巴（哈）以冲突认知战：网络连接与信息链接之战：

（一）网络连接力之争

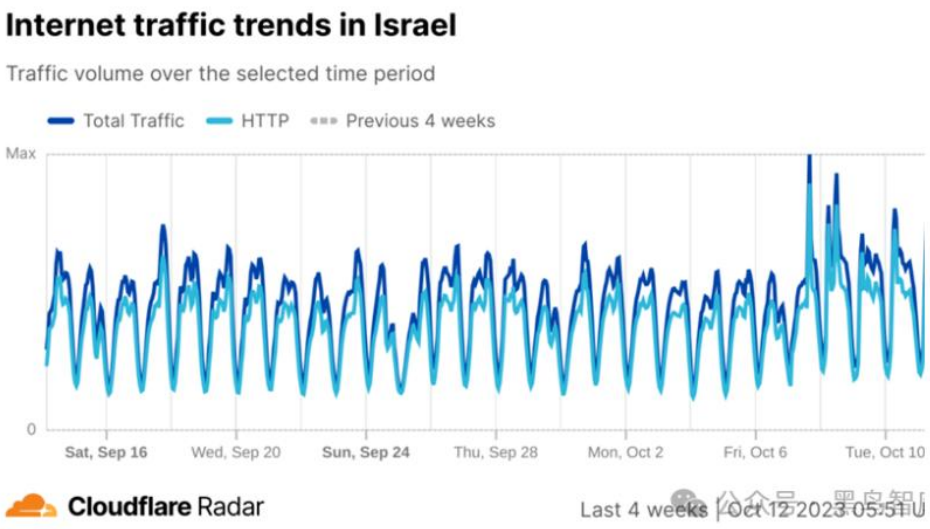
“皮之不存，毛将焉附”。伴随军事冲突的认知战，首先要摧毁或瘫痪敌方的关键信息基础设施，包括物理破坏和网络攻击，使对方成为网络孤岛和信息孤舟。

双方都通过军事硬攻击，试图摧毁对方的信息基础设施，切断对方通讯，阻滞信息传播。哈马斯所在的巴勒斯坦，信息基础设施落后且脆弱，有限光纤网络仅能勉强覆盖部分主要城市，带宽有限且稳定性差；无线通讯基站量少且分布不均，信号强度在偏远地区和冲突前沿地带薄弱。即便如此，以色列还是果断攻击巴信息基础设施，通过轰炸等对加沙断电断网，试图阻断加沙与外界通讯。以色列之所以对巴信息基础设施狂轰乱炸，就是为了阻止加沙居民和媒体向世界讲述悲惨境遇。联合国人权事务负责人特克谴责以色列中断加沙互联网和电信，“使加沙人民无法了解当地正在发生的事，并切断了他们与外界的联系，加剧平民的苦难。” 网络安全监测组织 Netblocks 表示，冲突爆发不久，加沙就发生大规模的单次互联网中断，互联网服务完全或接近完全中断，230 万加沙民众几乎与外界失联。10 月 9 日晚，以色列摧毁加沙地带一处电信大楼，并称将继续轰炸加沙两家主要电信公司 Paltel、Jawal 的总部。10 月 13 日，以色列通信部长

什洛莫·卡希（Shlomo Karhi）宣布关闭在战时“被用来进行哈马斯的宣传、煽动和破坏以色列国家安全”的半岛电视台频道，并表示从14日起切断加沙所有互联网服务（固定及移动业务）。10月27日晚，巴勒斯坦通信部部长希德尔表示，以军轰炸了加沙最后两个国际连接点，加沙内外通信已被彻底切断。以色列在切断加沙燃料和电力供应并轰炸当地两家主要电信公司后，加沙的电力和网络等基础设施服务中断，信息传播渠道阻断，进一步导致哈马斯在舆论上的弱势。哈马斯只能使用简易无线电通信设备，在有限范围维持断断续续的通信。不过，也有一些友好国家为其提供卫星通信频段与设备支持，使哈马斯能一定程度突破信息封锁。哈马斯通过卫星可以向国际社会反映加沙的平民苦难、医疗短缺等情况，争取国际支持与援助。

