Full dimensional Tradecraft of Tactical Intelligence Analysis

情报攻歼全维战法

——战术研判方法模型与实战操作

◎崔嵩 著

CPPSUP 中国人民公安大学出版社

Full dimensional Tradecraft of Tactical Intelligence Analysis

情报攻歼全维战法

——战术研判方法模型与实战操作

崔 嵩 著

（公安机关内部发行）

中国人民公安大学出版社

·北 京·

图书在版编目（CIP）数据

情报攻歼全维战法 / 崔嵩著. —北京：中国人民公安大学出版社，2012.10
ISBN 978-7-5653-1003-4

Ⅰ.①情… Ⅱ.①崔… Ⅲ.①军事情报—研究 Ⅳ.①E87

中国版本图书馆 CIP 数据核字（2012）第 222040 号

情报攻歼全维战法

——战术研判方法模型与实战操作

崔 嵩 著

出版发行：中国人民公安大学出版社
地　　址：北京市西城区木樨地南里
邮政编码：100038
印　　刷：北京蓝空印刷厂

版　　次：2013 年 1 月第 1 版
印　　次：2013 年 1 月第 1 次
印　　张：36
开　　本：787 毫米×1092 毫米　1/16
字　　数：725 千字

书　　号：ISBN 978-7-5653-1003-4
定　　价：98.00 元　（公安机关内部发行）

网　　址：www.cppsup.com.cn　www.porclub.com.cn
电子邮箱：zbs@cppsup.com　zbs@cppsu.edu.cn

营销中心电话：010-83903254
读者服务部电话（门市）：010-83903257
警官读者俱乐部电话（网购、邮购）：010-83903253
公安图书分社电话：010-83905672

以信息化之火

熔锻传统侦查思维的铁流

铸成全维战法之剑

剑锋所指

引领战术情报组织、机制、系统、资源的变革

炼就信息化条件下的精准战力

自序及导读

当前，各国警方、安全、军方正面临着共同的情报转型，以情报主导的侦控执法行动日渐成为警方打击犯罪的主流样式，同时也正在成为军队、安全（如英国的军情五局、美国的国土安全部、以色列的辛贝特）等各强力机构应对非传统安全威胁的勤务模式。实现这一转型，既要求实战人员创新求变，展开合理的想象，充分挖掘信息化所赋予的潜能，更要对传统侦查模式展开哲学思考，回归其中最为本质的部分，以信息化之火熔锻传统侦查思维的铁流，铸成全新的战法之剑，并以剑锋指引，主导情报安保工作的组织、机制和信息系统变革，锤炼成信息化条件下的精准战力。

本书，正是打造全新战法之剑的一种尝试。它可以被看作是2008年出版的《再造公安情报》一书的战术版续集。由于《再造公安情报》篇幅所限，虽然其提供了情报分析方法模型的总体框架，但在战术情报层面，许多研判工具没有充分展开。全维战法正是在此基础上发展而成的战术情报知识体系，是作者对国内外情报分析理论与实践最新发展进行持续跟踪和系统思考的结果。本书初衷是从方法论和模型角度对当前纷纭多样的战术情报分析理论和工具进行重新组织，努力实现战术情报分析方法的模块化、标准化和体系化，并尝试提供一套通用的术语，希望藉此为战术情报分析知识体系的交流和共享提供一个相对稳固的知识平台。

一套体系化的战法既是侦查研判的完全攻略指南，也是专案指挥的策略库；既是信息化警务在战术层面的顶层设计方案，也是战术研判平台的功能架构设计书；既是研判培训教程，也是传统侦查思维与网上作战的通用理论模型；既是通用兼容的技战法术语体系，也是强力机构应对非传统安全威胁的战术情报操作指南。这也正是全维战法的定位。

