以色列的网络安全问题及其治理*

艾仁贵

【内容提要】 网络安全威胁是当今国际社会普遍面临的主要威胁之一。受地缘政治与国际局势的影响，以色列成为遭受网络攻击最为频繁的国家之一。由于长期遭受网络攻击的威胁，以色列在国际社会中较早重视网络安全问题，建立了一系列网络安全应对机制。2010－2011 年是以色列加强国家网络安全建设的重要时间节点，以《2010 国家网络倡议》和以色列政府第 3611 号决议两个具有里程碑意义的文件为代表，以色列政府将制定国家网络战略提上议事日程。在国家网络局的统筹规划下，通过政府机构、军情部门、学术界、产业界等之间的密切合作，以色列构建了一整套较为健全的网络安全维护机制，不仅有效治理了网络安全问题，而且通过与技术研发相结合形成了科学合理的网络安全生态系统，蓬勃发展的网络安全产业也带来了可观的经济效益。作为全球网络安全领域的引领者之一，以色列在网络安全治理上积累了较为丰富的经验，并具备一定的网络战实战能力，值得其他相关国家学习和借鉴。

【关键词】 以色列网络安全治理；2010 国家网络倡议；国家网络战略；网络技术研发

【作者简介】 艾仁贵，河南大学以色列研究中心副教授，博士（开封 邮编：475001）。

【DOI】 10.14093/j.cnki.cn10-1132/d.2017.02.004

【中图分类号】 D815.5 【文献标识码】 A 【文章编号】 2095-574X（2017）02-0066-24

* 本文为国家社科基金重大项目“犹太通史”（项目批准号：15ZDB060）、河南省高等学校哲学社会科学创新团队支持计划“犹太－中东史”创新团队（项目批准号：2013-CXTD-01）的阶段性成果。感谢《国际安全研究》匿名评审专家和编辑部给予的中肯修改意见，文中存在的疏漏由作者负责。

20 世纪 90 年代以来，随着信息化和全球化的不断发展，互联网与每个公民个体、国家、国际组织乃至整个国际社会密切相关，几乎渗透到全球各个角落，网络也成为地球村的核心维系纽带。网络在当今国际安全领域是一个十分高频的词汇，网络安全也成为国际政治中一项备受关注的重要议题。特别是近年来一系列由网络安全引发的信息泄露事件，例如斯诺登事件、维基解密事件等，都充分体现了网络安全对于国际政治的极端重要性。在当前许多关键设施都已信息化、对网络的依赖程度越来越高的情况下，与实体世界一样，作为虚拟空间的网络世界也成为各方势力争夺的重要对象。从构建国家安全的维度来看，网络安全是国家总体安全体系中必不可少的重要一环，其应对、处理得好坏直接影响到其他安全领域的维护和巩固。以色列作为举世公认的网络安全强国，在网络安全领域有着世界领先的地位，其网络安全治理的经验和启示值得总结。① 本文拟对以色列的网络安全问题及其治理进行分析，具体围绕以色列面临的网络安全威胁、以色列社会对网络空间的认识、以色列的国家网络政策与国家网络安全战略、以色列网络安全的治理路径等方面展开，以期为其他相关国家的网络安全治理提供若干借鉴及启示。

一 以色列网络安全问题的表现形式及其特点

互联网是一把双刃剑，一方面为国家和民众生活带来了巨大的便利，另一方面也成为极端势力和恐怖势力用于从事恐怖活动的平台。网络和社交媒体对中东地区有着十分重大的影响，尤其在 2011 年初以来席卷整个中东地区的“阿拉伯之春”中发挥了重要作用，成为局势演变的关键推手。根据《阿拉伯社交媒体报告 2015》的研究，Facebook、Twitter、YouTube、Instagram 等网络和社交媒体在中东地区的使用率高达 80% 以上。② 受地缘政治与国际局势的影响，当前以色列遭受的网络安全威胁不断加剧，面临着网络恐怖主义的常态化攻击。据有关部门统计，以色列是遭受网络攻击最为频繁的国家之一，每天遭受大约 10 万次的网络

① 有关以色列的网络安全问题，最近成为国际学术界关注的热点问题。有关的重要研究，参见 Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts and Strategic Trends*, Tel Aviv: Institute for National Security Studies, 2012; Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel*, New York: Springer, 2015; Gabi Siboni and Ofer Assaf, *Guidelines for a National Cyber Strategy*, Tel Aviv: Institute for National Security Studies, 2016, etc。国内学者多数集中于以色列的传统安全领域，通常对其网络安全问题缺乏关注。

② *Arab Social Media Report 2015*, Dubai: Arab Social Media Influencers Summit, 2015, pp. 3-4.

攻击，平均每分钟就要遭受约 70 次网络攻击。[①] 当前，以色列遭受的网络安全威胁主要来自境内激进分子、周边政治对手和国际反以组织或个人，他们对以色列目标发动网络攻击或进行网络恐怖煽动，从而对以色列的关键设施（水、电、交通、通信、金融等）、军情机构以及其他严重依赖计算机的部门都带来了巨大的风险，网络威胁也被以色列政府列为四大主要安全威胁之一。[②]

境内激进分子的网络恐怖煽动，是当前以色列面临的重要安全威胁之一。巴以之间长期的冲突对抗，助长了针对以色列的网络攻击活动。以 2014 年夏的“护刃行动”为例，根据有关机构的统计，“护刃行动”期间，针对以色列的网络攻击较平时增长了近十倍以上，这些攻击不仅来自哈马斯，也来自其他阿拉伯和伊斯兰国家。[③] 以色列电力公司董事会主席伊夫塔克·罗恩－塔勒（Yiftach Ron-Tal）指出，“护刃行动”期间，该公司的服务器以及基础设施每天遭受的黑客攻击多达近百万次。罗恩－塔勒说：“如果我们把网络受袭的次数比作哈马斯在战争中向我们发射的导弹数量，那么以色列电网在 2013 年每天都会遭到两枚‘网络导弹’的轰炸，全年无休。2014 年，其数量则增至每天 15 枚。”他还补充道，一颗导弹充其量只能摧毁一个目标，而“直接命中”电网则会击垮整个国家。[④] 此外，不少巴勒斯坦人以 Facebook、Twitter、YouTube 等网络和社交媒体为平台，推送许多煽动性文字和视频鼓动对以色列人发动恐怖袭击。一些媒体将巴勒斯坦人借助网络发动针对以色列的抵抗和恐怖袭击的行为称为“电子因提法达”（Electronic Intifada）、“网络因提法达”（Cyber Intifada）。在 2015 年 9-10 月以色列遭受恐怖袭击浪潮时期，网络煽动发挥了十分重要的作用。[⑤]

就周边地区而言，当前以色列遭受的网络攻击主要来自伊朗、叙利亚、黎巴嫩真主党等传统地缘政治对手，还包括沙特阿拉伯和土耳其，这些周边的国家或组织具有较强的网络攻击能力，对以色列的网络安全带来了较大的威胁。在中东

---

① Yoni Kempinski and A7 Staff, “Expert: Israel Faces 100,000 Cyber Attacks Each Day,” *Israel National News*, June 16, 2013, http://www.israelnationalnews.com/News/News.aspx/168969.

② Matthew S. Cohen, Charles D. Freilich and Gabi Siboni, “Israel and Cyberspace: Unique Threat and Response,” *International Studies Perspectives*, Vol. 17, No. 3 (August 2016), p. 311.

③ Cyber Nation Staff, “Cyber Attacks on Israel Grew by 900%: The Other Side of Operation Protective Edge,” *CyberNation*, July 17, 2014, http://www.cybernation.co.il/featured/cyber-attacks-on-israel-grow-by-900/.