以色列的信息基础设施建设完善，其境内光纤网络密如蛛丝，基站遍布城乡，4G乃至5G信号覆盖广泛，时刻快速传输着海量信息。但是，哈马斯军事攻击力量较弱，主要是采取小规模袭扰方式攻击以色列的信息基础设施。冲突爆发之前，哈马斯采取无人机偷袭以边境通信基站、监视塔的策略，瘫痪部分以军监控网络，从而麻痹对手并完成突袭行动。由于双方军力悬殊，哈马斯的军事袭扰影响十分有限，以色列的信息基础损失较小。

当以色列对加沙和巴信息基础设施进行军事攻击的同时，大量黑客团体也根据各自利益和意识形态选边站队，展开激烈攻防，针对双方军政、能源、媒体等关键机构网站和数据库发动网络软攻击 [5]，试图瘫痪对方的信息基础设施和网络应用，进而制造社会混乱、扰乱公众心理、传播虚假信息。袭击仅发生几小时，以政府网站 www.gov.il 就无法访问，亲俄黑客团体杀戮网（Killnet）宣布对此负责。紧接着，亲以的黑客团体“印度网络力量”瘫痪哈马斯官网，并宣布攻击巴网络。10 月 11 日，美国威胁情报厂商“记录未来”称，近 60 个组织针对与巴或以有联系的实体发起网络攻击，其中大部分是分布式拒绝服务攻击（DDoS）。根据 2023 年开源信息梳理统计，当时有 20 多个黑客团体宣布支持以色列，80 多个黑客团体支持巴勒斯坦。 在哈马斯武装人员和火箭进入以色列境内数小时内，针对以、巴网站和应用的网络攻击就开始了。有黑客团体表示，他们对以网站实施分布式拒绝服务攻击。Cloudflare 的监测数据显示，以色列互联网流量出现了峰值。