基于上述定位，本书的目标读者包括以下十类群体：

- 警务决策者及信息化建设者
- 警学、侦查学、警务情报学界的专家、学者
- 专案指挥人员
- 综合、警种情报部门主管
- 研判情报技战法的创新者

■ 侦查、情报部门实战人员
■ 情报平台建设者及软件供应商
■ 情报培训机构及教官
■ 院校学员及新手
■ 安全、军情、反洗钱部门的反恐、安保情报人员

下面是分别写给这些读者的话：

• 致警务决策者及信息化建设者

全维战法 = 战术层信息化警务顶层设计的原型

国际警务趋势和国内警务改革经验均表明，信息化仍将是今后一段时间警务发展变革的主旋律之一。尤其是警务信息化建设进入深水区后，“摸着石头过河”的边用边建模式已经落伍，取而代之的是对信息化警务的顶层设计。当前，顶层设计更多停留在口号层面，而很难推出具有操作性的举措。其难点在于顶层设计的目标很难明确：信息化之后将会发生什么、走向何方、如何变化等等，没有现成的答案。全维战法的出现，为战术部分的信息化警务建设提供了明确的目标和指向。全维战法首先对信息化之后的研判操作进行了系统化的定义描述，提供了战术层信息化警务的“原型”。在此基础上，本书第五篇以全维战法为“体”，以战役应用、系统建设、机制规划、组织重构为“用”，“体”“用”结合，相互砥砺，结合各地的创新实践，对信息化警务的协同机制、战役模式、研判队伍、平台架构作出了全景式的总结和设计。这些构想一旦能够变为系统化的创新实践，必然会推动信息化建设的大跨越，从而摆脱“以用促建”的窠臼，实现由“造什么武器打什么仗”到“打什么仗造什么武器”的转型。

• 致警学、侦查学、警务情报学界的专家、学者

全维战法 = 理论 + 实战

理论与实践的脱节问题一直被关注，但始终未能被彻底解决。理论对实战指导乏力，实战中的理论总结不足，这些问题长期困扰着学界和实战界。全维战法是整合理论与实战，使两者回复一体，并推动理论界与实战界对话的一种尝试。它既是对侦查思维的系统化理论总结，也是对现有侦查实战操作和心理体验的体系化描述，对实战应用、顶层设计、平台建设、机制创新、战役组织、机构重组及战法创新具有参考价值。对于侦查学界而言，全维战法着眼于侦查过程的核心部分——研判战法，按照侦查人员在实战中的顺序思维习惯，对原有的侦查学知识进行了重组，形成了与原有侦查学理论表述体系完全不同的新范式，希望能对信息时代的侦查学理论升级转型有所补益。对于那些有志于在警务情报理论方面有所建树，但暂时无缘融入实战的研究人员而言，全维战法提供了了解研判实战底层运作的窗口，希望能为其更深层次的情报理论研究搭桥铺路。

值得一提的是，全维战法中虽然吸收了西方情报界的个别技法（如第二篇第 8 章

中的网络测量［J24］），但从总体上看，与“国际刑警”体系、“ANACAPA”体系、“IALEIA”体系等重数据操作、轻研判思路，重单项技法、轻流程组合的西方研判知识体系完全不同，全维战法是一套兼顾技法、战法和战法组合的模式，也是为数不多的一套全过程、全层次、模块化的战术研判知识体系。这样一套战法的诞生，客观上表明了我国的警务信息化和战术情报水准有可能与西方总体较为接近，甚至在某些方面有所超越。

- 致专案指挥人员

全维战法 = 全方位的侦查策略库

战术研判构成了专案侦查的核心流程，全面缜密的研判思路则构成了专案指挥的核心思路。由于各类重特大案件的犯罪分子、团伙行事手段日益诡秘狡诈，决定破案的各种偶然、必然因素交织影响，专案侦查的难度不断增大。传统意义上粗放式的原则指挥、会议指挥和按部就班的案情分析会、摸底排队显然已不能适应实战要求。现代条件下的专案指挥人员必须综合考虑各种信源的应用，融合网上网下各类情报手段，全力捕捉各种破案机会，全面覆盖各侦查阶段，提出一整套多路并进的侦查路径，部署多个团队同步开展侦查研判行动。这样一套系统化的路径正是全维战法体系中的“组合定式”和“任务模式”两个层次研究解决的问题。在第四篇第 16 章中，全维战法列出了串并分析的 24 条路径、拓展关系人的 14 条路径；在第 17 章列出了刻画作案人特征的 18 条路径、摸排作案人身份的 10 条路径、由案直接关联到人的 11 条路径、识别可疑对象的 8 条路径；在第 18 章列出了查证嫌疑人的 17 条路径、分析犯罪团伙特征的 10 条路径、排查目标人员其他身份的 9 条路径、追踪目标人员位置的 6 条路径；在第 19 章，全维战法明确了暴力、侵财等案件侦查的 9 个环节、刑嫌管控预警的 9 个环节、有组织犯罪侦查的 6 个环节、刑嫌人员审查的 5 个环节、在逃人员追缉的 8 个环节。这些环节、路径一经与专案实战结合，可立即激活成为侦查策略库和专案侦查方案，为专案指挥人员提供参考。