④ ［以］大卫·沙曼：《以色列电网日抗百万黑客攻击》，载《以色列时报》2015 年 3 月 25 日，http://cn.timesofisrael.com/以色列电网日抗百万黑客攻击/。

⑤ 有关网络煽动与 2015 年以色列恐怖袭击浪潮的关系，参见艾仁贵：《2015 年以色列安全形势报告》，载张倩红主编：《以色列发展报告（2016）》，北京：社会科学文献出版社 2016 年版，第 102-106 页。

国家中，伊朗具备较强的网络攻击能力，伊朗建立了最高网络空间委员会（The Supreme Cyberspace Council）、国家网络中心（The National Cyber Center）和网络空间防御司令部（The Cyberspace Defense Command），并在革命卫队下设专门的网络部队（Iran's Cyber Army）。[①] 2011 年，伊朗发动了以美国、以色列及其他西方国家政府网站为目标的“纽卡斯特”（Newcaster）网络攻击，有超过 2 000 台计算机遭到攻击；2014 年加沙冲突期间，在所有针对以色列的网络攻击中，来自伊朗的攻击有了大幅增长。[②] 有媒体强调，核武器和网络攻击是伊朗最让以色列忌惮的两大对象，后者甚至比前者更危险。[③] 由于伊朗与叙利亚、黎巴嫩真主党、哈马斯的密切关系，以色列政府指责伊朗是针对以色列的网络攻击的“幕后黑手”，内塔尼亚胡在特拉维夫举办的第四届国际网络安全大会上强调，“在针对以色列发动的网络攻击的背后势力中，首先和最主要的就是伊朗。”[④] 成立于 2011 年的叙利亚电子军（Syrian Electronic Army）在中东地区具有较高的知名度，被称为是“阿拉伯世界首支有能力发起网络攻击的信息化部队”。[⑤] 2013 年 5 月，叙利亚电子军对以色列第三大城市海法的供水系统进行了网络攻击，以作为对以色列空袭大马士革目标的回应，但没有获得成功。[⑥] 通过与伊朗、叙利亚的密切关系，黎巴嫩真主党也制订了自己的网络战计划（Cyber Warfare Program），其主要目的就是对以色列北部地区的关键设施发动网络攻击。此外，以色列也不时遭到来自沙特阿拉伯等其他周边国家的网络攻击。2012 年 1 月，一名代号为“0xOmar”的沙特阿拉伯黑客对特拉维夫证券交易所、以色列航空公司和以色列主要的信用卡公司等机构发起网络攻击，声称获取了 40 万个以色列信用卡账户信息，而以色列方

① Gabi Siboni and Sami Kronenfeld, “Iran and Cyberspace Warfare,” in Gabi Siboni, ed., *Cyberspace and National Security: Selected Articles*, Tel Aviv: Institute for National Security Studies, 2013, p. 91.

② Matthew S. Cohen, Charles D. Freilich and Gabi Siboni, “Israel and Cyberspace: Unique Threat and Response,” *International Studies Perspectives*, Vol. 17, No. 3 (August 2016), pp. 310-311.

③ “Report: Iranian Cyber Threat Will Pose Greater Danger than Nuclear Program,” *Ynet News*, March 28, 2015, http://www.ynetnews.com/articles/0,7340,L-4641788,00.html.

④ Tovah Lazaroff, “Netanyahu: Iran behind Cyber Attacks on Israel,” *The Jerusalem Post*, September 14, 2014, http://www.jpost.com/Israel-News/Watch-Live-Netanyahu-addresses-cyber-security-conference-375290.

⑤ Ahmed K. Al-Rawi, “Cyber Warriors in the Middle East: The Case of the Syrian Electronic Army,” *Public Relations Review*, Vol. 40, No. 3 (September 2014), pp. 420-428.

⑥ Gil Ronen, “Syrian Cyber-Attack on Haifa Water System,” *Israel National News*, May 25, 2013, http://www.israelnationalnews.com/News/News.aspx/168306.

面回应称有大约2万个账户信息被泄露。①

就全球范围来说，针对以色列的网络攻击主要来自国际反犹、反以组织和个人，一些国际黑客组织对以色列的政府机构和基础设施频繁发起攻击。在对以色列发动网络攻击的国际组织中，最具影响的就是著名黑客团体“匿名者”（Anonymous）所发起的“打倒以色列行动”（#OpIsrael campaign），该行动指反对以色列团体和个人，对以色列网站发动的联合网络攻击，其主要形式有攻占官方机构网站、泄露数据库数据等。该行动首次出现于2012年11月的加沙冲突期间。2013年4月7日，正值以色列纪念大屠杀烈士和英雄纪念日，“匿名者”号召将以色列从因特网上抹去，发动对以色列的“电子大屠杀”（the electronic holocaust），② 其攻击目标包括以色列总统和总理的官方网站、以色列银行、以色列国防军及以色列驻美国大使馆网站等，导致以色列3万个银行账户和10万个网站遭到攻击，据称造成了20亿美元的损失，5 000名以色列官员的个人信息（包括姓名、身份号码和电子邮件地址）被泄露。③ 不仅如此，该组织还公开向以色列宣战，把每年的4月7日作为“电子大屠杀”纪念日，宣称将于这一天对以色列的服务器、政府网站、军事网站、银行、公共设施等发起网络攻击。④ 此外，随着网络时代的发展，反犹主义也出现了新的形式，在网络上煽动反犹反以情绪的“在线反犹主义”（Online Anti-Semitism）流行开来，这些反犹言论主要通过网络的方式得到快速的传播，对以色列的外部形象造成了严重的破坏。⑤

---

① Gianluca Mezzofiore, “‘Nightmare’ 0xOmar Hackers Attack Israel’s Stock Exchange and El Al,” *International Business Times,* January 16, 2012, http://www.ibtimes.co.uk/nightmare-hackers-attack-israel-s-stock-exchange-282255.

② David Gilbert, “OpIsrael: Israel Prepares to be ‘Wiped off the Internet’,” *International Business Times,* April 5, 2013, http://www.ibtimes.co.uk/opisrael-israel-prepares-wiped-internet-anonymous-cyber-453943.

③ “Anonymous Launches Massive Cyber Assault on Israel,” *RT News,* April 8, 2013, http://www.rt.com/news/opisrael-anonymous-final-warning-448/.

④ Jack Moore, “Hacker Group Anonymous Threatens Israel with ‘Electronic Holocaust’,” *News Week,* March 31, 2015, http://www.newsweek.com/hacker-group-anonymous-threaten-israel-electronic-holocaust-317729.

⑤ 据反对反犹主义全球论坛（Global Forum for Combating Antisemitism）2016年初发布的报告——《对憎恨的估量：社交媒体中的反犹主义状况》（*Measuring the Hate: The State of Antisemitism in Social Media*），Facebook、Twitter、YouTube等社交媒体成为发表有关反犹言论的主要渠道，通过对这三大代表性社交媒体的统计分析，其反犹言论可以归纳为：传统的反犹主义（例如阴谋论和种族歧视）占49%、新反犹主义（将反犹主义与反以色列相结合）占34%、否认纳粹大屠杀占12%、煽动暴力（包括有关犹太人去死的言论）占5%，而且这些煽动性内容被移除的比例较低、移除的时间也滞缓。参见 Andre Oboler, *Measuring the Hate: The State of Antisemitism in Social Media,* Melbourne: Online Hate Prevention Institute, 2016, p.7。

由于网络安全威胁是信息化条件下的新现象，它具有与此前传统安全威胁相比所不具备的特点。就以色列的情况而言，其网络安全威胁呈现出以下新特点：第一，攻击来源更加多样。大部分针对以色列的网络攻击并不来自加沙地带或约旦河西岸，而主要来自以色列国境数千公里之外的地区，例如摩洛哥、伊朗、俄罗斯、印尼等地，这对以色列的网络安全带来了巨大的不确定性。第二，攻击对象更加广泛。不仅是军事部门和政府关键设施，而且普通公民的资料或信用卡账户也成为攻击对象。第三，攻击手段更加复杂。对以色列的网络攻击，不仅是单纯地对以色列网站进行攻击，而且也对以色列的水、电等关键设施进行攻击，此外还借助网络或社交媒体煽动恐怖活动。第四，攻击后果更加严重。对以色列发动的网络攻击，导致大批信息泄露或关键设施遭到破坏。第五，攻击时间具有阶段性，它与传统安全威胁存在一定的同步性。每当巴以冲突激烈时，对以色列的网络袭击往往成倍地增长。网络安全威胁与传统安全威胁有着密切的联系，两者的根源基本相同，都是由于政治和意识形态的对立所致，可以说，网络安全威胁是传统安全威胁在另一种形式上的延伸。

二 “第三次革命”：以色列社会对网络空间的认识

随着信息化时代的不断发展，网络作为虚拟空间与人们的工作生活越来越密不可分。在信息化条件下，许多国家和民众都过度依赖计算机系统，对网络空间依赖程度的不断增长，由此导致的网络安全问题也随之滋生。网络攻击包括摧毁基础设施系统（水、电、交通、通信、金融等）、窃取数据库、关闭重要服务、电脑病毒乃至破坏军事目标和卫星等国家设施等等。可以说，网络变得越来越重要，如今它已成为继陆地、海洋、天空和太空之后的第五大领域。[①] 而且，与传统的陆地、海洋、天空和太空等领域不同，在网络空间里不再有边界和距离的概念。许多国家都意识到，网络空间成为新的争夺领域，在该领域发生的战争被称为网络战，它完全不同于传统战争，无需弹药就可以摧毁对方的关键设施，从而取得战争的决定性胜利。由于网络攻击的空前破坏力，对网络防御的要求也就随之提高，亟需加强对于网络安全重要性的认识。

由于与众多的阿拉伯国家几乎持久地处于敌对状态，而且以色列存在人口与

① Larry D. Welch, “Cyberspace: The Fifth Operational Domain,” *IDA Research Notes,* Summer 2011, p. 1; Gabi Siboni and Ofer Assaf, *Guidelines for a National Cyber Strategy,* Tel Aviv: Institute for National Security Studies, 2016, p. 15.

