以色列国家网络空间安全战略研究报告

李敬[1*] 何**[1] 李**[1] 李*[1] 肖*[1] 王**[2] 张**[3]

[1]信息工程研究所 [2]成都计算机应用研究所 [3]近代物理研究所

2021年4月19日

辛丑三月初八

北京 · 怀柔

Contents

The Israel of 2025：On horror, hope and honey

Photo credit: @Ben Jennings https://www.politico.eu/article/israel-2025/

以色列国背景

以色列国（希伯来语：**לאֵרֶשְׂיִ תנַיִדְמָ**；阿拉伯语：ليئِارَسْإِ ةلَوْدَ），是位于中东地区的一个主权国家，1948年5月14日独立建国，人口926万（2020），主要人口为犹太人，以希伯来语为官方语言，通用英语。

依根据《以色列基本法》，以色列为“犹太和民主国家”。以色列为代议民主制国家，采用议会制、比例代表制和普遍选举制。总理为政府首脑，议会为立法机关。

以色列为一发达国家，经济合作与发展组织成员国，2014年其名义国内生产总值排名世界第37。该国具有较高水平的劳动力，为全球教育程度最高的国家之一，其公民拥有高等教育学历的比例亦为世界最高之一。其生活水平为中东最高和亚洲第四高，其人口预期寿命亦居世界前列。

国旗

国徽

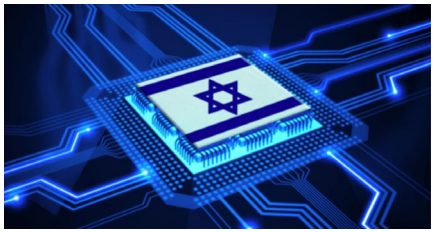
https://zh.wikipedia.org/wiki/以色列

以色列国背景（Cont.）

以色列因与邻国长期处于战乱（国土狭小、资源匮乏，被穆斯林国家围堵，恐怖袭击不断，且历经五次中东战争的国家），以色列的高军事预算、攻防武器研发及全民皆兵制度，被认为是目前网络安全技术及人力的重要关键基础。

以色列一开始是向各界寻找资源满足他们的信息化需求，同时引入了国际大厂在以色列设置研发中心，也带来了大公司的经验、知识、物流、人力资源及营销全球的相关资源，辅以推动高科技经济及全球营销的政策方向，加上以色列重视教育并鼓励思辨传统，造就创新不怕失败的民族性格，是他们网络安全技术创新及产业发展亮眼之根源。

以色列打造国家级的网络安全生态圈，主要面向政府（军队）、企业及学校发展。在政府部分，目前是由国家网络安全指导会(Israel National Cyber Directorate, **INCD**)统管整体网络安全的工作，直接对总理负责，约 250 位成员，设有技术研发(Technology Unit)、安全强化(Robustness Unit)及操作营运(Operation Unit)主要单位，分别负责网安技术能量提升、 各层面安全防护指引(如关键基础设施防护、产业引导等)、网安事件信息搜集及处理；另设有支持单位，负责策略规划、国际合作、法律咨询、人事及后勤等。



https://www.secrss.com/articles/24638

以色列国网络力量强大表现

- **疑似世界首个超级破坏性网络武器“震网病毒”制作者，**先摧毁伊朗核工厂1000台离心机，后席卷全球工业界，累计感染20万电脑；
- **全球五大网络力量之一，**用了不到10年时间，构建军、政、企、民全维度的网络攻防体系，互联网安全技术始终走在世界前列；
- **拥有400多家网络安全公司和50个跨国公司研发中心，**安全厂商数量甚至比英国、加拿大、印度、德国、法国的总数还多；超过90%的全球500强企业采用以色列的网络安全解决方案；
- **拥有42家纳斯达克上市的安全科技公司，**而且在全球顶尖科技当中，有一半都购买了以色列的创业公司

https://mp.weixin.qq.com/s/LvLbzaTv8kyNOc65qnNwTQ

安全战略起源

以色列国是世界上最早认识到捍卫其关键计算机系统重要性的国家之一。

1997年，启动了“Tehila”（互联网时代的政府基础设施-以色列的e-GOV项目），目的是保护政府机关与互联网的连接并为政府站点提供安全的托管。

2002年，以色列政府决定（在第84 / b号决议中）确定负责保护以色列计算机系统，定义关键计算机基础设施并建立国家信息安全局（National Information Security Authority, **NISA**）的责任范围，该机构负责监管和建设以色列的关键基础设施、信息安全领域。

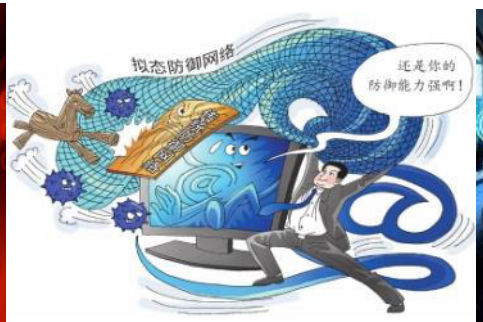
鉴于网络空间的发展和该领域威胁的扩大，以色列总理于2010年11月指示成立一个工作队，以制定国家计划，使以色列跻身引领网络领域的前五名国家。这项名为“国家网络计划”的工作由科学技术高级委员会牵头，该委员会由国家研究与发展委员会主席Isaac Ben-Israel教授领导。成立的特别工作组包括以色列网络领域（研究，开发，国防等）主要机构的代表，并由许多小组委员会组成，这些小组审查了以色列对网络空间的准备工作也必不可少的组成部分。分析在经济，学术和国家安全方面的国家利益。在网络倡议框架内提出的中心建议是建立一个国家网络局，作为服务政府及其首长的咨询机构。国家网络局的主要活动涉及政府在网络领域的总体政策和行动，从平民和军事角度看都十分广泛。

---

https://cyberweek.tau.ac.il/2016/about#bureau

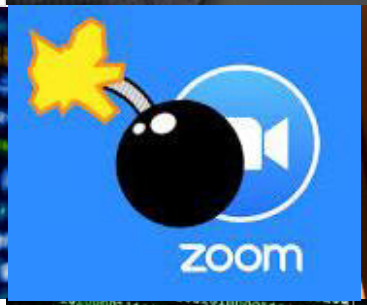
网络安全和国家安全

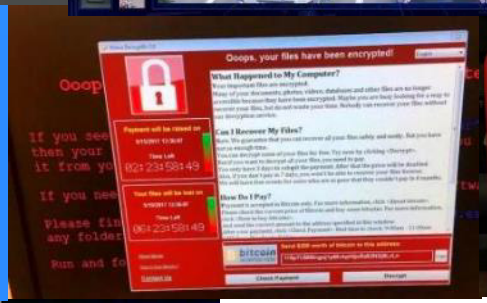

vunerabilty
SSLv3
warning
HACK

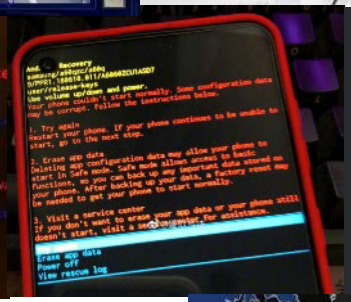

拟态防御网络
还是你的防御能力强啊！


SENSEVIDEO

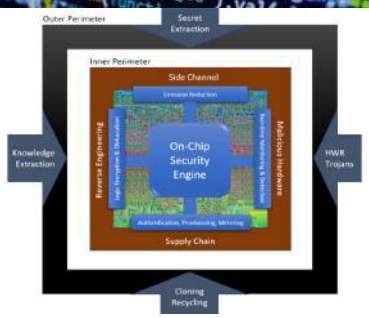

Web scraping


zoom


Ooops, your files have been encrypted!




ctf_


Outer Perimeter
Secret Extraction
Inner Perimeter
Side Channel
On-Chip Security Engine
Knowledge Extraction
HWR Trojans
Supply Chain
Cloning Recycling