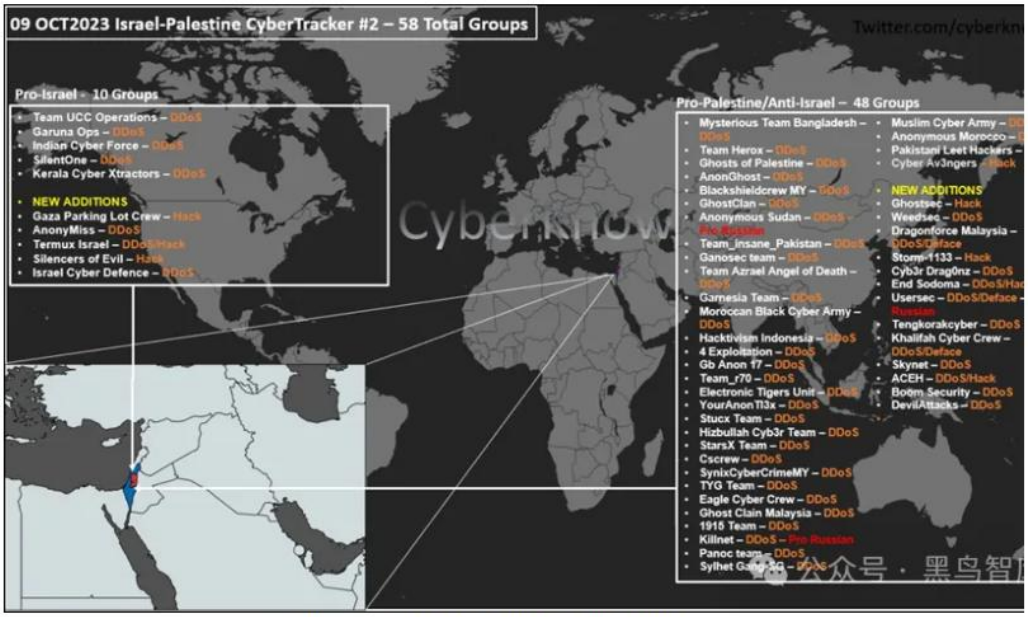


以色列互联网流量激增

支持哈马斯和巴勒斯坦的黑客团体主要来自俄罗斯、孟加拉国、巴基斯坦、摩洛哥和伊朗。他们大量使用 DDoS 攻击、网络钓鱼、篡改网站主页、勒索软件等通用手段，重点攻击以色列关键基础设施、公共服务设施等目标，扰乱以色列社会秩序。据威胁情报平台 FalconFeedsio 统计，到冲突爆发第 5 日，来自沙特、巴基斯坦、土耳其、 也门、黎巴嫩、伊朗、俄罗斯等的黑客团体， 包括“孟加拉国神秘组织”（Mysterious Team Bangladesh）、疯狂巴基斯坦组织（Team Insane Pakistan）、网络行动联盟（Cyber Operations Alliances）、SiegedSec、UserSec 等 77 个黑客团体表示支持哈马斯，对以的政府、司法、金融、电力、军队、通信和媒体等网站发动攻击，以的中央政府、国家安全局、第一大英语报纸《耶路撒冷邮报》等网站瘫痪。例如，“孟加拉国神秘组织”、“疯狂巴基斯坦组织”、“Garnesia 团队”

（Garnesia Team）、“甘诺赛团队”（Ganosecteam）、“摩洛哥黑客网络军”（Moroccan Black Army）、“网络行动联盟”等黑客团体发起代号为 OPISRAEL、OpIsrael V2 等的反以网络攻击行动。亲俄黑客团体，包括杀戮网、“匿名者苏丹”（Anonymous Sudan）和 俄罗斯网络军（Cyber Army of Russia）等，为报复以支持乌克兰，自发实施网络攻击。伊朗黑客团体“网络复仇者”宣称，瘫痪了以色列亚夫内市电网系统、200 个以色列加油站及多拉德发电厂。以色列空袭预警系统也成为攻击目标。 [7]10 月 10 日，Killnet 发帖称，将以色列的全球导航卫星系统、楼宇自动化和控制网络作为最新目标；其还与“匿名者苏丹”对《耶路撒冷邮报》网站（Jpost.com）发起攻击，导致网站瘫痪超 5 个小时。10 月 15 日，CyberAv3ngers 在 Telegram 频道宣布对以加油站控制服务提供商 ORPAK Systems 的大规模网络攻击负责，此次攻击导致 200 个加油泵中断运行，特拉维夫和海法等多个加油站关闭。伊朗背景的 Cyber Av3ngers 侵入以色列 10 个水处理厂，关闭自动监控设施、传感器和控件工业系统，影响赫德拉、帕尔马希姆、索雷克等 10 来个城市。支持哈马斯的黑客团体还一度瘫痪以色列财政部、社会保障机构甚至摩萨德，以及耶路撒冷市政府等 50 多个网站。例如，“孟加拉国神秘团队”与“巴基斯坦疯狂团队”合作，袭击了以色列航天局、港务局、媒体、国防军和金融机构等网站，但

损害不大。[8]“阿克萨洪水网络”宣称，能够侵入以色列国防部，并获取预备役士兵和以军的数百万数据。“疯狂巴基斯坦组织”黑掉以色列新闻、经济、科技和体育类网站并恶意披露网站数据。以色列的军政机构网站、通信服务商以及加油站等民用设施，频繁遭受网络攻击。网络安全服务商瑞德威（Radware）10 月 11 日发布的《以色列与哈马斯冲突后网络攻击加剧》报告，以色列遭受的网络攻击数量显著增加，包括政府网站（占比 36%）及以新闻媒体（10%）、金融服务（5.6%）和医疗（3.5%）等，围绕关键基础设施的网络攻击已成为现代战争新战场。