疆域规模上的巨大劣势，以色列要想生存和发展必须依靠技术，通过技术优势来弥补人口和疆域的劣势。因而自建国之初起，技术就在以色列的国家安全体系中占有十分重要的地位，“以质取胜”“以少敌多”成为以色列国家安全的核心概念之一。[①] 20 世纪 90 年代以来，以色列对网络这个新的技术领域给予了前所未有的重视。以色列社会主流精英将网络视为“第三次革命”，强调必须牢牢把握第三次革命的主动权，以色列著名网络战略家埃维塔尔·马塔尼亚（Eviatar Matania）强调，网络是一场人类革命：“我们认为，网络革命是继农业革命、工业革命之后的第三次革命，它正在彻底地改变我们所有人的生活”。[②] 以色列政界普遍对网络空间给予了高度的关注，内塔尼亚胡总理是其中的主要代表，自他执政以来，以色列政府将网络安全提升至空前的高度。内塔尼亚胡指出：“网络威胁可以使许多国家陷于瘫痪，这种战略威胁对许多领域的瘫痪和伤害力度丝毫不比其他威胁小，我们必须在国家和国际层面上对其做好准备。”[③]

不少以色列军事人员认为，网络战与以色列的军事信条十分契合，因为两者都特别注重先发制人、御敌境外，使小国可以发挥大国的威力。以色列军事情报局局长阿摩司·亚德林（Amos Yadlin）少将 2009 年在一次公开演讲中强调，“网络战非常适合以色列”，这是以色列军方首次公开承认网络空间对于军事的重要性：“网络对于今天的战争极端重要，正如空中支持的出现对于 20 世纪的战争一样。网络结合了军事维度的所有要素：情报搜集、防御和进攻……网络空间能够给予弱小的一方获得曾经只有超级大国才有的能力……比如借助无人驾驶机（网络部队）可以实施打击……无需冒着人员伤亡的风险。在网络领域，一切都可以自己制造而无需外国帮助，而且年轻的以色列人对这个领域非常熟悉。”[④] 继阿摩司·亚德林之后出任以色列军事情报局局长的阿维·科查维（Aviv Kochavi）少将在 2014 年指出：“在我看来，网络将很快被证明是（战争领域）的最大革命，超过枪炮和空军在过去这个世纪的使用”，他还补充道，网络领域的行动潜力几乎是

① Jeffrey Bardin, “Cyber Operations in the Middle East,” in Frederic Lemieux, ed., *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice,* New York: Springer, 2015, p. 102.

② “Israel Leads the Way in Cybersecurity,” *CXC Global,* February 1, 2016, http://cxcglobalemea.com/israel-leads-the-way-in-cybersecurity/.

③ Shmuel Even, “The Strategy for Integrating the Private Sector in National Cyber Defense in Israel,” *Military and Strategic Affairs,* Vol. 7, No. 2 (September 2015), p. 103.

④ Amos Yadlin, “Cyber-warfare -A New Dimension in Israel’s National Security Doctrine,” cited in Gil Baram, “The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case,” *Military and Strategic Affairs,* Vol. 5, No. 1 (May 2013), p. 27.

无限制的。[①] 以色列国防军总参谋长本尼·甘茨（Benny Gantz）中将，也将网络空间视为“极端重要”：“这是一个我们需要使用到极限的竞技场，我认为以色列国能够并且应该比现在已经做的要更多……必须达到超级大国的水平，它可以达到超级大国的水平。”[②]

鉴于网络空间在未来战争中的极端重要地位，以色列国防军总参谋部于 2009 年宣布，网络空间“对以色列来说是战略性的和可操作的作战地带”（strategic and operative combat zone for Israel）。[③] 2012 年，以色列国防军作战局起草了一份文件，对网络战的目标和用途进行了界定。根据这份文件，以色列国防军将网络空间视为与陆地、海洋、天空类似的另一个战场：“专业地讲，以色列国防军正在持续地在网络空间开展战斗，包括情报搜集和保护以色列国防军的网络。当需要时，网络空间也被用来执行攻击和其他信息行动。”[④] 以色列总理内塔尼亚胡直言不讳地宣告，网络战的时代已经到来：“今天，网络是战场的一部分，这不是明天的战争，它已经是今天的战争。”[⑤]

而且，以色列是世界上为数不多的具有网络战实战经验的国家，通过将网络战运用于实战之中，以色列取得了单纯依靠传统战争所未取得的骄人战绩。2007 年 9 月 6 日，以色列对叙利亚东部代尔祖尔的阿尔奇巴核设施发动袭击的“果园行动”（Operation Orchard）是将网络战与常规战完美结合的一次典范。在这次奇袭行动中，网络攻击成为以色列开展军事行动的先导，以色列国防军网络部队通过网络攻击手段将叙利亚空军雷达系统陷于瘫痪，然后派 8 架战机深入叙利亚腹地对核设施发动空袭，成功摧毁预定目标而没有遭到叙利亚方面的任何反击。[⑥] 伊朗核设施遭到大规模网络病毒攻击而陷于瘫痪的“震网”（Stuxnet，又名超级工厂病毒）事件则是单纯开展网络战的成功实例。2010 年 6 月，伊朗纳坦兹的

---

① Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel,* New York: Springer, 2015, p. 65.

② Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel,* New York: Springer, 2015, p. 65.

③ Gil Baram, “Israeli Defense in the Age of Cyber War,” *Middle East Quarterly,* Vol. 24, No. 1 (Winter 2016), p. 6.

④ Yaakov Katz, “IDF Admits to Using Cyber Space to Attack Enemies,” *The Jerusalem Post,* March 6, 2012, http://www.jpost.com/Defense/IDF-admits-to-using-cyber-space-to-attack-enemies.

⑤ Herb Keinon, “PM: Israel Needs ‘Digital Iron Dome’ to Stop Cyber Attacks,” *The Jerusalem Post,* September 6, 2013, http://www.jpost.com/Defense/PM-Israel-needs-digital-iron-dome-to-stop-cyber-attacks-315934.

⑥ David A. Fulghum and Douglas Barrie, “Israel Used Electronic Attack in Air Strike against Syrian Mystery Target,” *ABC News,* October 8, 2007, http://abcnews.go.com/Technology/story?id=3702807&page=1.

核设施遭到网络病毒“Stuxnet”的大规模网络攻击，该病毒感染了超过6万台电脑，大约摧毁了一千多台离心机，致使伊朗的核计划倒退了至少两年以上。尽管没有哪个政府或组织宣布对该事件负责，但“Stuxnet”病毒是由以色列和美国联合开发的网络武器。[①] 该事件被称为21世纪以来第一场大规模的网络战，揭开了未来网络战的序幕，它首次在世人面前展示了以色列在网络战方面的强大实力。

由于网络空间的诸多威胁，各国对于网络安全的强劲需求助推着网络安全产业的发展。以色列在这一方面走在世界前列，引领了网络安全产业的潮流。网络安全领域的出口成为促进以色列经济增长的重要动力之一，正如以色列国家经济委员会主席尤金·坎德尔（Eugene Kandel）所说，“网络安全领域是政府可以也是必须加强部门间合作和创造新的经济增长动力的极好范例。”[②] 不仅如此，以色列学术界也充分意识到网络安全与网络战的重要性。2010年，以色列著名智库国家安全研究所发起了“网络安全项目”（Cyber Security Program），由加比·斯伯尼博士（Gabi Siboni）担任负责人。本·古里安大学、特拉维夫大学、以色列网络防御研究所（Israeli Cyber Defense Institute）等也相继建立了网络安全和情报课程。[③]

三 《2010国家网络倡议》与以色列国家网络战略的制定

在世界范围内，以色列是最早意识到信息安全对于维护国家安全的重要性的国家之一，采取积极措施保护关键计算机系统。早在20世纪90年代初，因特网刚刚兴起之时，以色列政府就将加强国家网络建设提上议事日程。1995年4月，以色列政府通过了建立一个特别部门以确保“敏感信息”安全的决定，并对其涉及的军事和民用部分进行了明确区分，该特别部门——政府信息安全中心在1999年正式建立。[④] 为了提高办公效率，1996年，以色列财政部的总会计师办公室发起成立了“计算机分队”（computer unit），该分队成为以色列政府推进信息化的重要

① James P. Farwell and Rafal Rohozinski, “Stuxnet and the Future of Cyber War,” *Survival,* Vol. 53, No. 1 (February-March 2011), pp. 23-40.

