que o ciberespaço não possui fronteiras de poder delimitadas, essa característica amplia a possibilidade de ameaças. Como a principal delas, sem autoria confirmada, destacou-se a criação do *worm* Stuxnet, o qual conforme as evidências demonstram se constituiu como um ponto originário para o fortalecimento de infraestrutura em defesa cibernética por parte do Estado.

No segundo momento, apresentou-se o mapeamento acerca dessa infraestrutura. Constatou-se na pesquisa que ao contrário do esperado, o desenvolvimento de capacidades em ciência e tecnologia agregadas à defesa cibernética não se restringe somente a esfera das FDl, mas sim, tal processo faz parte de um plano de desenvolvimento ousado encabeçado por Estado, setor privado e academia resultado de uma cooperação tripartite, tendo a Resolução 3611 como marco. A seguir, apresenta-se dois quadros conclusivos do mapeamento dos resultados obtidos desta pesquisa sobre a cooperação tripartite:

Quadro 1
Estrutura Tripartite de Defesa Cibernética de Israel

Setor	Organismo	
ESTATAL	AGÊNCIAS ESTATAIS	National Cyber Directorate National Cyber Bureau National Cyber Security Authorithy
	FORÇAS ARMADAS (Forças de Defesa Israelenses)	Computing and Information System School for Computer Professions Unit 8200 C4I Directorate
PRIVADO	Israel Inovation Cyber Arena Israel Aerospace Industries (IAI) Israeli Companies Consortium (IC3) CyberGym[13]	
ACADÊMICO	Technion-Israel Institute of Tecnology (Haifa) Blavtnink Interdisciplinary Cyber Research Centre (ICRC) Israel Inovation Cyber Arena — Universidade de Nege/ Ben-Gurion University Magshimim e Nitzanei Magshimin Programs	

Fonte: Elaboração própria baseada em informações coletadas no site do governo israelense e sites das organizações privadas aqui trabalhadas.

Quadro 2
Documentos e Legislações de referência de Israel

Documento/ Legislação	Ano
Computers Low	1995
Resolução nº. 3.611	2011
Resolução nº 2.443, "Advancing National Regulation and Governmental	2015
Resolução nº 2.444 "Advancing the National Preparedness for Cyber Defense".	2015
Israel Defense Forces Srategy (IDF)	2015
Resolução nº 3.270	2017
Memorandum: Cyber Defense Law and the National Cyber System	2018[14]

Fonte: Elaboração própria baseada em informações coletadas no site do governo israelense.

O quadro 1 sintetiza o mapeamento realizado neste artigo ao apresentar os organismos responsáveis pela esfera cibernética nos âmbitos estatal, privado e acadêmico. Com exceção das FDI que são responsáveis pelo campo tático-operacional de Defesa e possuem suas informações restritas como de Segurança Nacional, todos os demais organismos exercem trans-

parência quanto ao investimento em cibernética. Na criação de tecnologias de inovação como no caso das empresas privadas listadas; no planejamento organizacional da inserção da cibernética como política de Estado como no caso das agências estatais e nos institutos de pesquisa de ensino superior que recebem investimentos público e privado para realização das pesquisas.

O quadro 2, por sua vez, apresenta as legislações de referência do Estado no tema da cibernética. Observa-se que a partir de 2011 o Knesset aprovou três resoluções que foram incorporadas a criação do NCB com suas subdivisões sequentes, sendo a Resolução 3611 seu marco de criação. Tais legislações são um marco de referência importante para que em 2015, com a divulgação do documento de Defesa Nacional, Israel demonstrasse publicamente, especialmente para seu entorno regional de rivalidade, suas intenções em investimento de cibernética para Defesa.

Neste sentido, por meio dos quadros acima apresentados, coaduna-se a dependência das três esferas para desenvolvimento da cibernética em Israel, o qual aponta-se ser um indicativo de cooperação tripartite. O resultado encontrado nesta análise demonstra, portanto, que é imprescindível, que para verificar a posição de destaque de Israel na esfera cibernética, em nível mundial de análise, seja necessária sua investigação a partir das três esferas de maneira conjunta.

Frente ao exposto, conclui-se que Israel, a partir da consolidada cooperação entre Estado, empresas privadas e Institutos de Pesquisa mencionados, se trata de um exemplo de Estado com alta capacidade de defesa cibernética, tanto para fins ofensivos quanto defensivos. Destaca-se ainda, que todos os organismos mencionados estão em atividade, dado que muitas das fontes coletadas se tratam de dados de 2018 e 2019. Ao que tudo indica, se os ditos "*cyberarms*" são o futuro, Israel lançou sua cartada no passado e a está lançando no presente.

REFERÊNCIAS

Barker, Ken. 2019. "Cyber attack: what goes around comes around". *The School of Public Policy Publications. SPP Briefing Paper* 12, no. 17. Canadian Global Affair Institute Institute. University of Calgary.