参与巴以网络攻击的部分黑客团体

对于这些黑客团体来说，摧毁以色列的信息基础设施并非易事。DDoS 仍是其主要攻击方式，而只有利用 API 漏洞的“红色警报（RedAlert）”攻击等少数事件造成较严重危害。例如，10 月 9 日，黑客团体 AnonGhost 攻击以色列应用程序

“红色警报”，并通过其发送有关核弹和火箭弹攻击的虚假警报，一度引发以民众恐慌。后续，还出现冒充“红色警报”的恶意应用。讲俄语的“匿名者苏丹”袭击了以“铁穹”导弹防御系统，干扰系统运行。美国“保卫民主基金会”(The Foundation for Defense of Democracies)网络与技术创新中心高级主任马克·蒙哥马利（Mark Montgomery）表示，“以色列可能是世界上唯一一个拥有与美国类似网络能力的国家”。以色列依靠自身网络能力以及美西方的支持，打造“网络穹顶”， 抵御网络攻击，并针对巴勒斯坦重要目标实施精准网络攻击，在网络空间、认知空间打造不对称优势。 [9]

以色列国家网络局

以色列还拥有技术精湛、装备精良的网络作战部队，在

网络攻防方面占据明显优势。他们善于利用漏洞对哈马斯和巴勒斯坦的通信网络、军事系统以及民用设施发动攻击。以色列通过网络间谍活动、恶意软件植入以及分布式拒绝服务攻击等手段，多次瘫痪巴勒斯坦通信网络，甚至破坏供电供水等民用设施，在网络空间实施全方位打击与威慑。以色列启用具有本国背景的黑客团体，并获得美国、印度等政府力量和黑客团体支持。疑似以色列政府背景的黑客团体“掠夺性麻雀”（Predatory Sparrow）宣布回归，该组织具有较强网络攻击能和专业行动能力，具备精确控制攻击行动并限制溢出影响的能力。该组织曾对伊朗加油站支付系统和钢铁厂成功发动过多次攻击。据 FalconFeedsio 统计，到冲突爆发第 5 日，支持以色列的黑客团体有“掠夺性麻雀”、UCC 等 20 多个，“印度网络力量”（Indian Cyber Force）、“沉默者”（SilenOne）、“UCC 运营组织”（Team UCC Ops）、“甘如那”（Garuna Ops）等宣布支持以色列，对巴勒斯坦关键基础设施实施网络攻击。10 月 7 日起，“印度网络力量”对多个巴勒斯坦关键基础设施进行网络攻击，包括哈马斯官方网站、巴勒斯坦国家银行、网络邮件政府服务和电信公司网站、购物网站等。随后几天，该组织对政府、通信、金融等行业网站进行攻击，还攻陷巴勒斯坦学校、医院等的 200 多个网络设备。“印度网络力量”还联合 Team UCC Ops、Garuna Ops 等印度黑客团体，攻击支持巴勒斯坦的国家，如

印度尼西亚、巴基斯坦和孟加拉国等的网站。9 日，印度黑客团体对巴勒斯坦国家银行和电信公司等发动网络攻击，导致巴国家银行等网站瘫痪。 同日，“掠夺性麻雀”侵入伊朗关键基础设施。该组织曾对伊发动多性破坏性攻击，包括攻击伊加油网络支付系统、钢铁厂等。该组织活动具有高度专业性，被认为具有复杂先进的攻击能力，也具备精确控制行动并限制活动溢出影响能力。据伊朗国家电视台 12 月报道，“掠夺性麻雀”入侵伊朗加油站系统，并恶意披露部分加油站内部文件。11 日，“甘如那”对巴勒斯坦实施 DDoS 攻击，恶意篡改网站内容。ThreatSec 宣称攻击了巴勒斯坦的互联网服务提供商 AlfaNet，一度控制加沙的 5000 多台服务器。这些网络攻击主要采取 DDoS 攻击，目标包括哈马斯主要网站以及巴勒斯坦的商业网络、广播公司、发电公司、投资基金、Al-Haq、网络邮件政府服务和交通部等。