② “Cabinet Briefed on the Israel National Cyber Bureau,” Prime Minister's Office, November 11, 2012, http://www.pmo.gov.il/english/mediacenter/spokesman/pages/spokecyber111112.aspx.

③ Jeffrey Bardin, “Cyber Operations in the Middle East,” in Frederic Lemieux, ed., *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice,* New York: Springer, 2015, p. 102.

④ Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel,* New York: Springer, 2015, p. 32.

先锋。[①] 为了推进“e－政府工程”（e-GOV project），1997 年，以色列政府主导成立了“特西拉分队”（Tehila unit），即“因特网时代的政府基础设施”（Government Infrastructure for the Internet Age），以保护政府各部门连接因特网并提供安全的信息基础设施。特西拉分队下设计算机紧急应对小组，它从一开始就致力于信息安全问题，成为以色列政府推进信息化建设的主导力量。[②]

为了形成统一的国家信息政策，以色列政府指派国家安全委员会制定信息技术发展规划。在国家安全委员会提交的报告的基础上，2002 年 12 月 11 日，以色列政府通过了名为“保护以色列国计算机系统的责任”的 B/84 号特别决议（Special Resolution B/84），[③] 该决议决定建立两大监管机构：“保护国家计算机系统最高指导委员会”和“保护国家关键计算机系统小组”，其中最高指导委员会由国家安全委员会的首脑出任主席，其成员由政府部门高管、以色列银行代表、国防军代表共同构成。B/84 号特别决议的重要成果之一是，宣布在以色列国家安全总局之下建立国家信息安全局（Re'em/National Information Security Authority），负责对以色列信息安全的关键基础设施进行监管并提供建议。[④] B/84 号特别决议使以色列成为首批采取关键基础设施保护（Critical Infrastructure Protection）政策的发达国家之一，通过这些举措以确保以色列政府在应对网络空间威胁的连续性。

2007 年爱沙尼亚和 2008 年格鲁吉亚相继遭遇大规模网络攻击导致许多机构陷于瘫痪状态，这些事件使国际社会充分意识到网络战的巨大威力，这也促使以色列将网络安全问题提升至前所未有的高度。2010 年在以色列网络安全发展史上具有十分重要的意义。为了应对网络安全威胁、建设网络安全强国，内塔尼亚胡要求国家安全委员会就网络安全问题以及以色列的应对进行评估。由于网络安全事务具有很强的专业性，国家安全委员会无法执行这项使命。2010 年 11 月，内塔尼亚胡任命退役将军、经济部国家研发委员会主席以撒·本·以色列（Isaac Ben Israel）为总理网络事务首席顾问，负责制定以色列的国家网络发展规划。[⑤]

---

① Gil Baram, “The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case,” *Military and Strategic Affairs,* Vol. 5, No. 1 (May 2013), p. 28.

② Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts and Strategic Trends,* Tel Avir: Institute for National Security Studies, 2012, p. 76.

③ Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel,* New York: Springer, 2015, pp. 35-36.

④ Lior Tabansky, “Cyber Security Challenges: The Israeli Water Sector Example,” in Robert M. Clark and Simon Hakim, eds. , *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level,* Switzerland: Springer Publishing, 2016, p. 208.

⑤ Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel,* New York: Springer, 2015, p. 43.

以本·以色列为首的国家网络行动小组（National Cybernetic Task Force）下设8个分委员会，包括来自国防和军事部门、学术界、研发部门以及以色列政府各相关部门（财政部、经济部、科技部）等许多领域的80名专家。经过6个月时间的系统调研，在本·以色列的主持下，行动小组对以色列网络安全的挑战和机遇进行了充分的评估，调研结果和建议最后汇总成一份报告提交给以色列政府——《国家网络倡议：一份提交总理的特别报告》（The National Cyber Initiative – A Special Report for the Prime Minister），也称《2010国家网络倡议》（2010 National Cyber Initiative）。[①] 该倡议的目标是，使以色列在五年内成为全球前五的网络强国，“保持以色列作为信息技术发展中心的国际地位，为其提供在网络空间领域超级大国般的能力，确保其作为开放、民主、知识社会的经济和国家弹性。”[②] 该倡议还就国家网络安全提出了总体性的政策建议：（1）教育：从小学做起，提升全社会的网络意识和加强网络教育；（2）研发：鼓励学术界和产业界开展有关网络安全的研发项目；（3）安全：发展在平时和紧急状态下的国家网络空间运作能力，以应对道德、法律、隐私和经济挑战；（4）机遇：网络技术为经济、学术和国际关系都提供了机遇。[③] 该倡议最核心的建议是，将政府机构、军情部门、学术界、产业界之间的密切合作作为增强国家网络安全的最佳途径，为了达到这个目标，有必要建立一个新的政府网络管理机构以协调各方面的努力。

2011年8月7日，以色列政府颁布名为《提升国家网络空间能力》（Advancing National Cyberspace Capabilities）的第3611号决议，基本采纳了《2010国家网络倡议》的主要内容。该决议被视为以色列网络安全政策的指导方针，通过鼓励学术界、产业界和私人、政府以及军情等部门的合作，以提升国家在网络空间方面的能力和确保以色列作为网络技术中心的地位，进而帮助以色列应对当前和未来的网络安全挑战。第3611号决议的核心内容如下：[④]

> 为了提升国家网络空间能力，更好地应对当前与未来网络空间领域的挑战；为了提升对以色列国至关重要的国家基础设施的保护，最大限度地保护它们免遭网络攻击；为了提升以色列作为信息技术发展中心的地位，鼓励学

① Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel,* New York: Springer, 2015, p. 44.

② Michael Raska, “Confronting Cybersecurity Challenges: Israel’s Evolving Cyber Defence Strategy,” *RSIS Policy Report,* January 2015, p. 7.

③ Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel,* New York: Springer, 2015, p. 44.

④ Lior Tabansky, “Critical Infrastructure Protection against Cyber Threats,” in Gabi Siboni, ed., *Cyberspace and National Security: Selected Articles,* Tel Avir: Institute for National Security Studies, 2013, p. 39.

术界、产业界、私人、政府部门与特别机构之间的合作。有鉴于此，根据 2002 年 12 月 11 日通过的国家安全部长级委员会的第 B/84 号决议以及不违背任何其他法律或政府决议，现在决定：

1. 在总理办公室之下建立国家网络局；

2. 规范处理网络领域事务的职责；

3. 提升网络防御能力和推动网络空间与超级计算机的研发；

……

第 3611 号决议最重要的内容之一就是，决定在总理办公室之下建立以色列国家网络局（Israel National Cyber Bureau，简称 INCB），直接对总理负责。经过半年的酝酿，2012 年 1 月，以色列内阁批准了建立国家网络局的提议，以规范和管理网络空间的活动。该机构的职能是“总理、政府及其委员会的咨询机构，依照一切法律和政府决议，就国家在网络领域的政策以及推动其实施提供建议。”① 国家网络局不仅是一个咨询机构，而且是一个重要决策机构。该机构主要有四个方面的活动：（1）制定国家网络政策和网络战略；（2）推动政府机构、军情部门、学术界、产业界及其他相关部门就网络安全进行协作；（3）促进以色列的网络技术研发与网络安全产业；（4）加强网络安全方面的国际合作。② 国家网络局通过一系列举措，推进以色列的网络安全防御能力，进而打造以色列在网络安全领域的领导地位。

根据《隐私保护法（1981 年）》（*The Privacy Protection Law, 5741-1981*）和 B/84 号特别决议，以色列法律只允许国家安全总局和警察局出于某些安全的目的介入民事事务。而随着国家网络局的设立，许多涉及民事层面的网络管辖权问题也就随之出现，国家网络局和国家安全总局之间就民用网络的管辖问题产生了矛盾。③ 为了调解这种僵局、理顺民事网络管辖权，2014 年 9 月，以撒·本·以色列领导的国家网络行动小组建议设立一个新的管理机构——国家网络安全局（National Cyber Security Authority），加强对民用领域的网络安全管理，以建立更加全面的网

① Gabi Siboni and Ofer Assaf, *Guidelines for a National Cyber Strategy*, Tel Avir: Institute for National Security Studies, 2016, p. 58.

