追踪网络攻击

托马斯·里德，本·布查南

英国伦敦国王学院

追踪网络攻击

托马斯·里德，本·布查南

英国伦敦国王学院，战争学系

提要：谁干的？溯源是个根本问题。人类生命和国家安全可能要仰仗于某个情报部门和某个特工。在网络入侵的背景下，溯源普遍被视为最棘手的技术问题之一，被视为既有办法也没办法得到解决，被视为主要依赖所掌握的证据。但它确是如此吗？这是对溯源的建设性认识吗？本文剖析了溯源的来龙去脉。为更好地阐述观点，我们引用了 Q 模型：用来解释、指导和完善溯源的全过程。找到发动进攻的攻击者就是一个从 3 个层面消除不确定因素的实践过程：战术层面，溯源就像是一门艺术，一门科学；操作层面，溯源是一个发现细微差别而不是非黑即白的过程；战略层面，溯源意味着政治上的利害攸关。成功的追查到攻击者需要一整套技巧，谨慎的管理，时间，领导，压力测试，频繁的沟通以及认识局限和挑战。

主题词：网络安全，溯源，追查能力，信息安全，信号情报

溯源是一门回答问题的艺术，就像故时的罪与罚：谁干的？成功的溯源是所有形式的国际、国内胁迫和威慑的核心。溯源能力差会削弱一个国家的信誉，效率并最终危及其自由与安全。

生与死的抉择取决于溯源。2013 年 8 月大马士革郊区姑塔东区发生的使用化学武器整件；2014 年夏乌克兰顿涅斯克州附近马航 MH-17 航班被击落；2014 年 6 月加沙战争期间引发的古什埃齐翁地区 3 名以色列少年被绑架；所有这些事件的共同之处是没有人立即出来承担责任，凶手身份的确认仍饱受争议，这种情况下最高层还要做出相应的政治决策。溯源问题近期才被引起广泛重视。1914 年 6 月 28 日奥地利弗朗兹·费迪南大公被刺带来了一个类似的难题：谁是刺客加夫里洛•普林齐普？他是塞尔维亚特工吗？

溯源是逐步展开的。这些国际事件证明了大量潜在因素在起作用。但系统讨论溯源问题时，它们又过于特殊，过于费解。从一个更有序的完整例证开始会更有建设性。对执法而言，确认罪犯可能从向紧急电话接线员报案开始。然后是调查。警官会保护现场，询问目击证人。法医专家尝试去发现和分析专门的物证，如把受害者身上发现的子弹与犯罪现场留下指纹的枪支进行比对。如果一切顺利，这些证据将被作为呈堂证供向法官展示，最终确认真凶。这一过程尽管常常充满戏剧性，但它确实是一个有方法、有顺序以及形成固定制度的程序。

这个场景虽然简单，但很有启发。它至少提示了 3 个普遍且广为熟知的特性：溯源常常过于庞大和复杂以至于任何个人都难以完成；溯源需要各类专家分工；溯源是一个不同层次工作的递增过程，短时间内证据的技术搜集，随后的调查与分析，法律进程，在各种相互矛盾的证据基础上形成观点并交给决策者。学术作品和流行文化对执法场景进行了全面的探讨。但追查网络攻击则不那么简单，二者的基础也不尽相同。

在网络安全领域，围绕溯源的争论进展出奇缓慢。[1]目前，数字领域的溯源受 3 个假设主导。第一个假设是溯源是新兴领域最棘手的问题之一[2]，它源自根本性的技术构架[3]和互联网的地理分布。[4]因此，

[1] 该领域早期的贡献，参阅戴维·惠勒（David A. Wheeler）和格里高利·拉尔森（Gregory N. Larsen），“网络攻击溯源技术”（弗吉尼亚州亚历山大市：国防分析中心，2003）；理查德·克雷顿（Richard Clayton），“网络空间的匿名性与可追溯性”，《技术报告》Vol.653，（剑桥：剑桥大学计算机实验室，2005 年）；苏珊·布伦纳（Susan Brenner），“光速：对网络犯罪、恐怖主义和战争的溯源与响应”，《刑法与犯罪学期刊》，97/2（2007），第 379-475 页。早期的案例研究可参阅克里福德·斯托尔（Clifford Stoll），《布谷鸟蛋》（纽约：双日出版社，1989 年）。