Stuxnet
infected

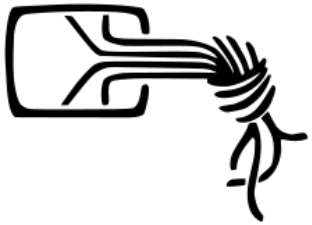

DDoS

网络安全生态圈


DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

公安部第三研究所
The Third Research Institute Of Ministry Of Public Security





中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS


政府参与网络空间安全的必要性

「以色列与中东概览」、「以色列的创新和创业生态圈」、「从安全稜镜看以色列生态圈：人力资本、产业发展和国家基础建设」、「未来的网络安全：物联网、智慧城市、人工智能」、「国家网络安全：从策略到实践」、「国家网络安全生态圈」、「影响运营、线上社群媒体和资讯战」、「网络立法与欧盟一般资料保护法规」、「网络教育：培育网络专业人才」、「挑战：培育网络研发的人力资本」、「资助网络产业：经验教训与未来趋势」、「物联网安全与防护：风险和机会-私营部门的观点」、「网络解决方案的演进-进进退退」、「网络安全和国家安全」、「指挥你的思维迈向成功」，涵盖了以色列的文化及历史演进，导引该国走向高科技建国及推展高科技经济为国本的政策方向与处理原则，也论述了未来的走向。

- **National Security Concerns，国家安全的顾虑**
- **Systemic Impacts，系统化的影响**
- **Market Failures，市场的失败**
- **Beyond the Organization，超越单一组织**

https://report.nat.gov.tw/ReportFront/PageSystem/reportFileDownload/C10703303/001

网络空间安全政策 – 战略文件

- Resolution No. 3611 文件
  - Government of Israel 发布
  - **2011年8月7日**
- IDF Strategy 文档
  - Israel Defense Forces 发布
  - **2015年**
- Resolution No. 3270 文件
  - Government of Israel 发布
  - **2017年12月17日**

网络空间安全政策 – 战略文件（Cont.）

Resolution No. 3611 文件

- Government of Israel 发布
- 《Advancing National Cyberspace Capabilities》
- **2011年8月7日**

- 明确国防部门、安全部门、学术机构和商业团体应相互协作，形成合力，共同推进提高国家网络空间能力，该决议源于国家网络计划；
- 成立国家网络局（Israel National Cyber Bureau, **INCB**）；

Prime Minister's Office
National Cyber Bureau

- 决心提高以色列作为信息技术发展中心的地位，以加强对维护以色列稳定和生产生活必不可少的国家基础设施的防御，并尽可能地增强这些基础设施以抵御网络攻击。

http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf

网络空间安全政策 – 战略文件（Cont.）

前进计划（KIDMA）

- 国家网络局、首席科学家办公室 发布
- **2013年**
  - 资助资金1亿新谢克尔
  - 资助网络安全技术研发，促进技术转移，培育本土企业

前进计划 2.0

- 国家网络局、首席科学家办公室 发布
- **2016年**
  - 资助资金1亿新谢克尔
  - 资助突破性和颠覆性技术研发
  - 资助优秀网络安全企业产品创新和概念验证
  - 促进产业合作

https://www.secrss.com/articles/25657

网络空间安全政策 – 战略文件（Cont.）

IDF Strategy 文档

- 以色列国防军（Israel Defense Forces ,**IDF**）发布
- 《 אסטרטגיית צה"ל 》 以色列国防军战略
- **2015年**

- 必须加强国家安全的网络层面，以与以色列现有的情报，空中和海军优势保持同等水平；
- 保护，收集和攻击行动将在网络领域内进行，以色列必须加强在这一领域的准备；
- 应当建立以色列国防军的网络部门，以发展该国的网络能力；
- 即使在受到网络攻击的情况下，IDF也必须能够运行；
- 网络安全的重要组成部分是发展网络战能力，以增强战略和战术威慑力。

https://www.idf.il/להצ-תייגטרטסא/להצ-תודוא/סירמאמ/

网络空间安全政策 – 战略文件（Cont.）

Resolution No. 3270 文件

- Government of Israel 发布
- **2017年12月17日**

- 将国家网络局和国家网络安全监管机构（National Cyber Security Authority, **NCSA**）合并为一个中心，即国家网络安全指导委员会（National Cyber Directorate，**INCD**）；
- 决心根据第3611号决议，继续提高国家网络部的行动能力；
- 总理内塔尼亚胡的愿景：以色列成为世界五大网络大国之一。

Prime Minister's Office
National Cyber Bureau

סייבר ישראל
Cyber Israel
מערך הסייבר הלאומי - משרד ראש הממשלה
National Cyber Directorate - Prime Minister Office

https://www.gov.il/he/Departments/policies/dec_3270_2017

网络空间安全政策 – 实施框架

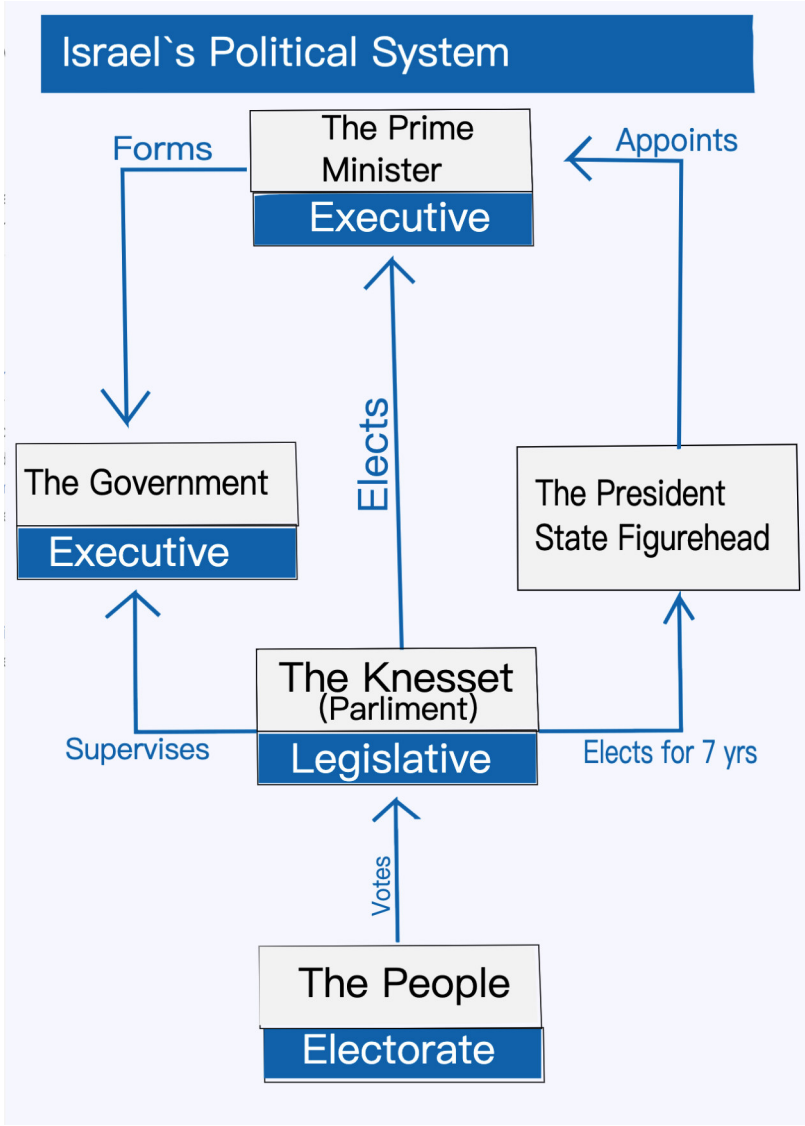
Government Plans, 2017-2018

- Government of Israel 发布
  - **2017年3月5日**

- 概述了国家网络局（INCB）和国家网络安全监管机构（NCSA）在2017-2018年的实施任务;
- 决议NSCA将继续推进创新的网络安全项目；
- 决议将实施由NSCA建立的技术系统；
- 概述了将关键基础设施保护的职责从安全服务转移到NCSA的计划。

