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

Júlia Loose[1]
Graciela de Conti Pagliari[2]

O artigo propõe analisar quais são as medidas tomadas por Israel em termos de infraestrutura de defesa cibernética. O objetivo principal é apresentar os elementos que compõe a infraestrutura de defesa cibernética do Estado judeu, bem como sua evolução, e para este feito, busca-se analisar os documentos e marcos de referência em matéria cibernética, incluindo o estudo do atual documento de defesa nacional divulgado em 2015, *The Israel Defense Forces Strategy (2015)*, quanto à interpretação do Estado em relação ao ciberespaço e construção de capacidades tecnológicas militares. Como hipótese preliminar, consideramos que Israel atribui prioridade para o setor cibernético em seu plano de defesa multidimensional, tendo uma infraestrutura de defesa composta pela consolidada cooperação tripartite entre Estado, setor privado e academia. Prioridade a qual, conforme será demonstrado 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.

Muitos temas que hoje são quase inerentes ao processo de socialização humana passaram a receber atenção no espectro das ameaças de segurança. O avanço da tecnologia de informação e comunicação (TIC's) e a popularização do acesso à internet criaram processos inseridos em um ambiente complexo por sua natureza e até então obscuro nas discussões das Relações Internacionais, no qual todos estão inseridos de alguma forma: o espaço cibernético. 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.

A literatura apresenta diferentes definições do ciberespaço, muitas ainda em desenvolvimento, e muitas são interpretativas, de modo que não há um consenso.

[1]Doutoranda do Programa de Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina. Bolsista da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). *E-mail:* loose.jl@gmail.com
[2]Professora Dra. da Universidade Federal de Santa Catarina. Pesquisadora e Vice-líder do Grupo Brasil e as Américas. *E-mail:* graciela.pagliari@gmail.com.

Para Kuhel (2009), 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” (KUEHL, 2009, p. 29). Por sua vez, Ventre (2011), identifica que “o ciberespaço é representado em três camadas: camada inferior: infraestrutura (hardware); camada intermediária (software) e a camada superior cognitiva” (VENTRE, 2011, p. 34). A essência da definição de Ventre (2011) é a característica de transversalidade do ciberespaço entre os espaços virtual e real. Terra, ar, mar e espaço sideral fazem parte do espaço real e são compostas pela existência de sistemas de telecomunicações, internet, infraestrutura, ordenadores, IP’s, etc. Na dimensão virtual encontra-se o ciberespaço – é quando essas duas dimensões se entrelaçam e interagem que ocorrem os ataques cibernéticos. Quando essa dimensão se insere em um conflito armado que ocorre a Guerra Cibernética (VENTRE, 2011).

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 – como no caso do Stuxnet. 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, p. 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) 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 (BARKER, 2019, p. 4). 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, p. 4). Esse elemento na configuração da guerra cibernética

interessa a esta proposta, dado que Israel pertence a um entorno regional caracterizado pela alta presença relativa de atores não estatais.

Israel enfrenta um cenário de legitimidade contestada no seu entorno desde sua fundação, 1948, até aos dias atuais. Autodeclarado como um Estado judeu, em meio a um "núcleo árabe fragmentado em múltiplos territórios" (HINNEBUSCH, 2003, p. 3), o investimento do Estado 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 dois mil, especialmente após seu suposto envolvimento no caso do *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. Quanto a primeira, Israel enfrentou ataques em sua maioria protagonizados pelo Irã, mas também por Turquia, África do Sul, Rússia e China (COHEN, FREILCH E SIBONI, 2015). Quanto aos atores não estatais estabelece-se o recorte de grupos armados não estatais, sendo os principais Hezbollah (sede no Líbano) e Hamas, (sede na Palestina), e a atuação da sociedade civil, que se inclui nesse processo por meio da atuação de Hackers ativistas.

O caso do worm Stuxnet representou em nível internacional um alerta para os Estados investirem em tecnologia cibernética. No cenário israelense, nesse mesmo contexto, foi criado em 2011 o National Cyber Boureau (NCB), 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 no meio. 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 E SIBONI 2015, p. 4).

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 (COHEN, FREILCH E SIBONI 2015).