- 致综合、警种情报部门主管

全维战法 = 战术研判流水线 + 资格认证标准

全维战法意味着战术情报机构及研判队伍在组织结构、职能分工、组织方式、能力培养等诸多方面的深刻变化，这些变化可以归纳为多源手段合成化、机关职能实战化、警种联动协同化、组织方式精细化等方面。全维战法不仅为战术研判人员提供了能力进阶的指南，也是衡量战术研判人员知识能力的客观标准之一，它的出现使得对战术研判人员的资格认证和等级评定成为可能。同时，由于全维战法对战术研判知识进行了模块化、标准化、流程化的组织，意味着专业化的职位序列设置、团队编组和流水线运作成为可能。第五篇第 23 章对研判队伍转型进行了设计和展望，希望藉此加速推进研判队伍的专业化进程，并促进侦查、综合情报、技术情报部门的横向一体化

联合，更好的促进警种联动。

● 致研判技战法的创新者

全维战法 = 通用兼容的技战法术语体系

在全国各地网上作战专家、业务骨干的推动下，研判技战法的创新仍然方兴未艾。然而在层出不穷的创新背后，通用术语的缺乏和战法系统化的不足，已经成为阻碍研判知识融合的瓶颈。同样的技战法在各地称谓不一，单项的技战法只有在面对特定条件时才能发挥作用，缺乏普适性，甚至到底何谓技战法，都没有形成共识。战法知识的支离破碎不仅限制了研判战法的跨地区、跨警种交流，也对更高级的战法创新形成障碍。全维战法致力于结束战法知识的分崩割据状态，将原本平铺于地面的技战法灌木丛嫁接为战法体系的参天巨株。本书首先在第一篇第 5 章对技战法的内涵外延做出了明确界定，给出了全维战法的总体框架，并在接下来的二、三、四篇中对全维战法各模块组件进行了结构化的实例展示。由于全维战法的“全兼容”特性，几乎所有各地的技战法都可在全维战法体系中找到对应的方法模型。本书第四篇的附录给出了全维战法与部分主要技战法之间的对照表。希望藉此，各警种、各地区之间的技战法知识壁垒得以消除，冗余的技战法术语得以合并和归一，知识共享和学习交流的成本得以大幅度降低，并为今后更为高端的研判技战法创新打下更为坚实的基础。

● 致侦查、情报部门实战人员

全维战法 = 全任务、全过程、全信源实战指南

单项的技战法对日常实战的直接指导意义是有限的，战法与实战具有相当的距离。单项的技战法通常只能适用于特定类别的案件，或特定种类的数据资源。但在实战中，实战人员可能会遇到各式各样类型的案件，也必须综合利用各类数据资源，研判任务很少恰巧符合单项技战法所框定的条件。要想使战法与实战合一，必须将单项战法组合成全面覆盖各类任务、贯穿各个环节、适用各类数据资源的体系。全维战法正是这样一套涵盖了数据操作、逻辑思维、基本战法和战法组合的体系，基于其全任务、全过程、全信源的特性，全维战法将既可以用来解读各类侦查、预警、追缉任务的研判过程，也可以用于辅助实战。第六篇以实际案例展示了全维战法在侵财、暴力案件侦查以及有组织犯罪经营侦查、管控预警、刑嫌审查、在逃追缉等各类任务中的实战应用，全面涵盖了人员轨迹、车辆 GPS、银行交易、通信等各类轨迹、交易、关系数据和重点人员库、案件库等背景数据和视频数据，不仅可供实战人员系统掌握技战法操作和研判思路，更有助于初学者感受复杂多变的实战局面。

● 致情报平台建设者及软件供应商

全维战法 = 战术研判平台的功能架构设计参考

由于信息化条件下的战法探索创新层出不穷，平台应用常常成为自身需求变更的动因，某一版本的情报平台与实战一旦成功结合，就立即会催生新的战法，衍生新的

功能需求，从而使得原有的设计显得过时。由于平台需求频繁变更，平台建设始终处于需求－研发－运行－培训－应用－新需求－再研发－运行－重新培训－……的短促而无休止的循环状态。对于平台建设者而言，意味着更长的建设周期、更高昂的建设成本；对于软件供应商而言，则意味着为以前的设计所投入的开发人工量被无情浪费。全维战法的出现，有望使平台建设者和软件供应商跳出“边建边用”的低级循环，直达现有技术条件下的平台建设目标节点。本书第五篇第22章给出了基于全维战法的平台架构及功能组群，并对各模块进行了功能描述。不仅为平台战术板块提供了初步定型的目标功能，而且为平台的模块化功能设计提供了参考，使得平台能够经过更少的改版频次、更低的投入、更短的建设工期达到更高的成熟水平。