http://www.plans.gov.il/pdf2017/index.html

以色列政治顶层设计

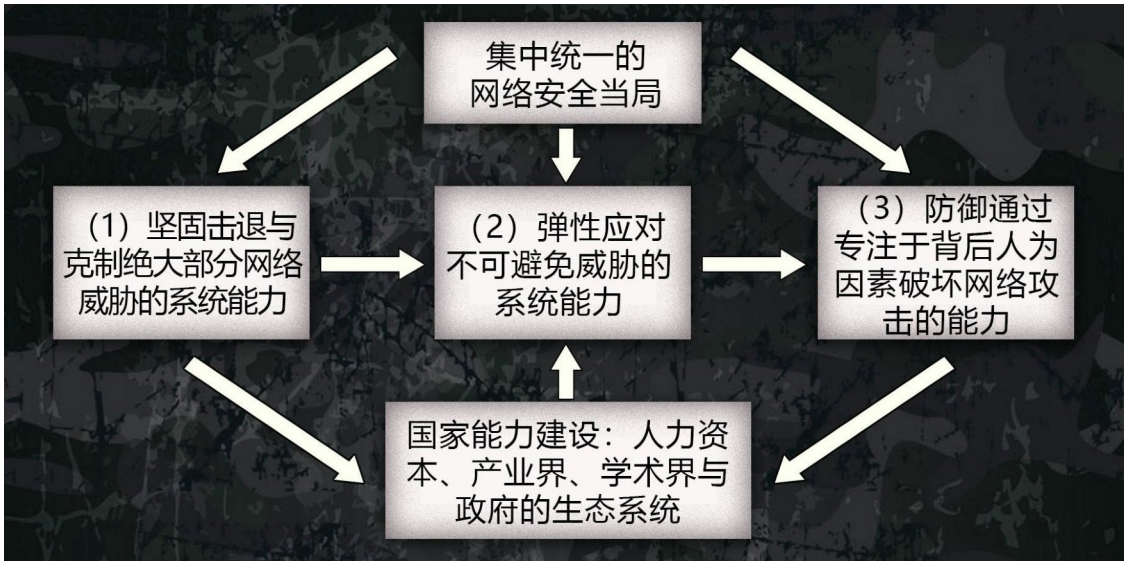


左：鲁温·瑞夫林（REUVEN RIVLIN）：总统。1939年生于耶路撒冷。2014年7月起，任以色列第10任总统，任期7年。

右：本雅明·内塔尼亚胡（BENJAMIN NETANYAHU）：总理。1949年生于特拉维夫。1996年当选总理。2009年3月再次出任总理。2013年3月、2015年5月、2020年5月连任。

https://en.wikipedia.org/wiki/Israel

以色列国家网络战略的三个层次



层次1：军事主导攻击性防御

国防军在以色列网络力量中有着绝对的主导权，“攻击型防御”战略，不可解的地缘政治冲突，让以色列网络战略极端地追求安全。

层次2：军政弹性防御体系

张弛有度，军政协同，对网络安全威胁进行不同层级的响应。

层次3：专注人为因素

网络安全，人是关键。以色列网络力量强大的根源，就是8200等部队不断输出技术型人才，反过来，就是以色列网络安全战略的第三个层次，即人的防御。 以色列通过严密的措施，防御以人本身为漏洞，进行的破坏性网络攻击。

---

https://mp.weixin.qq.com/s/LvLbzaTv8kyNOc65qnNwTQ

国家网络局（Israel National Cyber Bureau, INCB） 2011 - 2017

2011年8月7日成立，2017年12月17日与国家网络安全监管机构合并

该局是总理、政府及其委员会的咨询机构，负责根据法律和政府决议，建议网络领域的国家政策并促进其实施。
该局致力于提高国家在网络空间方面的能力，并提高以色列在应对当前和未来网络空间挑战方面的准备。

它负责改善对以色列国持续正常生活至关重要的国家基础设施的防御，并尽可能保护它们免受网络攻击，同时提升以色列作为信息技术发展中心的地位。 同时鼓励学术界，工业界与私营部门，政府部门和安全界之间的合作。

该局负责促进以色列网络领域的三个中心领域：

- 推进国防建设，增强网络实力；
- 建立以色列在网络领域的领导地位；
- 统筹推进支持前两个任务的流程，必须制定和促进全面和正式的网络战略的实施，阐明和领导国家网络政策。

Prime Minister's Office
National Cyber Bureau

https://cyberweek.tau.ac.il/2016/about#bureau

国家网络安全监管机构（ National Cyber Security Authority, NCSA） 2016 - 2017

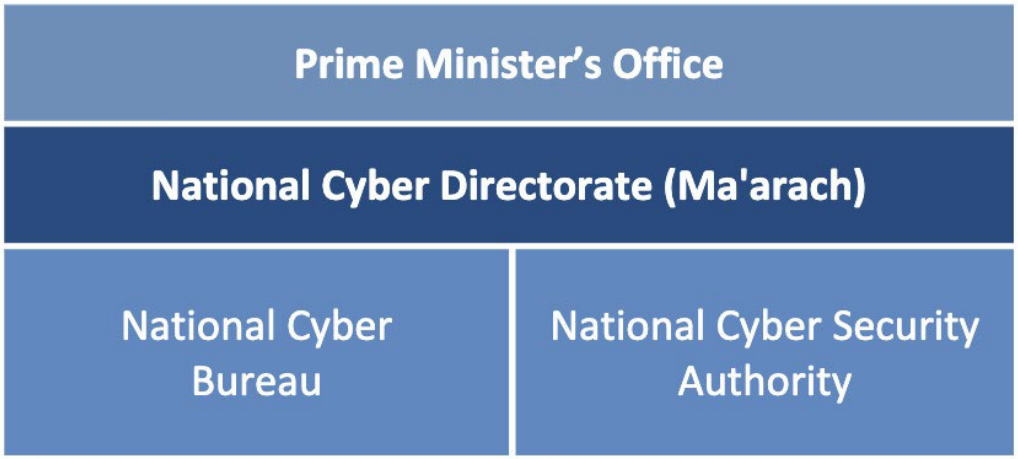
2016年9月成立，2017年12月17日与国家网络局合并

该局是总理、政府及其委员会的咨询机构，负责根据法律和政府决议，建议网络领域的国家政策并促进其实施。

- 由国家承担网络防御的总体责任：监督网络防御行动，以便对网络攻击提供全面的响应，包括实时处理威胁和事件；
- 运营了一个协助中心-网络事件准备团队（The Israeli Cyber Emergency Response Team，CERT），以及CERT-IL处理以色列国的民用网络领域中的网络事件以应对网络威胁，以增强组织和部门在经济中的应变能力

http://mfa.gov.il/MFA/PressRoom/2015/Pages/Cabinet-approves-establishment-of-National-Cyber-Authority-15-Feb-2015.aspx

国家网络安全指导委员会（ Israel National Cyber Directorate, INCD）2017 -



- 负责保护民用网络空间；
- 为所有平民实体以及以色列经济中的关键基础设施提供事件处理服务和指南；
- 致力于提高民用网络空间的弹性。

סייבר ישראל
Cyber Israel
מערך הסייבר הלאומי - משרד ראש הממשלה
National Cyber Directorate - Prime Minister Office

https://cyber.gov.il/

专门机构 - 以色列网络防御小组委员会

- Knesset Subcommittee for Cyber Defense
- 对The Knesset（以色列议会）和以色列议会外交和国防委员会小组委员会负责

https://www.knesset.gov.il/committees/eng/committee_eng.asp?c_id=4

专门机构 –国家检察官办公室紧急、信息安全与网络部

- Department of Emergency, Information Security and Cyber, State Attorney's Office
- 对Ministry of Justice（司法部）负责
- 该司的活动受到许多机构的指导：以色列警察，在人身安全领域，是信息领域的GSS GS5SS – 5758 – 1998年公共机构安全条例"的衍生版本。
- 安全–由政府决策B / 17衍生而来，是GSS法和部长安全领域安全法规的衍生版本。
- 负责起诉和起诉犯有网络犯罪的罪犯