② Jeffrey Bardin, “Cyber Operations in the Middle East,” in Frederic Lemieux, ed., *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice*, New York: Springer, 2015, p. 103; Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel*, New York: Springer, 2015, p. 47.

③ Barak Ravid, “Israeli Security Agencies in Turf Battle over Cyber War; Netanyahu to Decide,” *Haaretz*, September 14, 2014, http://www.haaretz.com/israel-news/1.615637.

络安全政策。[①] 2015 年 2 月 15 日，根据以色列政府相继通过的名为《提升国家在网络安全方面的规范和政府领导力》（Advancing National Regulation and Governmental Leadership in Cyber Security）的第 2443 号决议和名为《提升国家对网络安全的准备》（Advancing the National Preparedness for Cyber Security）的第 2444 号决议，正式建立国家网络安全局，其职能是“监管网络防御行动以对网络攻击提供全面的应对，包括处理威胁和实时反应”。[②] 在国家网络安全局之下设立国家网络紧急应对小组，以增强以色列在应对网络威胁上的弹性。国家网络安全局与国家网络局一起运作，共同构成以色列国家网络指挥部，内塔尼亚胡任命国家网络局局长埃维塔尔·马塔尼亚兼任国家网络安全局的负责人。为了规范民事网络管理活动，2016 年 6 月 9 日，国家网络安全局与国家安全总局起草了《谅解备忘录》。[③]

为了积极应对各种网络安全威胁，在国家网络局的具体负责下，以色列构建了总体性的国家网络政策，旨在增强以色列在网络安全领域的全球领导地位。2015 年 11 月，以色列总理办公室授权国家网络局公布了国家网络安全战略，其精神主要来自《2010 国家网络倡议》和《提升国家的网络空间能力》的第 3611 号决议这两份重要文件，它们共同规划了以色列国家网络战略的基本思路。以色列国家网络战略的目标是通过加强不同部门之间的合作以提升网络安全，维持以色列作为全球网络强国的地位，同时实现经济、技术与外交利益。由于网络空间超越了传统的国界，其威胁程度也远超常规安全领域的威胁，对此，以色列实施了总体性（holistic approach）的国家网络安全战略，致力于打造以色列的“数字化边界”（digital frontier），[④] 从而有效应对各种网络安全威胁、打造网络强国地位。

根据以色列国家网络局局长埃维塔尔·马塔尼亚的构想，总体性的国家网络

---

① Lior Tabansky, “Cyber Security Challenges: The Israeli Water Sector Example,” in Robert M. Clark and Simon Hakim, eds., *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*, Switzerland: Springer Publishing, 2016, pp. 215-216.

② “Cabinet Approves Establishment of National Cyber Authority,” Consulate General of Israel in Mumbai, February 15, 2015, http://embassies.gov.il/mumbai/NewsAndEvents/Pages/Cabinet-approves-establishment-of-National-Cyber-Authority-15-Feb-2015.aspx.

③ Shmuel Even, David Siman-Tov, and Gabi Siboni, “Structuring Israel’s Cyber Defense,” *INSS Insight*, No. 856, September 21, 2016, p. 1.

④ Lea Speyer, “Head of Israel’s Cyber Authority: ‘Holistic Approach’ Best Way to Counter Threats from ‘Borderless’ Realm of Cyberspace,” *The Algemeiner*, July 11, 2016, http://www.algemeiner.com/2016/07/11/head-of-israels-cyber-authority-holistic-approach-best-way-to-counter-threats-from-borderless-realm-of-cyberspace/.

战略包括以下要素（参见图 1）。第一，集中统一的网络安全当局，是维护网络安全的核心主导。它体现为以色列国家网络指挥部下的国家网络局和国家网络安全局，这两大机构负责以色列国家网络体系的管理和运作。第二，不同层次的网络防御目标，是维护网络安全的具体手段。集中统一的网络安全当局负责威慑，军事部门负责反击，而法律机构负责调查犯罪和反恐。就具体网络防御目标而言，可以分为三个层次：（1）坚固（Robustness），击退与克制绝大部分网络威胁的系统能力，尤其集中在私人领域的网络风险；（2）弹性（Resilience），应对不可避免地出现的威胁的系统能力，该层面超出了私人部分而只有政府可以提供缓解能力；（3）防御（Defense），通过专注于背后的人为因素来破坏网络攻击的能力，绝大部分网络攻击可以在前两个层次得到处理，但仍有少数高级别的网络攻击必须在第三层次进行应对，有必要采取威慑和反击的手段和措施。① 第三，国家能力建设和网络安全生态系统（Cybersecurity Eco-system），是维护网络安全的基本保障。网络安全需要以先进的技术作为支撑，而这需要技术研发部门的配合，尤其是政府机构、军情部门、学术界、产业界之间的合作。②

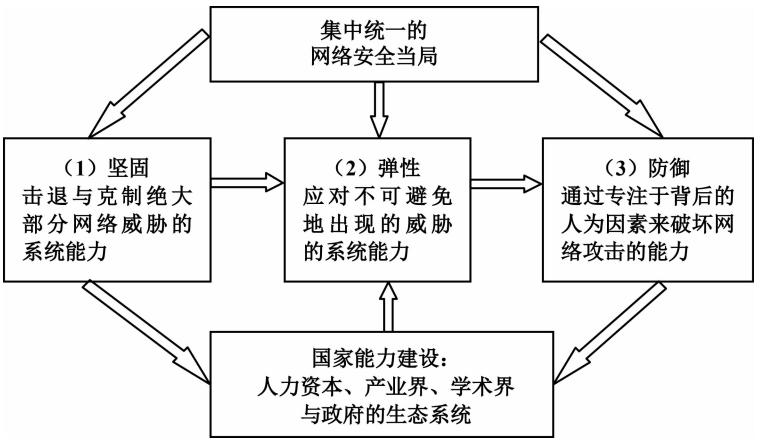


图 1　以色列国家网络战略的三个层次③

① "Elements of a National Cyber Security Strategy: The View from Israel," *The CyberWire*, September 16, 2016, http://thecyberwire.com/events/7thBillCSSummit/elements-of-a-national-cyber-security-strategy-the-view-from-israel.html.

② Barbara Opall-Rome, "Interview: Eviatar Matania, Head of Israel's National Cyber Directorate," *Defense News*, July 11, 2016, http://www.defensenews.com/story/defense/show-daily/farnborough/2016/07/10/f-35-tap-airbus-data-protection-technology/86925068/.

③ "Israel's Cyber Security Strategy," *Israel National Cyber Bureau*, November 2015, p. 15, http://scirex.grips.ac.jp/center/wp-content/uploads/2015/12/151110_matania.pdf.

四　以色列网络安全治理的主要路径及其成效

在世界各国中，以色列较早建立起健全的网络安全维护机制，不仅形成了较为完备的国家网络安全战略，更重要的是，构建了以“网络防御＋技术研发”为中心的网络安全生态系统。通过政府层面、军情部门、民间领域（包括产业界和学术界）等各部门之间密切合作而形成的生态系统成为网络安全的基本保障，不仅有效治理了以色列网络安全问题，而且将之转化为创新创业的重要契机，实现了安全与经济的双赢目标。内塔尼亚胡指出：“我们致力于使以色列国成为世界网络领域的先锋。除了安全上的重要性，还有巨大的经济机会。”①

（一）政府层面

以色列国家网络系统的中枢为国家网络指挥部（National Cyber Directorate），该机构在总理办公室下设立，由国家网络局和国家网络安全局两大机构构成，其共同负责人为埃维塔尔·马塔尼亚，就有关国家网络安全事务直接对总理负责。国家网络局的主要职责为制定国家网络政策和推动网络安全的研发，下辖政策司、研发司、能力建设司；国家网络安全局的主要职责为保护民用网络系统和开展网络防御行动，下辖提升安全和市场管理司、国家网络紧急应对小组、行动司；而国际合作司和法律框架司由国家网络局和国家网络安全局共同领导，直接对国家网络指挥部负责（见图2）。② 其中，国家网络紧急应对小组（Israel National Cyber Event Readiness Team，简称 CERT-IL）于2015年在贝尔谢巴重新组建，是以色列信息安全和网络事务的民用中心。

为了有效应对网络安全威胁、打击网络犯罪活动，以色列国家网络局推动了对有关法律的修订，对网络犯罪和隐私保护之间的界定进行了区分。以色列政府制定的《计算机法（1995年）》（*Computers Law, 5755-1995*）是对有关信息

① “Cabinet Approves the Creation of the National Cyber Directorate,” Prime Minister’s Office, August 7, 2011, http://www.pmo.gov.il/english/mediacenter/spokesman/pages/spokecyber070811.aspx.