面对以色列对信息基础设施的攻击，巴勒斯坦的网络攻防力量相对薄弱，主要以防御为主。他们通过构建防火墙、加密通信线路、培训网安人员等方式，试图抵御以色列的网络侵袭。同时，巴勒斯坦尝试利用网络技术开展情报收集、舆论宣传及国际形象塑造。巴勒斯坦通过社交媒体平台、网络新闻发布等渠道，向全球传播战争真相、以军暴行以及民众苦难，争取道义支持，发出呐喊声音。

由于俄罗斯、伊朗等支持巴勒斯坦，美国及其盟国支持以色列，这些国家也成为黑客团体的攻击目标。“巴勒斯坦幽灵”号召全球黑客瞄准以色列和美国的基础设施，还声称对印度进行网络攻击。10 月 9 日，印度政府网站遭到网络攻击。10 月 12 日，有黑客团体以韩国支持以色列为由对韩外交部驻全球多个国家网站发起攻击并导致瘫痪。“红魔（Red Devil）”则成功渗透伊朗电网，造成其全国大范围电力中断。

总而言之，黑客团体在复杂动机驱动下采取多样化网络战策略，包括 DDoS 攻击、网站篡改和数据泄露，目的是切断网络服务、窃取情报和阻断信息流动或传播己方信息，甚至扰乱人心。值得注意的是，工业控制系统（ICS）成为主要攻击目标，因为这类攻击会产生运营中断、安全隐患、经济成本和声誉损害等严重影响，并对对方民众心理情绪、战斗意志等产生扰乱性影响，兼具软硬杀伤力。亲巴黑客团体“网络复仇者”攻击以色列城市电力系统，造成一系列电力故障。“所罗门士兵”侵入以色列最大的面粉生产厂的生产线控制系统，一度造成食品供应中断。“伊朗网络游击队”通过侵入以色列生产的控制器，破坏了美国阿里奎帕市供水系统的增压水泵，导致设备被关停。12 月，“匿名者苏丹”

持续对以色列工业控制系统、全球导航卫星系统、楼宇自动化和控制网络、现场总线技术工业控制系统等实施攻击，造成以 GPS 系统离线。据微软发布的《2023 年数字防御报告》，Storm-1133 对以的攻击早在哈马斯发动突然袭击前就已开始，攻击目标包括以色列能源、国防和电信行业。Storm-1133 还侵入以国防部网站窃取数据。

这些网络攻击的技术门槛低、实施成本低、隐蔽性强。同时，数据擦除攻击更具针对性复杂性。例如，亲巴黑客团体使用数据恶意擦除器 BiBi-Linux-Wiper，其已在俄乌冲突中被使用，可以“擦除”数据、覆盖数据或损坏数据。黑客团体还通过 DDoS 攻击、篡改攻击、窃取攻击等手段，渗透以巴关键网络目标，造成网络瘫痪、文件泄密、虚假信息等后果，会引起民众恐慌和社会动荡。 [10]冲突爆发第一周，以巴约有 100 个网站遭到 SQL 注入，导致网页篡改污损。

支持以色列的黑客团体则将巴勒斯坦骨干网络的 DNS 服务、电子邮件服务列为攻击目标，这些信息基础设施一旦瘫痪，会导致整个区域的域名解析，导致网站、电子邮件服务等无法访问，造成网络通信中断。同时，这些黑客团体为制造社会生活秩序混乱，干扰对方民众情绪和信心，把民生设施作为重点攻击目标，既包括传统网络攻击的重灾区，如军