- 致情报培训机构及教官

全维战法＝教程＋能力培养方案

在短期内培养大批胜任专业的研判人员，提高全警的信息化深度应用能力，以缓解研判人才资源与实战需要的供求矛盾，是新形势赋予培训机构及教官的重要使命。但如何通过短期培训，真正赋予受训人员应对实战的操作能力，始终是培训机构和教官面临的重大挑战。全维战法不仅对受训人员施加理念上的影响，还将复杂的研判过程拆解为简单的数据操作技法、逻辑思维工具和基本战法，受训人员可以很容易地掌握情报实战所需的每一个单项操作。在此基础上，通过对8项组合定式和5项任务模式的熟练掌握，受训人员可以初步具备技战法的组合应用能力，从而实现由理念到思维习惯的实战化。全维战法不仅意味着战术研判训练内容的充实丰富，还意味着培训方式的深刻变化，更使得模拟演练、比武竞赛等更为高级复杂的能力培养途径成为可能。在新的能力培养模式下，原来需要几年才能形成的研判能力有可能通过系统的训练和仿真化的模拟演练在短期内生成，从而实现研判专业人员的标准化量产。第五篇第23章给出了研判能力培养速成化的思路，供各培训机构及教官参考。

- 致院校学员及新手

全维战法＝完全攻略指南

信息化浪潮已经对警方的运作方式产生了深刻的影响，并必将决定警务工作明天的发展和走向。毫无疑问，信息化深度应用能力已成为警务实战人员的一项核心能力，对于那些有志于在信息化警务变革中一展身手的新人，全维战法提供了少走弯路的、能使实战能力晋级的指南。全维战法不仅是对几十年传统侦查思维的提炼，也是对全国警界十年来网上作战最佳实践的系统总结。如果把一项战术研判任务比作CS对战游戏，全维战法就好比是CS游戏的完全攻略指南。新手虽然不可能仅仅通过书面文字就变成行家里手，但是只要能通过自我训练、团队演练，熟练掌握本书第二、三、四篇展示的各层次的知识和技能，并在实战中不断切磋砥砺，将其变为的自身的常识，运用自如，就可以跨越以往实战人员需要三年、五年、甚至更长时间才能完成的实战能

力成长过程。这正是本书的初衷和期望。

- 致安全、军情、反洗钱部门的反恐、安保情报人员

全维战法＝强力机构应对非传统安全威胁的战术情报操作指南

安全、军情等强力机构不仅要实现从传统安保任务到非传统安全保卫任务的转型，同时要尽快跟上信息化变革的时代脚步。

一方面，在反恐维稳、安保警戒等非战争军事行动中，军情部门原来针对敌方和他国军事集团的情报工作模式已经不完全适用。对于安全机构和军事情报机构而言，应对非传统安全威胁的职能已超出传统的国防、对外情报范畴，属于国家警察职能，因而也必须按照警务情报的一般规律和工作模式来重新组织。

另一方面，随着国内与国外、网上与网下、恐怖主义与政治、民族、经济、社会等各方面因素的复杂交织，如同警察机构一样，这些强力机构也必须摒弃原来“以搜集获取情报”的陈旧理念，尽快树立“信息加分析等于情报”的信息时代情报观。尤其是在战术研判环节，形式上的“情报整编”已远远不能胜任各强力机构应对非传统安全威胁的实战要求，而必须以更为标准化、实战化、流程化的研判战法武装战术情报人员的头脑。美国等西方国家的军事、情报机构已经在这方面取得了初步成效。

基于上述背景，全维战法不仅适用于一般违法犯罪的侦查预警工作，而且也具有军事价值。对于安全、军情、反洗钱、反走私等机构的反恐情报预警、反恐突击情报准备、反游击情报侦察、反间谍侦查、反洗钱及反走私监测等战术研判任务同样提供了系统化的操作指南。这些战法一旦为战术情报人员掌握，不仅可以推进情报转型，而且可以在安全、军情、反洗钱、反走私、警务情报人员之间建立通用的术语通道，进而将安全、军情、警务、反洗钱等机构联成一张情报协作的大网，极大地提高整个国家抵御化解非传统安全风险的能力。