② “Cabinet Approves the Creation of the National Cyber Directorate,” Prime Minister’s Office, August 7, 2011, http://www.pmo.gov.il/English/MediaCenter/Spokesman/Pages/spokecyber070811.aspx.

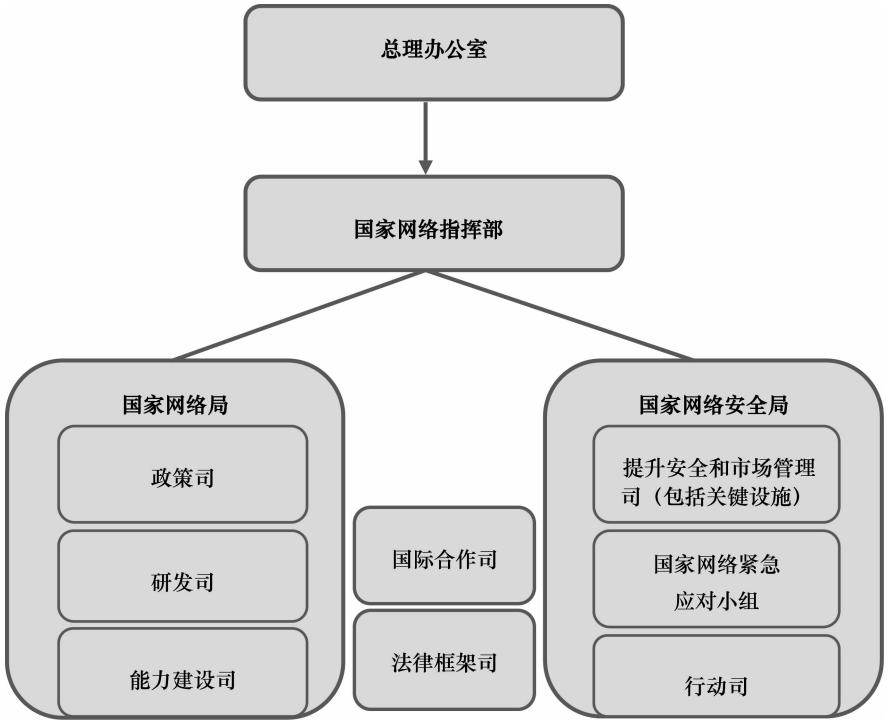


图 2　以色列国家网络管理系统架构图①

与通信技术领域的首次系统规范，但随着网络安全形势的快速发展，其中许多条文已不再适应变化的现状。2012 年 7 月 10 日，在国家网络局的推动下，议会对《计算机法（1995 年）》进行了修订，以与《布达佩斯网络犯罪公约》（*Budapest Convention on Cybercrime*）② 的精神相一致，修正案补充了有关使用计算机和计算机软件从事犯罪活动的条款，允许出于保护民用网络安全的目的对网络空间加大监控力度。③ 随着网络恐怖主义的新发展，国家网络局与司法部等部门合作制定

① 图 2 是笔者根据相关资料制作而成。参见 Barbara Opall-Rome, "Interview: Eviatar Matania, Head of Israel's National Cyber Directorate," *Defense News*, July 11, 2016, http://www.defensenews.com/story/defense/policy-budget/leaders/interviews/2016/07/11/israel-cybersecurity-directorate-matania/86445128/。

② 2001 年 11 月，欧洲理事会的 26 个欧盟成员国以及美国、加拿大、日本和南非等 30 个国家的政府官员在布达佩斯共同签署了针对网络犯罪的《布达佩斯网络犯罪公约》，该公约成为全世界第一部针对网络犯罪行为制定的国际公约。该公约除序言外分为四章，共计 48 个条文。

③ Ruth Levush, "Israel: Criminalization of Certain Activities Involving Computer Software," The Library of Congress, August 21, 2012, http://www.loc.gov/law/foreign-news/article/israel-criminalization-of-certain-activities-involving-computer-software/.

新的网络安全法。2016 年 6 月 15 日，以色列议会通过了新的《反恐怖主义法（2015 年）》（*Counter Terrorism Bill , 5775-2015*），其中加入了打击网络恐怖主义的条款，禁止通过因特网或社交媒体煽动恐怖主义。①

国家网络局还致力于推进以色列的“e－政府计划”，② 该计划由国家网络局与外交部、财政部联合负责，充分借助网络技术处理政务、提高工作效率，同时防范网络安全风险。此外，国家网络局还与以色列银行、能源部等关键部门合作建立了银行网络防御联合中心（Joint Center for Cyber Defense in the Banks）、能源网络安全中心（Energy Cyber Security Center，简称 ECSC）等，③ 以加强关键部门的网络防御能力。此外，该局还大力支持学术界和产业界的创新。为了改善以色列的学术基础设施，国家网络局联合科技部在 2012－2013 年间出资 5 000 万新谢克尔资助了超过 20 个大型学术研究项目，并设立了专项奖学金，以鼓励在校大学生从事网络安全的相关研究。

从 2014 年开始，以色列国家网络局与外交部、经济部合作，举办每年一度的网络科技峰会（Cyber Tech International Conference and Exhibition），展示以色列的网络安全初创企业和现有的网络安全公司。这已成为以色列最具影响力的网络科技盛会，也是美国以外的有关网络安全科技的最大规模的展览，吸引着来自五十多个国家和地区的万余人与会。④ 此外，以色列注意加强网络安全领域的国际合作，共同探讨维护网络安全的经验，以色列先后与美国、英国、印度和日本等国开展了不同程度的网络安全合作。2014 年 5 月，以色列国家网络局、科技部与英国内阁办公室、工程与物理科学研究委员会（EPSRC）达成一份《网络防御合作

① David Fidler, “Israel’s New Counter-Terrorism Law and Terrorism in Cyberspace,” *Net Politics,* August 22, 2016, http://blogs. cfr. org/cyber/2016/08/22/israels-new-counter-terrorism-law-and-terrorism-in-cyberspace/.

② Daphne Getz and Itzhak Goldberg, *Best Practices and Lessons Learned in ICT Sector Innovation: A Case Study of Israel,* World Development Report Background Papers, Washington, D. C.: World Bank Group, 2016, pp. 58-59.

③ Shmuel Even, “The Strategy for Integrating the Private Sector in National Cyber Defense in Israel,” *Military and Strategic Affairs,* Vol. 7, No. 2 (September 2015), p. 112; Sharon Udasin, “Israeli Hi-tech Firm to Launch Energy Cyber Security Center,” *The Jerusalem Post,* July 20, 2014, http://www.jpost. com/Enviro-Tech/Israeli-hi-tech-firm-to-launch-Energy-Cyber-Security-Center-363606.

④ Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel,* New York: Springer, 2015, p. 53.

协议》，设立总额高达 700 万新谢克尔的双边联合研究基金。[①] 2016 年 6 月，以色列国家网络局局长埃维塔尔·马塔尼亚和美国国土安全部副部长阿勒简德罗·梅奥卡斯（Alejandro Mayorkas）联合签署了《网络防御合作协定》（Cyber Defense Cooperation Agreement），建立了专门的美国—以色列网络安全行动小组（U. S. -Israel Cybersecurity Task Force），促进两国在网络安全研发方面的合作，提倡通过两国各自的国家网络紧急应对小组实现实时操作连接。通过该协定，以色列成为加入美国主导的自动指标共享计划的首批国家之一，该计划由美国国土安全部管理，允许共享网络威胁指标，以预防和矫正网络防御操作。[②]

（二）军情部门

以色列是世界上较早将网络技术应用于实战的国家，由于现代战争的需要，以色列军事情报部门对网络技术有着高度的追求。以色列军情部门中负责网络安全的主要机构为 8200 部队和 C4I 司令部，另外辛贝特等也承担了部分职责。首先，军事情报局下设的“8200 部队”（Unit 8200）作为以色列国防军的高科技分队，是承担网络防御和网络战任务的主力。该部队集中于网络战的三大领域：情报搜集、密码编写和网络攻防。以色列国防军还在 8200 部队之下成立“网络参谋部”（Cyber Staff），以指导和协调以色列军队在网络空间方面的行动；[③] 隶属于 8200 部队的“马姆拉姆”（Mamram/Software Unit），为以色列国防军各兵种和总参谋部提供数据处理服务。[④] 其次，创建于 2003 年的“C4I 司令部”（C4I Directorate），即指挥与控制、通讯与计算机（Command, Control, Communications, and Computers），负责国防军的电子通信和组织网络防御能力。2011 年，以色列国防军总参谋部在 C4I 司令部下建立了网络防御司（Cyber Defense Division），负责保护国防军的网络

---

① Ari Soffer, “Israel, UK Establish Joint Fund for Cyber Defense,” *Israel National News*, May 15, 2014, http://www.israelnationalnews.com/News/News.aspx/180655.