משרד המשפטים

MINISTRY OF JUSTICE | وزارة العدل

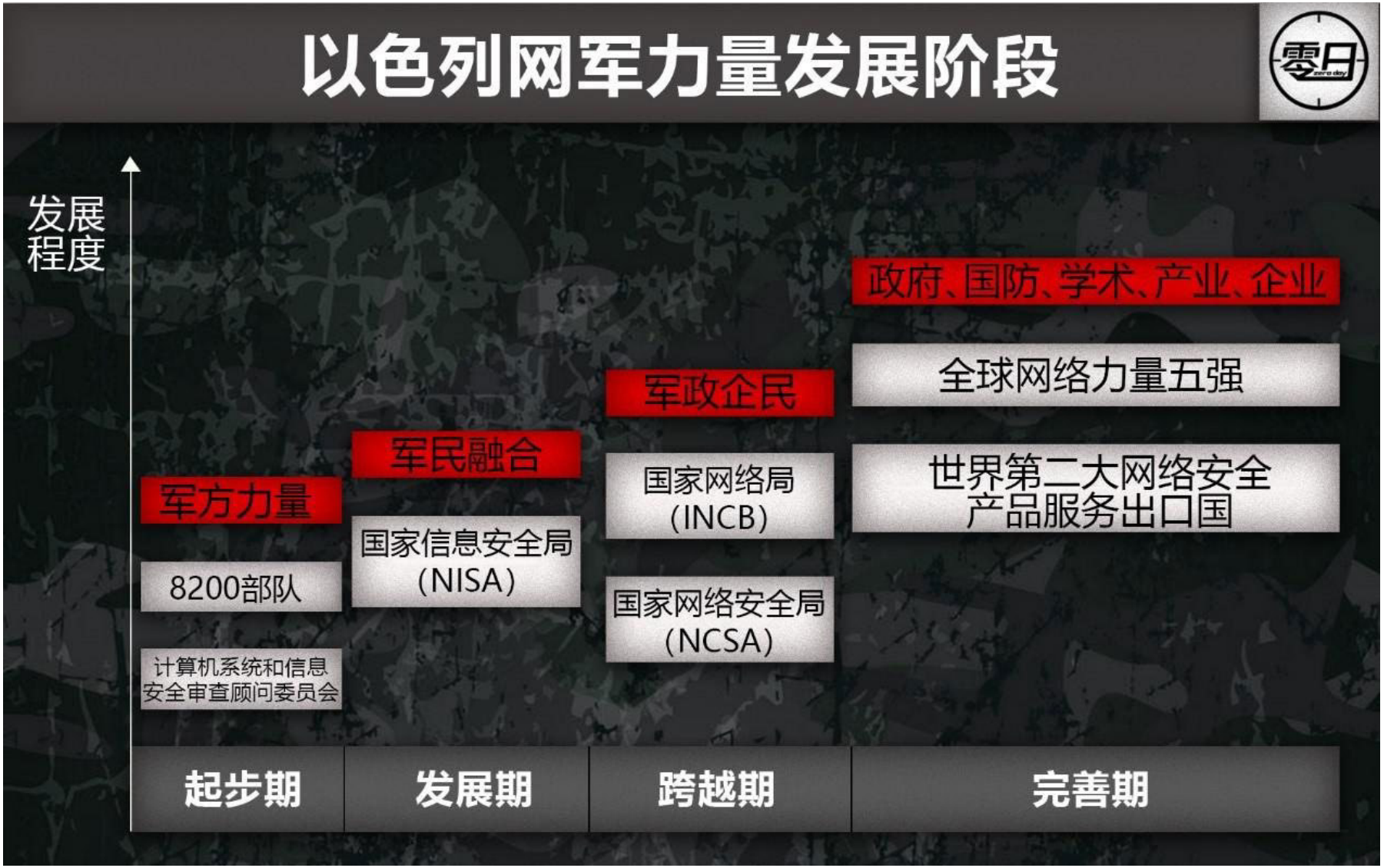
https://www.gov.il/en/Departments/General/moj_security