政（以国防军、防空系统）、金融、能源、通信等领域，也包括服务民众生活的民用设施，如社会福利团体、楼宇自动化和控制网络(BACNet)、装修设计、酒类售卖等网站。

此外，网络攻击直接延伸至认知域，针对网络话语权展开激烈争夺。黑客团体控制了大量僵尸账号，散布虚假信息，进行认知宣传，制造恐慌。 10 月 12 日，哈马斯短暂劫持了特拉维夫的两个用于视频广告的智能广告牌，播放了反以挺哈的镜头。哈马斯在也门和阿富汗的支持者向以色列人发送威胁短信。以色列官媒则积极抢占网络传播平台，引导国际舆论，旨在影响国际认知走向，博取国际同情和支持，为军事行动争取“法理道义”。

总体而言，由于支持巴勒斯坦的黑客团体数量更多，以色列总体处于守势，但其凭借出色的舆论动员、领先的国防力量和发达的网络安全产业（如领先网络安全公司 Checkpoint、Radware）等优势，基本维持住了本国基础设施运行秩序，并展开了有效反击。由以退伍军人组建的网络安全公司 HUB 提供先进解决方案，保护敏感数据和关键基础设施。Check Point 公司推出协作平台“Horizon Playblocks”，自动遏制攻击并防止其扩散。网络安全初创公司 Code Blue Cyber 与网络危机管理公司 Gitam BBDO 联合成立“平民作战

室”，通过面部识别技术将社交媒体的人员图像与以官方数据库及失踪者家属提供的照片比对，两周内确认约 60 名失踪人员身份,并在网上打击谣言和不利言论。Akooda 推出“铁之言”（Words of Iron）的 AI 应用，可以加强支持以色列的社交媒体帖子和叙事，并发现批评以色列的内容。以色列还通过间谍软件公司，窃取约 100 万部巴勒斯坦民众手机的数据，监视加沙人群活动。尽管以网络情报公司 NSO Group 和 Candiru 被美国列入黑名单，但它们仍按照以色列要求快速升级间谍软件功能,窃取手机信号以评估哈马斯突袭时的现场人物，分析攻击前后手机信号移动方式。NSO 还建立“战争室”，负责追踪、解锁被谋杀或失踪人员的手机，以及嫌疑人的手机。以色列开发的“福音”人工智能系统，可以分析手机短信、卫星图像和无人机镜头等多种数据源。

值得注意的是，以哈还展开加密货币战。以色列 Fireblocks、MarketAcross、Blockchain B7 等区块链公司联合发起“加密货币援助以色列”项目，阻止加密资金流向哈马斯。以色列初创公司 Lionsgate Network 定位和拦截哈马斯的加密钱包，迅速冻结约 100 个账户。以警察网络部门 Lahav433 还与加密货币交易所币安（Binance）合作，冻结了数百个哈马斯的加密货币账户。Lahav433 与以国防部、国安局和其他情报机构合作，阻止恐怖组织使用加密货币渠道。

以网络安全厂商被动员起来保护本国的数字边界免受黑客攻击。以大型科技企业成员组建志愿者队伍“以色列科技卫队”，利用网上帖文线索搜寻人质和失踪人员，还致力保护关键服务，例导弹袭击预警应用程序。

网络战成为现代战争的首要选项。在网络信息技术深度融入社会生产运转、民众工作生活的当下，网络空间在冲突爆发时已成为各方争夺的焦点。由于其成本低、隐蔽性强、溢出效应显著，在损毁敌对国关键信息系统，窃取军事情报，瘫痪互联网、交通等关键基础设施方面已成为现代战争的首要选项。俄乌冲突和巴以冲突中表现尤为明显。

综上可见，网络战和认知战已经成为现代战争的重要组成部分，且两者相互交织渗透。黑客组织将卷入所有重大地缘政治冲突，此类非国家行为体选边站队会影响网络攻防和认知态势。DDoS 攻击成为国家级网络攻击重要手段，而针对关键基础设施的攻防对抗成为网络战和认知战的关键所在。