② “Israel and the US Sign Operative Cyber Defense Cooperation Agreement,” *Israel Ministry of Foreign Affairs*, June 21, 2016, http://mfa.gov.il/MFA/PressRoom/2016/Pages/Israel-and-the-US-sign-operative-cyber-defense-cooperation-agreement-21-June-2016.aspx.

③ Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts and Strategic Trends*, Tel Aviv: Institute for National Security Studies, 2012, p. 79.

④ Yoav Zitun, “The IDF Prepares for Cyber-battles,” *Ynet News*, September 2, 2015, http://www.ynetnews.com/articles/0,7340,L-4696003,00.html.

体系。[①] 此外，辛贝特也承担了保护政府系统、国家基础设施和金融数据等的部分职责。为了增强军事情报局和 C4I 司令部之间的合作，2009 年设立了玛特佐夫网络分队（Matzov/Cyber Unit），负责搜集以色列的对手在电脑黑客方面的情报，同时为国防军、辛贝特、摩萨德等编写密码。[②]

为了加强以色列的网络实战能力，以色列国防军与国家网络局正在实施一系列研发计划以提升以色列军队应对网络袭击的能力。2012 年 10 月，国家网络局与国防部研发中心联合宣布建立一个军民两用的网络安全研发计划——马沙德计划（Masad program，Civilian and Defense Cyber R&D），促进网络安全研发项目以服务于国防和民用目的。首期启动预算达到 1 000 万新谢克尔，三年内投资 5 000 万新谢克尔。[③] 2013 年，国家网络局与首席科学家办公室合作启动了“卡迪玛计划”（Kidma Program），即“促进网络防御研发计划”（Advancement of Cyber Defense R&D），前两年的启动预算为 8 000 万新谢克尔，以促进以色列网络防御的研发活动。该计划有两大目标：一是进一步发展以色列的网络基础设施；二是为以色列公司在全球市场确立优势地位。[④]

2014 年 9 月，以色列宣布启动“数字铁穹”计划（Digital Iron Dome），具体由国防部研发中心负责开发，计划在三年内建立一个庞大的网络安全系统保护以色列的关键信息和国防系统。[⑤] 内塔尼亚胡借用成功抵御大部分来袭火箭弹的“铁穹系统”来为该网络安全计划命名，他强调，“以色列的重要力量在于网络空间之中。我们的进步主要体现在保卫现代国家方面。正如我们发展出了前所未有的‘铁穹系统’成功地拦截了火箭弹，因而我们现在正发展‘数字铁穹系

① Yaakov Katz, “IDF sets up New Cyber-defense Division,” *The Jerusalem Post,* June 28, 2011, http://www.jpost.com/Defense/IDF-sets-up-new-cyber-defense-division.

② Yaakov Katz, “IDF sets up New Cyber-defense Division,” *The Jerusalem Post,* June 28, 2011, http://www.jpost.com/Defense/IDF-sets-up-new-cyber-defense-division.

③ Chana Ya'ar, “Gov't Establishes Dual Cyber Security Program,” *Israel National News,* November 1, 2012, http://www.israelnationalnews.com/News/News.aspx/161605.

④ Daniel Shkedi, “The Cybersecurity Sector in Israel,” *Embassy of India,* 2015, p. 5, http://www.indembassy.co.il/pdf/Report-on-the-Cybersecurity-Industry-in-Israel.doc.

⑤ Asher Zeiger, “Israel Developing ‘Digital Iron Dome’ to Guard against Cyberterrorism,” *The Times of Israel,* October 14, 2012, http://www.timesofisrael.com/israel-developing-digital-iron-dome-to-guard-against-cyber-terrorism/.

统’以保卫这个国家的电脑系统不受攻击。”① 该网络安全防御系统将分为四个层次：确认网络威胁、保护现有系统、清除网络威胁和实施网络反击。与“铁穹系统”确认并拦截火箭弹不同，“数字铁穹系统”无需对目标主动发起攻击，而是为以色列国防军和以色列政府提供网络攻击的准确来源，进而提升自身防御能力。②

为了应对愈演愈烈的网络恐怖活动，统筹整合军情部门下的众多网络防御单元，并指挥以色列的网络战，组建网络司令部（Cyber Command）的呼声在以色列国防军内部不断高涨。2015 年 6 月 15 日，以色列国防军发言人宣布，国防军总参谋部已决定建立网络司令部，以领导以色列军队在该领域的行动。③ 网络司令部计划在未来两年内建立，完成对军事情报局和 C4I 部队等机构的整合，新的网络司令部由前者首脑领导。④ 网络司令部是以色列国防军序列中继北方军区司令部、中央军区司令部、南方军区司令部和后方司令部之后设立的第五个司令部。在以色列国防军总参谋长加迪·埃森科特（Gadi Eisenkot）看来，“以色列国防军需要在各个战争层面出类拔萃，这也包括网络层面，网络正在变得日益重要。新的网络司令部将使以色列国防军在这些战线上有更好表现，也将充分利用以色列现有的技术和人才优势。”⑤ 网络司令部这个新机构的出现，反映出以色列国防军对于网络战的高度重视，主动把握网络时代的军事发展潮流。

（三）民用领域

以色列将民用领域的网络安全研发作为国家重点优先发展的领域。2012 年，以色列科技部确立了国家四大优先研究领域：脑科学、超级计算机和网络安全、

---

① “Cabinet Briefed on the Israel National Cyber Bureau,” Prime Minister’s Office, November 11, 2012, http://www.pmo.gov.il/english/mediacenter/spokesman/pages/spokecyber111112.aspx.

② Asher Zeiger, “Israel Developing ‘Digital Iron Dome’ to Guard against Cyberterrorism,” *The Times of Israel*, October 14, 2012, http://www.timesofisrael.com/israel-developing-digital-iron-dome-to-guard-against-cyber-terrorism/.

③ Ben Caspit, “IDF to Unify Cyber Warfare Units,” *Al-Monitor*, February 16, 2015, http://www.al-monitor.com/pulse/originals/2015/06/israel-idf-cyber-intelligence-new-unit-eisenkot-war-future.html; Yaakov Lappin, “IDF to Set up Unified Cyber Division within 2 Years,” *The Jerusalem Post*, June 16, 2015, http://www.jpost.com/Israel-News/IDF-to-set-up-unified-cyber-division-within-2-years-406161.

④ News Desk, “Israel to Establish a New Cyber Command,” *Defense Update*, June 15, 2015, http://defense-update.com/20150615_israel-to-establish-a-new-cyber-command.html.

⑤ Meir Elran and Gabi Siboni, “Establishing an IDF Cyber Command,” *INSS Insight*, No. 719, July 8, 2015, p. 1.

海洋研究、可替代能源，其中之一就包括网络安全。网络安全领域由以色列国家网络局联合科技部共同负责，具体集中于人工智能、防火墙、超级计算和云计算等。[①] 此外，以色列经济部首席科学家办公室支持竞争性的网络安全研发活动。2011 年，首席科学家办公室给 21 个处于起步阶段的网络安全初创企业拨款 6 200 万新谢克尔；2012 年，首席科学家办公室给 45 个处于起步阶段的网络安全初创企业拨款 9 000 万新谢克尔。[②]

在以色列政府的规划下，地处沙漠腹地的贝尔谢巴市被打造成网络科技中心，在以色列网络安全产业中发挥着重要的作用，该城市云集了大量网络初创企业和网络研发平台，被誉为“以色列的网络之都”。[③] 2014 年 1 月，内塔尼亚胡在特拉维夫举办的网络科技峰会上宣布，以色列政府在贝尔谢巴建立庞大的网络科技园区——“网络火花：以色列网络创新平台”（Cyber Spark-the Israeli Cyber Innovation Arena），强调贝尔谢巴将“不仅是以色列的网络之都，而且也是世界网络安全领域最为重要的地方之一。”[④] 该网络创新平台由以色列国家网络局提议创立，在贝尔谢巴建立包括本·古里安大学、以色列国防军、国家网络紧急应对小组以及网络初创公司在内的网络安全生态系统。以色列政府对该科技园的定位是，结合经济和国防部门的力量，形成产业界、学术界、军情部门和政府机构密切合作的网络安全生态系统，目标是将贝尔谢巴打造为全球网络创新的中心，进而使以色列在网络安全领域领先于世界。

在以色列政府的大力支持下，贝尔谢巴的网络科技园产生了显著的集群效应，大量著名国际公司进驻该园区，例如国际商业机器公司（IBM）、思科（CISCO）、易安信（EMC）、洛克希德·马丁（LMT）、德国电信（Deutsche Telekom AG）等公司都在贝尔谢巴设立研发中心。[⑤] 2014 年，以色列国家网络局、贝尔谢巴市与本·古里安大学达成合作协议，共建网络安全研究中心（Cyber Security Research

---

① Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel,* New York: Springer, 2015, p. 52.

② Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel,* New York: Springer, 2015, p. 53.

③ Viva Sarah Press, “The Cyber-security Capital of the World,” *Israel21c,* February 16, 2014, http://www.israel21c.org/the-cyber-security-capital-of-the-world/.

④ Viva Sarah Press, “The Cyber-security Capital of the World,” *Israel21c,* February 16, 2014, http://www.israel21c.org/the-cyber-security-capital-of-the-world/.

⑤ “IBM and Lockheed Martin Invest in Israeli Cyber Complex,” *Security Week News,* January 29, 2014, http://www.securityweek.com/ibm-and-lockheed-martin-invest-israeli-cyber-complex.

Center at Ben-Gurion University），该中心包括网络攻击模拟实验室、恶意软件分析实验室、移动安全实验室等先进设备。根据以色列风险资本研究中心（IVC Research Center）的数据，到 2014 年，贝尔谢巴已有二百多家网络安全初创企业以及 20 个跨国公司的研发中心，在这些初创企业中，78 家在初创阶段成功筹资到 4 亿美元。①

以色列的网络安全产业发展十分迅速，在以色列高科技产业中获得的投资额最多，如今它已成为以色列经济增长的重要引擎之一。根据国家网络局的官方统计数据，以色列的网络安全研发投资位于世界前列，占全球该领域支出的 13%。② 不少以色列网络安全公司在国际市场上具有很高的知名度，例如 Check Point、CyberArk、Checkmarx、CYBERBIT 等。根据网络安全风险投资的统计，在世界 500 强网络安全公司中以色列占了 26 家，其中有 9 家以色列公司位于前 100 强，Check Point 公司更是高居全球第 4 位。③ 网络安全产业的巨大市场前景推动着网络安全初创企业的发展。2000 – 2012 年，平均每年有 52 家新的初创企业成立，而在 2012 – 2016 年间，该数字增长到平均每年 60 家。到 2016 年，以色列已有 40 个网络安全方面的全球研发中心，20 世纪 90 年代中期仅有 13 个。网络安全初创公司在以色列的整个投资系统中占据了重要地位，占以色列整个初创企业的 1/5 左右，构成了以色列所有投资的 16%。④ 截至 2016 年底，以色列已有超过 350 家网络安全公司，其规模仅次于美国，是英国的 3 倍；⑤ 2014 年，以色列在网络安全领域的出口总额高达 60 亿美元，占据了全球网络安全市场领域 10% 的份额，⑥ 而且这

---

① David Shamah, "BGU, Government Sign CyberSpark Security R&D Deal," *The Times of Israel*, April 20, 2014, http://www.timesofisrael.com/bgu-government-sign-cyberspark-security-rd-deal/.

② Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel*, New York: Springer, 2015, p. 53.

③ "Cybersecurity 500: Meet the Hot Cybersecurity Companies to Watch in 2016," *Cybersecurity Ventures*, November 15, 2016, http://cybersecurityventures.com/cybersecurity-500/.

④ Yoav Leitersdorf, Ofer Schreiber, and Iren Reznikov, "The Startup Landscape for Cybersecurity Companies in Israel," *Tech Crunch Network*, January 24, 2016, http://techcrunch.com/2016/01/24/the-startup-landscape-for-cybersecurity-companies-in-israel/.

⑤ Steve Morgan, "Israel is Number Two in Cybersecurity behind the U.S.," CSO, September 8, 2015, http://www.csoonline.com/article/2981246/security-industry/israel-is-number-two-in-cybersecurity-behind-the-us.html.

⑥ "Israel Accounts for 10 Percent of Global Cyber Tech Sales," *I24news*, May 26, 2015, http://www.i24news.tv/en/news/technology/72537-150526-israel-accounts-for-10-percent-of-global-cyber-tech-sales.

个比例还在继续增长。而这一切都是在仅有八百多万人口（仅占全世界总人口的1‰）的情况下做到的。

五　启示与建议

2016 年 4 月 19 日，习近平总书记在北京主持召开网络安全和信息化工作座谈会并发表重要讲话，强调面对复杂严峻的网络安全形势，要保持清醒头脑，各方面齐抓共管，切实维护网络安全。第一，树立正确的网络安全观。第二，加快构建关键信息基础设施安全保障体系。第三，全天候全方位感知网络安全态势。第四，增强网络安全防御能力和威慑能力。网络安全和信息化是相辅相成的，没有网络安全就没有国家安全，没有信息化就没有现代化。在当今世界网络技术飞速发展过程中，网络安全的维护直接关系到国家安全，必须从国家战略的高度对网络安全加以重视，并系统规划网络安全战略，切实推进网络强国建设和推动网信事业发展。

在人口和资源都极其有限的情况下，以色列积极抢占先机、走在世界前列，加强网络安全建设和发展网络安全产业，不仅有效维护了国家网络安全，而且取得了显著的经济效益。正是通过一系列卓有成效的治理举措，以色列如今成为网络安全领域的全球引领者之一，跃居为世界上首屈一指的网络强国，被誉为“网络安全的国度”（Cyber Security Nation）。以色列政府和军事部门的网络系统被称为是世界上最为安全的网络之一。根据国际电信联盟等机构联合发布的年度报告，在 2015 年全球网络安全指数（Global Cybersecurity Index，简称 GCI）中，以色列高居世界第六位。[①] 纵观以色列对网络安全问题的治理历程，可以大致归纳出以下经验和启示：

首先，必须将网络安全提升至国家战略高度。从 20 世纪 90 年代初开始，以色列积极把握信息时代的发展潮流，从国家战略高度重视网络安全问题，提高全

① ITU and ABI Research, *Global Cybersecurity Index and Cyberwellness Profiles*, Geneva: ITU, 2015, p. 2. 全球网络安全指数，是由国际电信联盟联合著名市场情报公司 ABI Research 自 2013 年起发布的年度分析报告，对各主要国家和地区的网络安全程度进行排名，统计范围包括 196 个国家和地区。

民的网络安全意识。以色列社会普遍对网络空间给予了极大的关注，将网络革命视为继农业革命和工业革命之后的“第三次革命”；以色列政府把网络安全列为国家优先地位，先后出台了《2010 国家网络倡议》以及多个涉及网络安全的政府决议，有力地推动了国家网络安全建设。

其次，必须建立并健全维护网络安全的顶层设计。以色列在总理办公室之下设立包括国家网络局和国家网络安全局在内的国家网络指挥部，这些重要管理机构直接对总理负责，就有关国家网络安全事务进行处理和应对，并积极协调不同部门之间的关系，形成了网络安全治理的国家管理体系。在军队层面，设立不久的以色列网络司令部是加强网络战指挥系统的重要举措。

再次，必须重视网络安全的技术研发。网络安全不同于其他安全领域，它对技术的依赖度很高，只有加强网络安全的技术研发，才能从技术层面应对各种网络安全风险；以色列通过加大网络安全技术研发力度，成功地建立起规模庞大的网络安全产业，在维护了国家安全的同时又取得了重要的经济效益，将之转化为创新创业的重要契机。

最后，必须加强国家能力建设，构建网络安全的生态系统。网络安全是国家经济和安全体系中的重要环节，各有关部门的鼎力支持和密切配合是打造坚固防火墙的基本保障，而这关键在于加强国家能力建设。以色列在网络安全治理方面取得的成就离不开高度发达的创新生态系统，正是政府、军情、民间（包括产业界和学术界）等各部门之间的密切合作，促成了以色列在网络安全领域的全球引领地位。

【收稿日期：2016-12-24】

【修回日期：2017-01-10】

【责任编辑：苏　娟】