专门机构 - 以色列"FBI"拉哈夫433

- 以色列警方于2012年设立了一个网络部门，以处理网络犯罪，并作为发展数字取证和证据专门知识的中心协调中心。
- 该部门设在国家警察精英部门拉哈夫433。

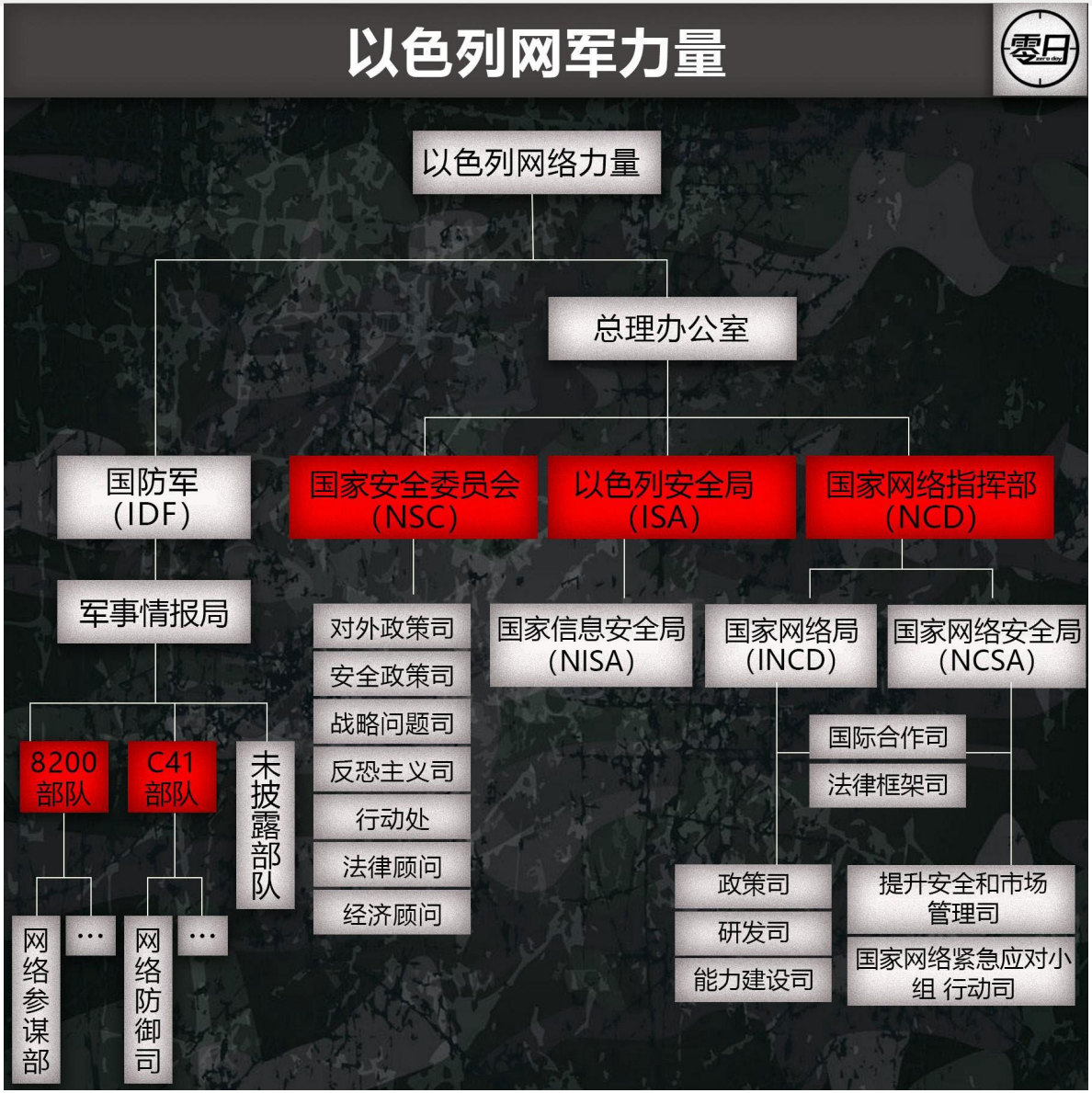
https://en.wikipedia.org/wiki/Lahav_433

以色列宏观组织发展总结



https://mp.weixin.qq.com/s/LvLbzaTv8kyNOc65qnNwTQ

以色列宏观组织发展总结（Cont.）



https://mp.weixin.qq.com/s/LvLbzaTv8kyNOc65qnNwTQ

立法指导文件 - Government Resolution No. 2443

- 2015年2月15日通过
- 解决方案：推进网络安全方面的国家法规和政府领导，规定了一系列法律规范

1. Communications (Telecommunications and Broadcasting) Law of 1982 1982年通信（电信和广播）法
2. Computers Law of 1995 1995年计算机法
3. Electronic Signature Law of 2001 2001年电子签名法
4. Encouragement for Industrial Research and Development Law of 1984 1984年鼓励工业研究与发展法
5. Inclusion of Biometric Means of Identification in Identity Documents and in an Information Database Lawof-2009, 2009年信息数据库法生物识别
6. Law for Regulating Security in Public Bodies of 1998, 1998年管制公共机构安全法
7. Protection of Privacy Law of 1981,1981年隐私保护法
8. Regulation No. 5761-2001 on Privacy Protection (Transfer of Data to Databases Abroad),2001年隐私保护法规
9. Supervision of Security Exports Law of 2007, 2007年安全出口监管法
10. Israel Government, Government Resolution 3058 27 March 2011, 以色列政府第3058号决议
11. Israel Government, Government Resolution 2097, 10 October 2011,以色列政府第2097号决议
12. Israel Government, Government Resolution No. 2444, 15 February 2015, Advancing the National Preparedness for Cyber Security, (Hebrew),以色列政府第2444号决议 推进国家网络安全防范
13. Israel Government, Government Resolution No. 1046,15December2013, The National Initiative 'Digital Israel' (Hebrew),以色列政府第1046号决议 "数字以色列"国家计划
14. Israel Government, Government Resolution No. 3611, 7August 2011, Advancing the National Capacity in Cyberspace, 以色列政府第3611号决议提高网络空间的国家能力

https://ccdcoe.org/uploads/2018/10/IL_NCSO_final.pdf

刑事立法 - Computers Law, 1995

- 1995年7月25日颁布
- 1995年10月25日生效
- 2012年7月17日修改
- 指定对计算机犯罪的处罚，包括破坏或干扰计算机或计算机材料，虚假信息或虚假输出，对计算机材料的非法侵害以及为了实施另一种犯罪而对计算机资源的渗透

https://www.unodc.org/res/cld/document/computer-law_html/Israel_Computers_Law_5755_1995.pdf

现有规章条例支撑网络空间监管

打击网络犯罪

《计算机法》界定了网络犯罪行为，能够有效配合《布达佩斯网络犯罪公约》打击跨国网络犯罪。

数据安全和个人隐私保护

《隐私保护条例（数据安全）》全面关注包括个人隐私、组织数据及数据库在内的数据安全保护。

网络监管

《监听法》《通信数据法》《公共机构安全监管法》等多项法律授权政府合法监管的权利

网络空间安全防御

《网络防御和国家网络指挥部法草案》，从法律层面明确了国家网络防御行为。

cic 工信安全

https://www.secrss.com/articles/25657

绿色网络环境规范

- 国家立法：儿童在线保护：刑法第214条
- 联合国公约：《儿童权利公约关于买卖儿童，儿童卖淫和儿童色情制品的议定书》
- 制度支持：

  教育部：为父母，老师和孩子提供有关在线安全的各种工具

  专门网站：http://safe.org.il/，为父母，儿童和教育者提供安全的互联网

  专门机构：IUCC计算机紧急响应小组负责以色列高等教育中的网络安全。

- 举报机制：CERT和ISOC-IL支持在线举报

https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Israel.pdf

拟定中的法律法规

- 关于以下方面的拟议决议：扩大国家网络部（NCD）的领导作用；
- 授予NCD授权，以发布跨部门和行业的网络安全问题的国家指南；
- 向NCD授予访问私有基础设施和扣押设备的权限，以减轻敌对的网络活动；
- 为NCD与私营部门的合作制定法规和指南。

2016年6月20日，以色列特拉维夫大学一年一度的网络周会议入口处
展示了由数千个受感染的电脑和手机比特组成的“网络空间马”(Cyber Horse)

https://www.cfr.org/blog/look-israels-new-draft-cybersecurity-law

标准建设背景

在商业世界中，标准从不是中立的，而是反映了开发标准的人的实力和创新能力。 制定国际标准是一项极具战略价值的事情，直接影响到创新产品的开发。参与国际标准化过程的目的是使公司曝光并更容易进入海外市场。

1995 年 4 月，以色列政府专门研究“敏感领域”的信息安全管理与防护问题。
随后，正式成立了名为“计算机系统和信息安全审查顾问委员会”的职能机构，
组织以国防部门职业军人为主的专业队伍，为政府研究设计信息安全领域的管理标准。

虽然以色列在网络安全上有着巨大投入，但是多年以来在自己的独立网络安全标准的研究上，仅在2017年拟出了一份草案，是否投入使用以及何时投入使用还是一个未知数。

代表以色列加入国际标准化组织ISO的组织是 Standards Institution of Israel
负责以色列国家的标准研究制定。
该组织确定了以色列国内目前在网络以及网络安全方面所使用的一切标准

THE STANDARDS INSTITUTION OF ISRAEL

https://www.sii.org.il/

使用的国际标准

- 国际组织（美国）：ISO/IEC 27000 系列标准，信息安全管理体系；
- 美国：Sarbanes-Oxley Act，萨班斯—奥克斯利法案，金融证券监管；
- 国际组织（美国）：PCI-DSS，支付卡行业数据安全标准；
- CSA， Cloud Security Alliance，云安全联盟；
- 美国：NIST，美国国家标准与技术研究院；
- 英国：ITIL，信息技术基础架构库；
- 美国：cobIT，信息系统和技术控制目标标准；
- 欧盟：GDPR，通用数据保护条例；
- 国际组织（美国）：ISA/IEC 62443，网络安全标准体系结构；
- 国际组织（美国）： CC认证，信息技术安全评估通用标准

关键基础设施安全防护

以色列政府会就重要的关键基础设施进行辅导及协助，与其共同进行信息分享、安全防护及信息通报，提供经费给中小企业进行网络安全风险评估及网络安全概念宣导。

以色列因长年战火使民众对国家安全具有高度认知，在追求安全的目标下，民间团体较易形成良性竞合关系，如 10 家业者组成以色列网络联盟 IC3，协助发展网络安全解决方案，这也是以色列推展网络安全作业的关键因素之一。

其中，包括Cyberbit、 CyberGym等公司均根据政府政策，关注关键基础设施安全防护和演练验证。CyberGym 公司是由以色列电力公司和网络安全顾问公司 Cyber Control 共同出资成立，主要业务为替政府和私人公司提供网络安全实战演练培训课程，针对不同的产业客户，量身发展一套完整的网安教育训练模式，提供仿真的场地及设备，复制实际工作环境流程，在为期数天的训练过程中，培养学员在实际环境中防御网络攻击及处置的能力。

该公司针对关键基础设施安全的攻防训练，注重 2 个部分，分别是SCADA安全防御认知的建构以及区分角色模拟各种网络安全事件的攻防演练。

https://www.secrss.com/articles/25657

细粒度PDCA管理

Planning:

Stage 1: mapping the defense objectives

Stage 2: required defense level

Stage 3: the right defense

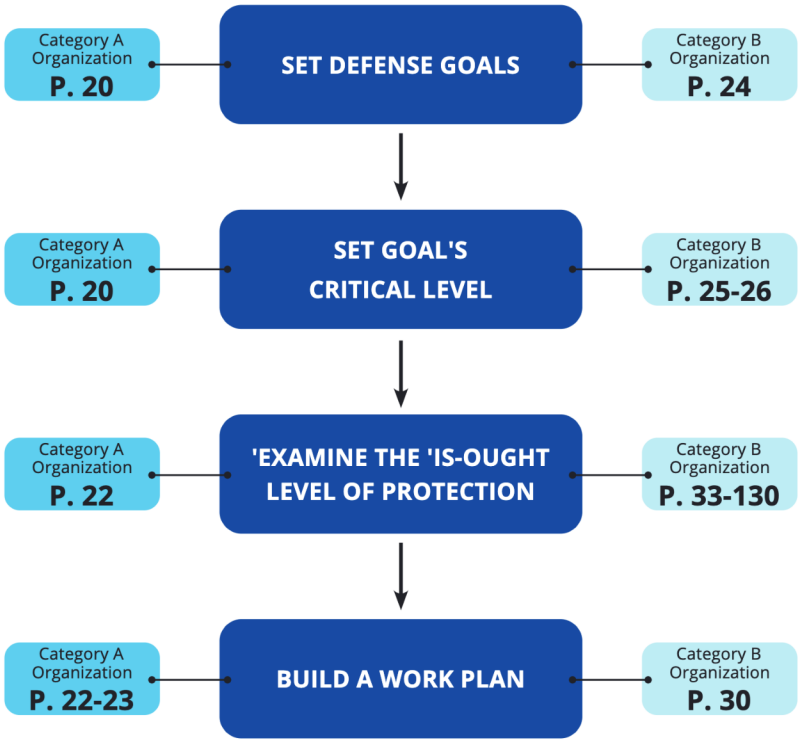
Stage 4: defining existing defense gaps

Stage 5: Work plan

https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/en/Cyber%20Defense%20Methodology%20for%20an%20Oragnization.pdf

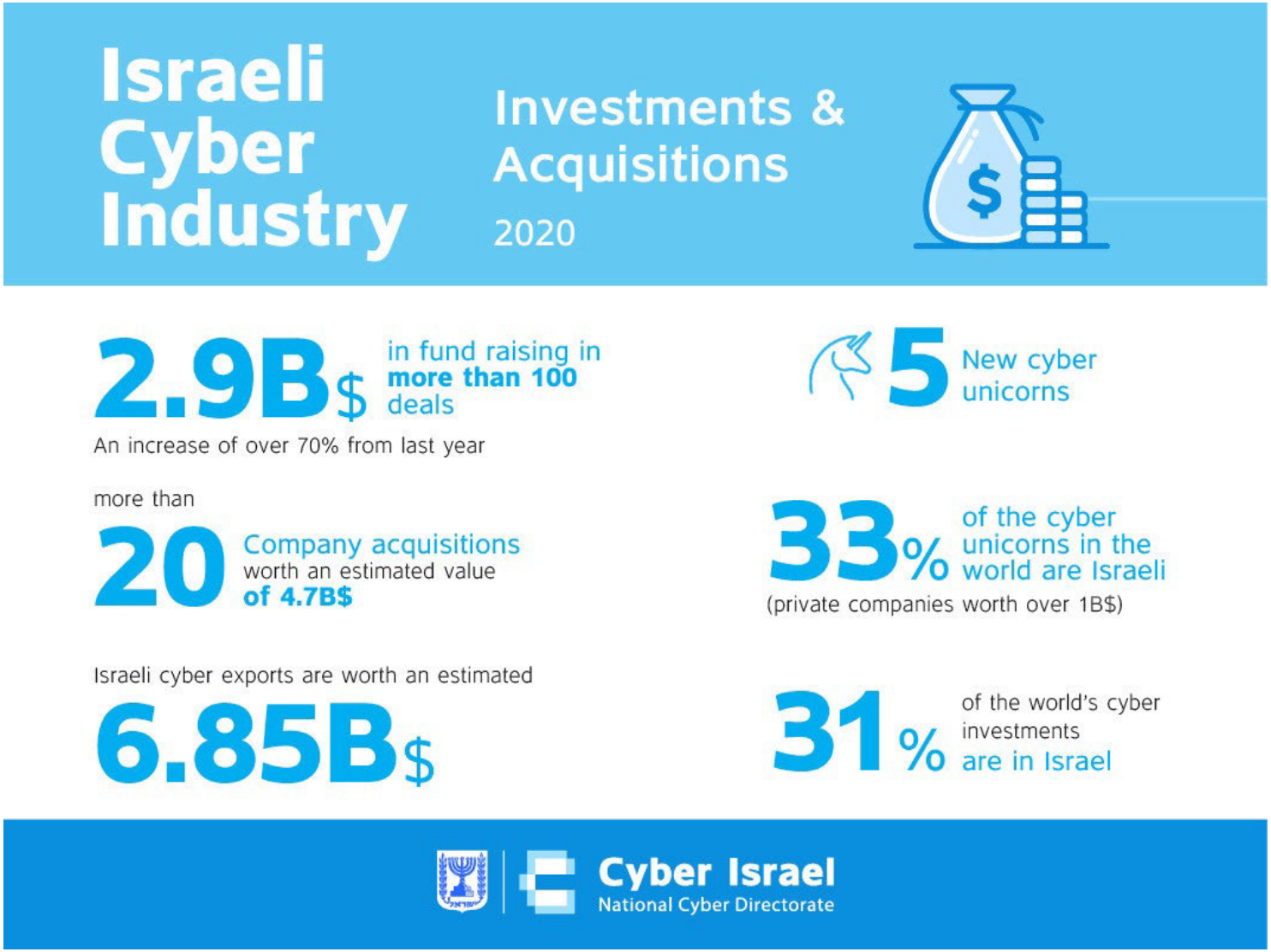
细粒度等级保护

Question	1	2	3	4
1. What is the level of damage caused to the organization following leakage from the asset? **C**	The damage is estimated at: A) Cost of up to NIS 500,000 to the organization. and/or B) An investment of up to two man-months for handling the incident.	The damage is estimated at: A) Cost of more than NIS 500,000, but less than NIS 5,000,000 to the organization. and/or B) An investment of more than six man-months, but less than five man-years, for handling the incident. and/or C) The asset is defined as a database to whom apply the medium security level in accordance with data protection regulations of the Law, Information and Technology Authority. and/or D) There is a clear danger to public health.	The damage is estimated at: A) Cost of more than NIS 5,000,000 to the organization. and/or B) An investment of more than five man-years for handling the incident. C) The asset is defined as a database to whom apply the medium security level in accordance with data protection regulations of the Law, Information and Technology Authority. D) There is a clear danger to human life.	A significant damage will occur, which will include one of the two scenarios below: A) There is a clear and present danger to the lives of many people. B) The estimated economic damage is over NIS 20,000,000.
2. What is the level of damage caused to the organization following the disruption of information existing in the system? **I**				
3. What is the level of damage caused to the organization following a long-term system shutdown? **A**				



https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/en/Cyber%20Defense%20Methodology%20for%20an%20Oragnization.pdf

以色列网络空间安全产业概览



https://www.gov.il/en/departments/news/2020ind

以色列网络安全技术全景

GLILOT CAPITAL PARTNERS

CYBERSCAPE

THE ISRAELI CYBERSECURITY TECHNOLOGY LANDSCAPE

February
2021

- *Source: IVC & Glilot Capital*
- **= Recently Acquired*
- *The landscape of private security companies in Israel*

Identity & Access Management
POLYRIZE* · SILVERFORT · transmit security · TRUSONA · Authomize · plainID · SECRET DOUBLE OCTOPUS · AKEYLESS

Application security
Checkmarx · WhiteSource · enso · snyk · imperva · apiiro · cycode · noname · neosec · NeuraLegion · aqua · SALT · L7 DEFENSE

Security Operations & Threat Intelligence
INTSIGHTS · CARDINALOPS · sixgill · SECBI · Hunters. · XM CYBER · Siemplify · zecOps · Cymulate · SafeBreach · exabeam

Fraud Detection/Prevention
BioCatch · nsknox · payglant · THETARAY · FORTER · EverCompliant · Click-Ins · ACTIVE FENCE · riskified

Email Security
odix · REDEC · CYBEREADY · PERCEPTION POINT · cyberfish · IRONSCALES · BitDam

Web Security
Cyabra · reflectiz · source · GameSec · DEFENSE · perimeterx · NAMOGOO

GRC & Vulnerability Management
anecdotes · cyber OBSERVER · cyberPion · cognni · PCYSYS · at bay · VULCAN · Panorays · ORCHESTRA · vicarius · AXONIUS · KOVRR · CYCOGNITO

Blockchain Security
valid.network · Fireblocks · curv · GK8

Privacy & Data Protection
BigID · UNBOUND · Duality · ITsMine · satori · Mine. · 1touch.io · D-ID · SURFDATA.AI