目录

四 组合篇

五 转型篇

六 案例篇

一 总诀篇

情报攻歼，即以战术情报分析思维和技战方法主导侦察、调查、侦查、经营过程，并根据战术情报成品采取精准的干预处置行动。由于应用领域不同，其在警界通常被称为情报主导侦查，在军事领域则被称为情报主导战。前者专注于从警务执法角度对违法犯罪人员采取执法行动，开展取证审讯，后者则注重以特种作战打击暴力恐怖、城市游击战等敌对活动。

情报攻歼是信息时代警方、军方、安全等强力机构共同面对的情报转型任务。对于警方而言，情报导侦是情报主导警务的重要方面，也是传统侦查工作的一场变革。对于新军事变革的推进者而言，情报主导战则是军方在应对非传统安全威胁，遂行反恐、缉毒、反游击等非战争军事行动任务时必须掌握的作战样式。

转型的快慢，决定了警方、军方、国家情报部门等强力机构能否迅速适应信息社会的丛林，循迹猎取潜伏其中的恐怖分子、敌对团伙、有组织犯罪集团和惯犯，并破解敌方的反侦查伎俩，实现快速、精确、灵巧的打击。

而在决定这一变化进程快慢的诸方因素中，所有的限制均不是技术上的限制，而是传统观念、旧有习惯、个人偏好和想象力的限制。要想突破传统理念和旧有习惯的重重阻碍，战术情报分析的方法模型是制胜的重要一环。方法模型是否成熟，决定了情报信息系统的功能性和稳定性，从而框定了与之配套的研判流程和勤务方式。当我们对信息化条件下的新型作战样式做出令人激动的种种展望时，不应忘记，到目前为止变革仍是一种可能，将这种可能变为现实，需要我们将研判机理融会贯通于研判流程、系统设计及勤务方式之中，使未来的信息系统、机制体制、组织文化真正体现情报主导的要义。

对于警界而言，战术情报分析的方法模型一直是公安信息化进程中最令人兴奋的环节，但也是最令人困惑的领域。

说它令人兴奋，因为它融汇了传统侦查和现代情报工作的一般规律、思维方式和操作手段：

实战人员只要熟练掌握了这一方法模型体系，就可以尽快成长为情报和侦查骨干；

将其引入培训课程，可以实现情报、侦查专业人员的“速成”和“量产”；

将其转化为情报平台软件需求，可以建成引领实战的新一代“武器系统”，实现跨越式发展；

将其作为信息化作战体制机制的框架体系，可以提升警务情报系统的顶层设计水平。

说它令人困惑，是因为当前各方提出的“网上战法”可谓五花八门，无论是所用术语和分类体系都处在众说纷纭、莫衷一是的状态，各类战法间交叉重复，不同的战法创建者常常使用不同的称谓描述相同的战法，在某种程度上已经禁锢了战术情报专业的发展空间。

当前信息化深度应用的主要障碍并不是如何在战法的某一思路、某一技法、某一类数据资源应用上实现突破，而是如何将这些零件组合起来，形成导侦攻歼的情报流水线。

全维战法，正是打造这一流水线的尝试。

第1章 挑战与转型

信息时代挑战与非传统安全威胁

步入21世纪，社会信息化的飞速发展和非传统安全问题成为各国情报安保机构无法忽视的两大因素。尤其是两者交织作用，已经对各国警察、军队、安全等强力机构形成了全方位挑战。近年来发生的一系列重要案事件，都表明了恐怖组织、犯罪集团和职业惯犯对信息技术应用的驾轻就熟。现代社会发达的信息通信网络、资金交易网络、交通网络和物流网络深刻改变了我们的生活面貌，同时也为犯罪活动的网络化、全球化提供了土壤。基地组织不仅使用互联网收集信息、宣传煽动，而且将现代信息技术用于恐怖活动的招募、筹资、策划和组织指挥。依托现代通信网络，本·拉登仅仅呆在阿富汗的山洞里就完成了“9·11”恐怖袭击的一系列前期准备工作。当基地组织在2001年11月向深山逃窜时，携带的不仅仅是AK-47步枪，还随身带着大量笔记本电脑。而俄罗斯车臣共和国的分裂分子则使用因特网公布银行账号，接受支持者的捐款。[①] 据美国国防部副部长助理盖瑞·里德透露，在轰动一时的美国圣诞节炸机未遂案中，尼日利亚籍嫌疑人阿卜杜勒·穆塔拉布是在网上被恐怖组织招募的。[②] 在2008年11月26日的印度孟买恐怖袭击事件中，恐怖分子不仅携带手榴弹和自动武器，还带上了GPS、智能手机、卫星电话等信息化装备；[③] 策划过程中，恐怖分子专门在谷歌地球上了解了整个孟买城市布局，选择最佳潜入路线，[④] 有消息称他们甚至尝试通过这一卫星地图产品定制一个沙盘模型进行战前演练；袭击过程中，恐怖分子还不断利用手