Blavatnik Interdisciplinary Cyber Research center, ICRC. *Activity Report: 2014-2016*. https://icrc.tau.ac.il/home.

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

Cohen, Matthew S., Charles Freilich, and Gabi Siboni. 2015. "Israel and Cyberspace: Unique Threat and Response". *International Studies Perspectives*: 1–15 (December).

Cohen, Stuart A. 2008. *Israel and its Army: from cohesion to confusion*. New York: Routledge.

Fildes. Jonathan. 2010. "Stuxnet *Worm* 'targeted high-value Iraninan Assets'". *BBC News* (Setembro). https://www.bbc.com/news/technology-11388018.

Hinnebusch, Raymond. 2003. *The International Politics of the Middle East*. Manchester; Nova York: Manchester University Press.

Israel Cyber Police Portal. *Cyber Security Policy*. http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf.

Israel Defense Forces. IDF. 2016. *C4I and Cyber Defense Directorate*. Disponível em> <https://www.idf.il/en/minisites/c4i-and-cyber-defense-directorate/> Acesso: junho de 2019.

Israel National Cyber Directorate. 2016. *The Government Services and Information Website — Gov.il* . https://www.gov.il/en/Departments/israel_national_cyber_directorate.

Israel. 2016. *The Israel Defense Forces Strategy*. Translation by Susan Rosenberg. Research Assistance by Henry Rome.

Israeli Cyber Innovation Arena. 2019. *Cyberspark*. http://cyberspark.org.il/.

Kuehl, Daniel. 2009. *From Cyberspace to Cyberpower: defining the problem*. In *Cyberpower and National Security*, edited by Franklin Kramer, Starr Stuart, and Larry Wentz: 24–42. Duller: National Defense University Press.

Milevski, Lukas. 2011. *Stuxnet and Strategy: A special operation in cyberspace?* 63 (4th quarter): 64–9.

Pitts, Vanessa. 2017. *Cyber Crimes: History of World's Worst Cyber Attacks*. Alemanha: Alpha Editions.

Raska, Michael. 2015. *Confronting Cybersecurity challenges: Israel's envolving cyber Defence Strategy. Policy Report. S. Rajaratnam School of International Studies*. Nanyang Technological University (NTU). Singapore.

Symantec Cooportation (NASDAQ: SYMC). *W.32. Stuxnet.* https://www.symantec.com/security-center/writeup/2010-071400-3123-99.

Tabansky, Lior. 2016. *Towards a Theory of Cyber Power: The Israeli Experience with Innovation and Strategy.* 8th International Conference on Cyber Conflict. Tallinn: NATO CCDCOE Publications.

Ventre. Daniel. 2011. Ciberguerra. In: *Academia General militar. Seguridad global y potências emergentes em um mundo multipolar.* XIX Curso Internacional de Defensa. Espanha: Universidad Zaragoza.

World Economic Forum Report 2015-2016. *The Most Inovatives Countries in the World*, https://www.weforum.org/agenda/2016/11/the-most-innovative-countries-in-the world/.

NOTAS

1. Este texto foi desenvolvido como parte da pesquisa vinculada ao Pró-Defesa IV: "Ciência, Tecnologia e Inovação em Defesa: cibernética e defesa nacional".
2. Israel enfrenta um cenário de legitimidade contestada no seu entorno desde sua fundação, 1948, até aos dias atuais. Conforme relatório apresentado pelo CSIS (2003), o Médio Oriente é a região mais militarizada do mundo, por possuir: alta porcentagem de gasto em armamento por país, alta porcentagem de exportação de armas de grande porte, proliferação nuclear, guerra assimétrica, guerra proxy, presença de atores não estatais, coalizações externas e regionais e guerra de informação.
3. Cabe destacar a discussão presente na literatura que considera o ataque preliminar ao Stuxnet, ocorrido na Geórgia, em 2008, reconhecido como o primeiro ataque que coincidiu em uma guerra real, no entanto, sem possibilidade de consequências nucleares imediatas.
4. No original: *"The Stuxnet malware, in the context of international sanctions, ultimately has not affected Iranian political will to a sovereign nuclear program or Iranian capabilities sufficiently that their goal cannot be pursued regardless of intent. What would a strategically successful Stuxnet look like? That sort of attack would have to be destructive enough to at least leave a permanent mark on Iranian capabilities by overwhelming the material redundancy available to their nuclear programs. It would also have to be able to overcome increased Iranian nuclear efficiencies. Such success may be possible, since malware such as Stuxnet has one significant advantage over physical special operations: unlike actual people, a program can be in multiple places at once — hundreds of thousands, millions, or more — if necessary"*.
5. Importante ressaltar que os ataques à Israel são realizados, em sua maioria, no mesmo período das Operações Militares lideradas pelas Forças de Defesa Israelense (FDI), no território da Faixa de Gaza. No entanto, esse fato não é uma regra. Conforme apontam Cohen, Freilch e Siboni (2015), algo interessante a ser notado no rastreamento dos ataques contra Israel é que nem sempre há uma motivação direcionada a um período ou acontecimento, mas sim a motivação geral é a desestabilização interna do país para um "cessar fogo" de suas políticas ofensivas.
6. O Objetivo da operação era a destruição do armazenamento de armas e túneis subterrâneos do Hamas utilizados para romper o bloqueio da Faixa de Gaza. Por ser realizada no âmbito urbano, as consequências foram um índice extremo de baixas de palestinos, que não ocorria desde as Intifadas da década de 1980.
7. Poder que se manifesta no espaço cibernético.
8. O mapeamento aqui apresentado foi feito a partir do levantamento minucioso de relatórios das próprias agências estatais israelenses, institutos de pesquisa e empresas privadas. No entanto, ressalta-se que o material di-