Cloud Security (IaaS/SaaS)
MITIGA · AtmoSec · ermetic · ADAPTIVE SHIELD · Solvo · alcide · build.security · SafeHouse · Lightspin · WIZ · KINDITE · bridgecrew · Apolicy.IO · AVANAN

Workload Protection
rezilion · Guardicore · portshift * · ARMO · orca security · INTEZER

Endpoint Security
SentinelOne · cybereason · Cynet · deepinstinct · GYTPOL · Cyber 2.0 · HYSOLATE

Network Security & Zero-Trust
perimeter 81 · axis security · algosec · ZERO Networks · Cyolo · QuantLR · TRAPX SECURITY · CATO NETWORKS · illusive · FORESCOUT · semperis

IoT & Industrial Control Systems
Upstream · D-FEND SOLUTIONS · APERIO · GUARDKNOX · ARMIS* · CYBERX* · MEDIGATE · CYBER MDX · ICS security · Karamba Security · shieldIOT · CYLUS · cervello · InfiniDome · IXDen · CYDOME · CLAROTY · Cynerio · radiflow · FIREDOME · ArcusTeam · SEPIO SYSTEMS · REGULUS · nanolock · vdoo · STERNUM · C/O CYBELLUM

产学研、跨学科、多部门结合 - 国家网络安全研究中心项目

学术界是以色列蓬勃发展的网络安全生态系统的重要支柱，因为长期而言，最先进的研究对于维持具有全球领导地位的创新产业至关重要。

为了实现这一愿景，以色列国家网络部与领先的大学建立了六个合资研究中心。这些研究中心正在培养大量的跨学科研究和真正全面的解决方案，而每个研究中心都专注于网络安全的不同领域，并利用现有能力推进新的突破性主题。

以色列国家网络部邀请来自行业，学术界和政府的合作伙伴并利用优良的研发环境与这些研究中心合作。

1. 海法大学-网络安全法律与政策中心（隐私）
2. 以色列理工学院-Hiroshi Fujiwara中心（工程导向）
3. 特拉维夫大学–Blavatnik中心（跨学科）
4. 巴伊兰大学-BIU中心（应用密码）
5. 希伯来大学-HUJI中心（网络协议、国际法）
6. 本·古里安大学-Cyber@BGU（应用研究）

https://www.gov.il/he/departments/general/research_centers

科研经费

以色列的8所主要大学包括魏兹曼研究院既是培养科技人才的基地，也是以色列的主要研究机构。20万名研究生中的20%直接从事R&D工作，8万名大学生中40%在科技相关领域。虽然以色列的大学有较大独立性，但预算的一半仍来自政府。以色列大学也积极参与应研究工作,但基础研究在大学中占统治地位。

一般来讲,大学的基础研究费用来自大学本身的学费、私人捐赠等，政府拨款和企业合同弥补一部分,其余大部分来自研究人员从各种基金获得的资助。每个大学都有各自的“研究主管机构”,为研究人员提供申请资金的机会。

例如,希伯莱大学的研究主管机构每年为该大学争取到4100万美元的资金。该大学四分之三的研究项目属基础研究,其余四分之一项目中的一半是由公司资助的应用研究。项目的资助期限一般为3年,资助金额每年1-8万美元不等。项目申请要经过专门的外部专家委员会严格的评审,竞争非常激烈,中选率只有10%-30%。

以色列著名的魏兹曼研究院院长哈拉里教授认为,研究机构争先申请经费有好处。他指出,魏兹曼研究院原先从工业界只得到400万美元捐助,如今却能得到1300万美元,如果完全靠政府支持,就不会得到这么多的资金以色列的大学对技术转让工作给予高度重视,都设有专门负责技术转让的机构（R&D公司）,负责申请和许可大学科研产生的专利,寻找合作机构和投资者。一般来讲该机构总是代表大学作为合伙人参加到新的合作公司中。

军队作为网络安全人才的孵化器

以色列国防军开发了两种教育方案：

一、一些优秀的高中生参军前获得以色列国防军资助的工程学位，但必须再服役3至5年

二、为期40个月的针对优秀高中生的精英培训项目，由美国国防研发理事会负责。

由于他们在40岁至50岁之前都是国防军预备役部队的一部分，军队也从他们的教育过程中获益。

借助军队力量培养网络安全产业领军人才

- Check Point公司的创始人之一Gil Shewd，以及Palo Alto Networks、CyberArk等公司的创始人或中坚力量都有过在8200部队的服役经历。

军用网络安全技术作为网络安全技术创新的重要源泉

- Check Point早期的技术就源于军用防火墙系统。

社会组织“战友会”为民间初创公司提供“孵化”服务

- 8200部队的“战友会”拥有超过1.5万名成员，他们自愿为初创企业提供指导。

产业促进计划助力军队与企业的合作

- 2012年，以色列国家网络局与国防部联合推出军民两用的网络安全研发计划，即“马沙德计划”。

人才培养思路

面临网络安全安全人才不足问题，以色列政府采取四要素策略，透过教育向下扎根的方式，强化人才的培育：

- 构建多层次多元化网络安全教育体系
- 建立实用的课程
- 促进未来研发领袖
- 加强高中计算机学习项目
- 扩大网络安全科技发展

https://www.secrss.com/articles/24638

小学教育

以色列从小学教育即强调鼓励理性思考，质疑辩论，挑战威权，鼓励思考更好的想法与不断地反省，让创新成为生活的习惯与方式。

建立儿童科学俱乐部，完善科技馆，出版科普刊物，支持与科普有关的项目和开展科学夏令营工作。以提高全民的科技意识，为进步发展奠定良好的基础。

在一些以色列学校，一年级的时候，学习字母，然后学习如何读和写；四年级学生学习计算机编程；而有天赋的十年级学生则在课后学习加密策略、编码以及如何阻止恶意黑客攻击。

https://report.nat.gov.tw/ReportFront/PageSystem/reportFileDownload/C10703303/001

中学教育

在中学阶段，学校即教授信息安全，另规定要专修网络安全，则另需要修习数学课程，以奠定坚实的学习基础。

以色列提供了许多国家级的网络安全研究和培训计划。从高中开始即有计划跨部合作培养，如 Magshimim(Achievers)计划， 这个计划是以色列国防军联合教育部、非政府组织(NGO)之间的人才培养合作计划，重点放在训练高中学生的网络技能。另外参与Gvahim(高地)计划的学生，会被要求 900 小时的学习时数。每天都必须学习程序编写、网络设计实施以及如何对抗网络威胁等。

Cyber Week
June 28th - July 2nd, 2020
Tel Aviv University, Israel

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

https://report.nat.gov.tw/ReportFront/PageSystem/reportFileDownload/C10703303/001

中学教育（Cont.）

在Magshimim项目中，申请者必须首先通过一个关于谜语和挑战的家庭测验，包括数学、逻辑和算法。电脑专业知识是不需要的，甚至可以在网上查找答案或向家长寻求帮助。组织者说，这样做的目的是招收那些不会被挑战吓倒的学生。

接受该计划的学生每周放学后两次会面，每次3小时的课程，每周完成10小时的网络作业，每年参加两次研讨会。

在最近的一次为10年级学生举办的研讨会上，一个由15名犹太教女孩组成的小组参加了一场关于人工智能的讲座。

上课的时候，其中一个女孩正在织橘黄色的绒布。在大厅对面一间昏暗的教室里，一群身穿运动衫和运动裤的青少年弯腰坐在笔记本电脑前，玩着模拟游戏：一个虚构的电脑网络被黑客入侵，他们有45分钟的时间学习一个陌生的电脑代码，重新控制网络，并侵入黑客的系统以确定其身份。“我闯进来了！”一个学生突然惊叫起来。那个虚构的黑客是一个受欢迎的卡通人物。

16岁的沙列夫·古德曼（Shalev Goodman）紧盯着电脑说，他希望入伍后能在军事情报中运用自己的网络技能。“我不是最爱运动的人，”他说。“我确实想给国家一些东西。因此，网络是一件好事。”