① 托马斯·弗里德曼，《世界是平的》（第二版），湖南科学技术出版社2006年9月，第396页。

② Schmitt, Eric (December 31, 2009). Schmitt, Eric, and Lipton, Eric, “Focus on Internet Imams as Al Qaeda Recruiters”, “The New York Times”, December 31, 2009, accessed January 4, 2010. Nytimes.com. http://www.nytimes.com/2010/01/01/us/01imam.html. Retrieved April 13, 2010.

③ Rina Chandran Dec 11, 2008). “Mumbai attacks show up India's technology shortcomings,” accessed 15 February 2012. Reuturs. http://www.reuters.com/article/2008/12/11/india-mumbai-tech-idUSBOM33944720081211.

④ Rahul Bedi (9 December 2008). “Mumbai attacks: Indian suit against Google Earth over image use by terrorists”, accessed 15 February 2012. London: The Daily Telegraph. http://www.telegraph.co.uk/news/worldnews/asia/india/3691723/Mumbai-attacks-Indian-suit-against-Google-Earth-over-image-use-by-terrorists.html.

机上网，实时了解印度安全部队的人数、装备和兵力部署①，境外指挥人员不断通过卫星电话向恐怖分子下达指令，与印度军警展开对攻。美国有专家称：对于恐怖分子来说，他们永远比我们快。就像病毒一样，先有病毒，后有杀毒软件，但面对病毒带来的危害，杀毒软件往往无能为力。除了恐怖袭击这种“高端”犯罪，每天发生在我们身边的违法犯罪也都深深打上了信息技术的烙印，境外毒枭通过移动通信网络遥控指挥境内的毒品交易，跨区域贩毒分子通过网络视频聊天商定毒品交易的时间和地点；入室抢劫惯犯通过互联网搜寻作案对象；电信诈骗团伙利用网络电话和任意显号等手段实施犯罪，在得手后通过电话、网络银行对犯罪收益进行快速分级转账，这类案例越来越多地出现在警方的案件信息库中，并频频见诸媒体报道。

随着传统和非传统安全因素的交织，国家面临的非传统、非对称威胁日益严峻，恐怖主义、网络攻击及洗钱、海盗等不法活动被越来越多的政府划入国家安全范畴，锁定这些敌对分子并对其开展精准有效的打击，也成为各国警方、军方和安全机构共同的职责。对警方而言，这意味着打击犯罪行列中出现了更多的合作伙伴和竞争对手。对安全机构而言，这意味着破译与反破译、渗透与反渗透的传统暗战，将部分地让位于反恐战和国内安全保卫战。对军队而言，则意味着针对他国正规军的传统情报手段和大兵团作战部分失效，取而代之的是大海捞针、抽丝剥茧般的情报经营和精准的定点打击。但要实现这一变化，警方、军方和安全机构都必须克服社会信息化带来的根本性难题——信息过载。

实际上，现代信息技术在降低犯罪成本、使犯罪活动的机动性和破坏性倍增的同时，也为警方、情报机构提供了机遇，一个根本的变化就是信息的极大丰富。在计算机、电话和互联网尚未普及的年代，有关犯罪活动的信息分散在犯罪分子、被害人、目击者、警察及情报人员的头脑中，获取这类信息全部要靠面对面的调查走访，信息匮乏成了那时的侦查情报工作需要克服的主要矛盾。在信息网络日益发达的今天，图谋不轨的罪犯与我们正常人一样，同样会将诸多生活和工作的细节，暴露在移动电话和互联网上。信息时代的每个人身后都拖着一条由个人信息组成的长长的“尾巴”，人们点击网页、切换电视频道，使用手机、信用卡购物，情报人员只要收集这些表面上稀松平常的信息，进行汇总、分析并加以关联，就有可能取得有关目标人员活动的关键信息。正如扬州市公安局的余炜警官所说的，一个犯罪嫌疑人，其姓名、性别、出生年月日、身高等自然属性存在于公安机关的人口资料数据库之中，其学历、就业、医疗保障、保险、驾驶、通讯记录等社会属性存在于相关部门、行业的数据库之中。