vulgado ao público sobre as políticas israelenses em matéria de defesa cibernética é bastante escasso, dado que muitas informações são restritas ao Estado, o que denota o cuidado e a importância que Israel atribui ao tema.

9. No original: *"The cyberspace is an additional combat domain. This domain shall feature defensive, intelligence gathering and offensive actions. IDF force buildup in this domain shall be based on the following: a. Establishing a Cyber Arm, which will serve as a Principal Command, subordinate to the Chief of the General Staff, for operations and force buildup of the IDF's cyberspace capabilities. It will be in charge for planning and implementing the cyber domain campaign.b. Development of technological capabilities for cyber defense for the operational capabilities and for supporting capabilities (personnel, logistical systems)".*
10. A discussão sobre "cyberarsenal" é incipiente. A dificuldade está na categorização e diferenciação entre arma cibernética e arma eletrônica. Para mais informações, ver Barker (2019).
11. Cabe mencionar nesta seção a dificuldade em separar as startups que são direcionadas especificamente para defesa nacional, visto que em todas as fontes trabalhadas menciona-se apenas a esfera de cibersegurança. Um apontamento por parte das autoras infere essa configuração como uma opção estratégica do Estado, inserida no campo tático-operacional de Defesa, o qual possui, portanto, informações restritas como de Segurança Nacional.
12. No projeto de unificação do exército Nacional de Ben-Gurion (1948) as Forças militarizadas judaicas presentes no território desde o Mandato Britânico (Haganah) unificam-se em um exército nacional, as FDI.
13. Nessa rede de startups se incluem cerca de 360 companhias especializadas em cibersegurança. Para mais informações consultar: https://www.startupnationcentral.org/.
14. Em progresso, sujeito à aprovação do Parlamento.

ISRAEL E DEFESA CIBERNÉTICA: ESTUDO DA VINCULAÇÃO ESTADO, SETOR PRIVADO E ACADEMIA

RESUMO

O contínuo avanço das tecnologias de informação e comunicação intensificou o desenvolvimento de um espaço complexo, o ciberespaço, o qual se tornou objeto referente de securitização, proveniente da vinculação entre Estado, corporações privadas e sociedade civil. Em face deste cenário, os Estados passam a compreender a esfera cibernética como uma ameaça contemporânea existencial, necessitando o desenvolvimento de medidas de infraestrutura de defesa, como no caso de Israel. Busca-se neste artigo analisar quais são as medidas tomadas pelo Estado israelense em termos de infraestrutura de defesa cibernética. A metodologia empregada será de técnica de pesquisa de revisão bibliográfica, a partir de fontes primárias, que compreendem uma inicial análise do documento de defesa nacional (publicado ineditamente em 2015) e demais marcos de referência, bem como fontes secundárias. Como conclusões preliminares, infere-se que Israel atribui prioridade para o setor cibernético em seu plano de defesa multidimensional, tendo uma infraestrutura de defesa formulada a partir da cooperação tripartite entre Estado, setor privado e academia, condicionada devido à sua específica dinâmica regional securitária de legitimidade contestada com presença efetiva de ameaças cibernéticas de fontes não tradicionais e tradicionais.

Palavras chave: Israel; Defesa Cibernética; Política de Defesa.

ABSTRACT

The rise of ICTs (information and communication technology) has intensified the development of cyberspace research in International Politics in the last years. Cyberspace became an object of securitization, that includes State, private corporations, and civil society. In this way, States began to recognize the cyber sphere as a contemporary threat, which demanded the development of a qualified defense infrastructure by them. This research seeks to understand the measures taken by Israel in its cyber defense infrastructure. The following methodology applied includes bibliographic reviews (primary and secondary sources which includes the preliminary analysis of the national defense document published for the first time in 2015). In the end of the article, we apply as some conclusions, that Israel allocates priority to the cyber sector, by having a defense infrastructure formulated from tripartite cooperation between the State, the private sector and the academic sector, as a part of its multidimensional defense plan. We assume that this situation is related to the regional security context of Israel in Middle East, defined by a contested legitimacy and the existence of cyber threats from non-traditional and traditional actors.

Keywords: Israel; Cyber Defense; Defense Policy.

Recebido em 30/06/2020. Aceito para publicação em 20/04/2021.