A partir dos dados divulgados pelo NCB, estima-se que Israel sofre ataques com origem de grupos estatais e não-estatais, os quais o país aponta serem lideradas

pelo Irã, Hezbollah e Hamas. Em 2011, Israel acusou o Irã de liderar a Operação “Newscaster” contra Israel 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 (2013), 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 E SIBONI 2015, p. 4).

1. RESULTADOS OBTIDOS

Israel é reconhecido mundialmente pelo seu envolvimento com tecnologias de inovação, fomento à pesquisa científica 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 judeu ocupou o segundo lugar de liderança dos gastos (como porcentagem do PIB nacional) em pesquisa e inovação tecnológica, conforme aponta o relatório desenvolvido no CCDCOE. Estão incluídos nesse processo de desenvolvimento, a instalação de tecnologias avançadas de infraestrutura de comunicação, que incluem além de cabos fixos, a construção de fibra ótica (CCDCOE, 2017, p. 6).

Conforme aponta Tabanksy (2016), o alto investimento em tecnologia sob iniciativa do Estado, fez com que o país se utilizasse de cyber poder na aplicação do *hard power* e dissuasão da sua política defesa, especialmente frente ao Irã nuclear. No que tange o investimento de tecnologia cibernética para defesa nacional, Tabansky (2016) 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 (TABANSKY, 2016, p. 51). A seguir, apresenta-se o resultado obtido da pesquisa com o mapeamento deste investimento a partir da sua consolidada estrutura tripartite de defesa cibernética composta por Estado, Setor Privado e academia.

Quadro 1: Estrutura Tripartite de Defesa Cibernética Israelense

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[3]	
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.

Quadro 2: Documentos e Legislações de referência de Israel

DOCUMENTO/ LEGISLAÇÃO	ANO
Computers Low	**1995**
Resolução No. 3611	**2011**
Resolução No. 2443, “Advancing National Regulation and Governmental	**2015**
Resolução No. 2444 “Advancing the National Preparedness for Cyber Defense”.	**2015**
Israel Defense Forces Srategy (IDF)	**2015**
Resolução No. 3270	**2017**
Memorandum: Cyber Defense Law and the National Cyber System	**2018**

Fonte: Elaboração própria.

REFERÊNCIAS BIBLIOGRÁFICAS

BARKER, Ken. Cyber attack: what goes around comes around. **The School of Public Policy Publications. SPP Briefing Paper. Vol. 12:17.** Canadian Global Affair Institute Institute. University of Calgary. 2019.

[3]Na grande rede de star-ups israelenses se incluem cerca de 360 companhias especializadas em cibersegurança. Para mais informações consultar: <https://www.startupnationcentral.org/>.

BLAVATNIK INTERDISCIPLINARY CYBER RESEARCH CENTER, ICRC. **Activity Report: 2014 – 2016.** Disponível em: < https://icrc.tau.ac.il/home> Acesso, julho de 2019.

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

COHEN, Matthew S. FREILICH, Charles. SIBONI, Gabi. Israel and Cyberspace: Unique Threat and Response. **International Studies Perspectives.** December 29, 2015. 0, 1 – 15. 2015.

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

HINNEBUSCH, Raymond. **The International Politics of the Middle East.** Manchester University Press. Manchester e Nova York. 2003.

ISRAEL CYBER POLICE PORTAL. **Cyber Security Policy.** Disponível em: <http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advanci ng%20National%20Cyberspace%20Capabilities.pdf> Acesso: Junho de 2019.

ISRAEL DEFENSE FORCES. IDF. **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. **The Government Services and Information Website – Gov.il**. Disponível em: <https://www.gov.il/en/Departments/israel_national_cyber_directorate> Acesso: Abril de 2019.

ISRAEL. **The Israel Defense Forces Strategy.** Translation by Susan Rosenberg. Research Assistance by Henry Rome Design & Layout by Andrew Facini, President and Fellows of Harvard College. Printed in the United States of America. 2016.

ISRAELI CYBER INNOVATION ARENA. **CYBERSPARK.** Disponível em: <http://cyberspark.org.il/> Acesso: Junho de 2019.

KUEHL, Daniel. From Cyberspace to Cyberpower: defining the problem, In: KRAMER, Franklin; STUART, Starr; WENTZ, Larry. **Cyberpower and National Secutiry.** Duller: National Defense University Press, p. 24 – 42, 2009.

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

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