① Damien McElroy (November 28, 2008). “Mumbai attacks: Terrorists monitored British websites using BlackBerry phones”, accessed 15 February 2012. London: The Daily Telegraph. . http: //www. telegraph. co. uk/news/worldnews/asia/india/3534599/Mumbai - attacks - Terrorists - monit.

看似不着边际，毫无规律的犯罪活动也可通过存在于各种数据库中的数据，即通常所说的“电磁痕迹”全部都以0和1的形式呈现在我们面前[①]。正是这些电磁痕迹，形成了信息社会中侦查打击所依托的的数据环境，使实时的信息获取成为可能。

然而，任何机遇都是一柄双刃剑，对情报机构、警方和军方而言，信息暴涨带来了更多的破案机会，也带来了巨大的压力。随着社会信息化步幅加快，军、警、情报机构都在经历信息化变革，他们日益为大量的信息包围。案事件数据、技术侦控数据、互联网信息等各类数据资源，每天源源不断地通过一线人员，积累到机构业务信息系统中。但这些机构的分析处理能力并没有随着信息量增长同步提高。看看各国的重大情报失误就会发现，美国的“9·11”袭击、伦敦“3·11”袭击、印度孟买恐怖袭击都凸显了信息过剩而分析不足的矛盾。美国国家安全局对此有深刻的体会。冷战时期，美国政府和军队都仰仗国家安全局的密码研究能力来保护至关重要的情报，同时破译密码，截取敌方的秘密情报。但是随着苏联解体、冷战结束，恐怖分子、国际毒枭、洗钱犯罪分子开始成为美国新的敌人，发现这些敌人成为比破译密码更为重要的任务[②]。有报道称，即使是在计算机技术尚未普及的年代，美国国家安全局（简称国安局）已经具备了惊人的信息获取能力，其每六个小时截获和存储的内容相当于一个美国国会图书馆的信息量[③]，但是如何有效利用这些海量信息，一直是令国安局头疼的问题。到20世纪90年代末，随着手机通信网、光缆通信网及互联网的突飞猛进，国家安全局已经被其汇集的海量的电子数据压得喘不过气来。“9·11”恐怖袭击事件更是使国安局的高层蒙羞。2001年9月10日，当基地组织的劫机者在国家安全局总部大楼之外几英里远的汽车旅馆里，准备第二天举世震惊的袭击时，国安局对此毫不知情。只是在袭击后，国安局的官员倒查其监控系统才发现，系统已经从阿富汗和沙特阿拉伯截获了“明天开始较量”、“明天就是零点”等语音片段[④]。虽然美国在“9·11”恐怖袭击事件后大力推进情报改革，但信息过载的矛盾仍未得到彻底解决。就在2009年底至2010年初，7名中情局特工在阿富汗被“双重间谍”设套炸死。中情局这次在阿富汗吃大亏有一个重要原因，他们只看到被策反的约旦人巴拉维是医生，有很好的家庭背景，与约旦情报机构合作过，并多次提供“准确情报”。但事实上，只要稍对巴拉维作进一步研究就会发现，他经常在网上发表抨击西方国家的言论，甚至还直白地表示愿意献身“圣战”。事件后，《纽约时报》引述反恐专家约翰·法摩尔的话说，美国情

① 余炜，《试论“数据库侦查方式”》，《中国刑事警察》2005年03期。

② 斯蒂芬·贝克，《当我们变成一堆数字》，中信出版社2009年7月，第127页

③ “NSA Collects as Much Data as Is Stored in the Entire Library of Congress Every Six Hours [???]” (May 24, 201(1), accessed 15 February 2012. Cryptogon. com. http: //cryptogon. com/? p=22485

④ Walter Pincus and Dana Priest. “NSA Intercepts On Eve of 9/11 Sent a Warning Messages Translated After Attacks” Washington Post at June 20, 2002 Page A01, accessed 15 February 2012. http: //www. prisonplanet. com/NSA_Intercepts_On_Eve_of_911_Sent_a_Warning. htm.