项目负责人说，网络道德是强制执行的——利用自己的技能进行黑客攻击的学生将不会被军方录取，并可能毁掉他们在网络行业的未来。

社会人才储备制度

针对政府机关网络人才培训部分，主要区分为 3 级：

第 1 级属于基础的人员，为执行网络安全从业人员；

第 2 级属于进阶的人，可再细分为网络安 全技术专员、网络安全方法专员、网络安全鉴识专员及网络安全测试专员；

第 3 级为专业级的专家。

不同级别的人力需求需透过国家或国际认证制度以获得对应的相关人才，即建立网络安全人才认证制度，由以色列民间机构进行基础、进阶、专业网络安全认证制度的推动，且在未来必须要有执照才能担任网络安全职务，每年依科技进展不断更新知识，并通过实际执行业务自我成长，以因应网络安全环境的日益复杂。

https://report.nat.gov.tw/ReportFront/PageSystem/reportFileDownload/C10703303/001

双边和多边协定

1、布达佩斯公约 Budapest Convention

- 欧洲理事会网路犯罪公约
- 2016年9月1日加入

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=O4NuhJKq

2、澳大利亚-以色列领导人网络安全圆桌会议和网络安全合作谅解备忘录

- 国家网络部签署、总理签署联合声明
- 2017年10月30日达成
- 就政府和商业环境中网络安全领域的挑战和最佳实践对策交换意见

https://www.australiandefence.com.au/defence/cyber-space/pm-signs-cyber-security-mou-with-israel

双边和多边协定（Cont.）

3、亚美尼亚-以色列讨论

- 区域合作部签署
- 2017年7月26日达成
- 关于许多问题的讨论，包括网络安全

https://hti.am/pages.php?lang=3&id=6753&page_name=news#

4、维谢格拉德集团-以色列联合声明

- 总理签署
- 2017年7月19日达成
- 商定除其他外，探讨在国防和国防工业，网络安全，混合威胁，不扩散以及信息和专门知识共享领域进一步加强联合合作的可能性。

V4 CONNECTS
HUNGARIAN PRESIDENCY 2017/2018 OF THE VISEGRAD GROUP

http://www.visegradgroup.eu/calendar/selected-events-in-2017-170203/joint-statement-on-the

双边和多边协定（Cont.）

5、德国-以色列网络政策磋商

- 2017年5月11日达成
- 关于与国际网络政策和网络安全有关的问题的对话

https://www.auswaertiges-amt.de/en/aussenpolitik/themen/170511-kons-dt-isr/289894

6、日本-以色列在网络安全领域的合作协议

- 经济产业大臣签署
- 2017年5月11日达成
- 在该领域增加投资和开展联合活动，建立联合培训计划和联合工作研讨会。

http://mfa.gov.il/MFA/InnovativeIsrael/Economy/Pages/Israel-and-Japan-launch-new-cyber-security-collaboration-11-May-2017.aspx

双边和多边协定（Cont.）

7、洪都拉斯-以色列协议

- 2017年5月11日达成
- 洪都拉斯与以色列国防部之间就许多问题达成的框架协议，包括在洪都拉斯建立国家CERT。

http://www.israeldefense.co.il/en/node/28961

8、非洲七国-以色列合作协议

- 总理签署
- 2016年7月5日达成
- 以色列与7个非洲国家（赞比亚，埃塞俄比亚，乌干达，南苏丹，卢旺达，肯尼亚，坦桑尼亚）之间在安全和经济事务（包括网络安全）方面的合作。

https://www.lusakatimes.com/2016/07/05/israel-and-7-african-countries-agree-to-collaborate-on-security-and-economic-matters/

双边和多边协定（Cont.）

9、全球网络专业知识论坛成员

- 2015年加入
- 一个供各国，国际组织和私人公司在网络能力建设方面交流最佳实践和专业知识的全球平台

https://thegfce.org/

10、捷克共和国-以色列在网络安全领域的联合合作

- 国家网络部签署
- 2014年11月25日达成
- 同意共享有关网络安全威胁和事件以及与其国家网络安全框架有关的其他相关问题的信息，最佳做法和经验教训

https://www.govcert.cz/en/info/events/2455-the-czech-republic-and-israel-signed-a-declaration-on-the-co-operation-in-the-field-of-cyber-security/

双边和多边协定（Cont.）

11、国际电信联盟成员

- 1948年6月24日加入
- International Telecommunications Union (ITU)

https://www.itu.int/zh/Pages/default.aspx

12、联合国成员

- 1949年5月11日加入
- 第五十九个会员国

联合国

https://www.un.org/zh/

I. 战略全局观

II. 组织管理体系

III. 法律法规体系

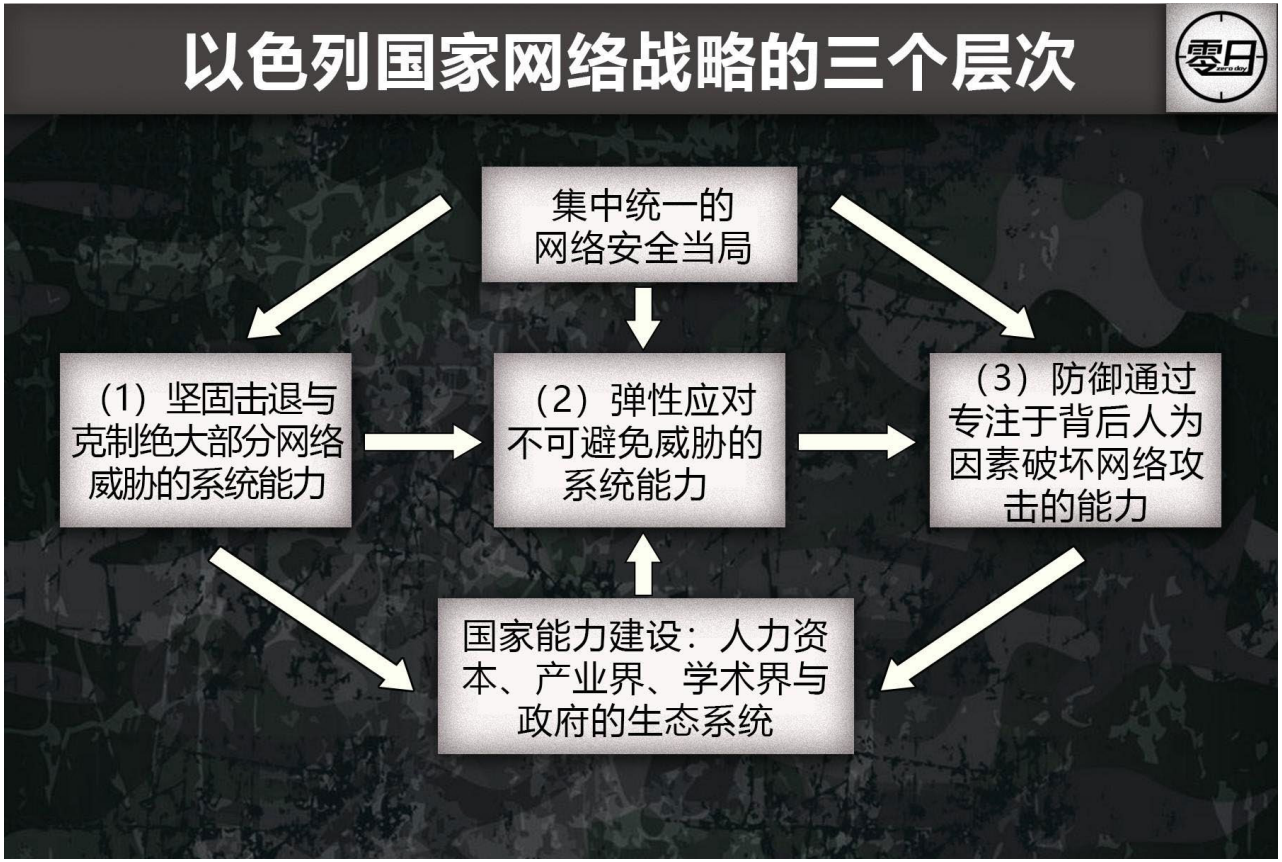
IV. 安全标准体系

V. 技术体系框架

VI. 科研体系

VII. 教育体系

VIII. 合作体系



欢迎批评指正

THANKS