[2] “溯源可能是最大的难题”，P.W.辛格（P.W. Singer）和艾兰·弗里德曼（Allan Friedman），《网络安全

只有在技术上重新设计互联网才能根本解决这一个问题。[5]类似的看法在有关法律问题争论中亦占上风。[6]第二个假设是对溯源持二元论观点：在给定情况下，这一问题要么能解决[7]，要么解决不了。[8]溯源要么能找到真凶，要么只是找到一个仿冒的 IP 地址，混乱的网络日志或其他毫无用途的痕迹。[9]第三个假设是能证明责任归属的证据十分广泛，主要挑战就是找到证据本身，而不是分析、提炼和展示。[10]上述观点均很普遍，它们是直观的认识，也没有错——但它们却有局限且不充分。溯源的本质在过去 10 年中发生了显著地变化。相对目前已有的研究而言，真正实现对网络事件的追溯已经变得更为微妙，更

与网络战》（纽约/牛津：牛津大学出版社，2014 年，第 73 页）；另可参阅，戴维 • 贝茨（David Betz）和蒂姆 • 斯蒂文斯（Tim Stevens），《网络空间与国家》（阿德菲系列，伦敦：国际战略研究所/劳特利奇出版社，2011 年），第 75-76 页。

[3] 例如，可参阅 W.厄尔 • 博伯特（Earl Boebert），“对溯源挑战的调查”，“制止网络攻击委员会”编，《制止网络攻击研讨会纪录》（华盛顿特区：国家学术出版社，2011 年），第 51-52 页。另参阅马丁 • 利比基（Martin Libicki），《网络威慑与网络战》（加利福尼亚州圣塔莫尼卡市，兰德公司 2009 年），第 43 页。

[4] 杰克 • 戈德史密斯（Jack Goldsmith）和蒂姆 • 吴（Tim Wu），《谁控制了互联网？无边界世界的假象》（牛津：牛津大学出版社，2006 年）。

[5] 麦克 • 迈康奈尔（Mike McConnell），“如何赢得我们正在失去的网络战”，《华盛顿邮报》，2010 年 2 月 28 日。

[6] 参阅马修 • 韦克斯曼（Matthew C. Waxman），“网络攻击与使用武力”，《耶鲁国际法期刊》，2011 年第 36 期，第 421-459 页，第 447 页；尼古拉斯 • 查哥里亚斯（Nicholas Tsagourias），“网络攻击，自卫与溯源问题”，《冲突与安全法律期刊》2013 年第 17 期，第 229-244 页。有关溯源对使用武力讨论的必要性，参阅马尔科 • 罗西尼（Marco Roscini），《网络作战与国际法中的使用武力》，（牛津：牛津大学出版社，2014 年），第 33-40 页。

[7] 美国前国防部长莱昂 • 帕内塔（Leon Panetta）在“无畏号”航空母舰上曾发表了一段著名的演讲：“在解决阻遏网络敌人更复杂的问题——确定攻击起始的难题——方面，（国防部）取得了重大进展”。帕内塔“对企业高管发表的国家安全中网络安全的讲话”，纽约，华盛顿特区：国防部，2012 年 10 月 12 日。

[8] 戴维 • 克拉克（David D. Clark）和苏珊 • 兰多(Susan Landau)，“解开溯源难题”，“制止网络攻击委员会”编《制止网络攻击研讨会纪录》，（华盛顿特区：国家学术出版社，2011 年）。另可参阅杰森 • 希利（Jason Healey），《一个激烈竞争的领域》（华盛顿特区：大西洋理事会，2013 年），第 265 页

[9] 罗伯特 • 内克（Robert K. Knate），“解决溯源：迈向网络空间的问责发展，谋划应对网络攻击的未来”，华盛顿特区：第 111 届国会技术与创新附属委员会听证会，2010 年 7 月 15 日。

[10] 在入侵分析方面最有影响的文章似乎都假设证据自己能说话，持这一观点的人们并不把注意力放在如何与非技术人群沟通上。其中最有影响力和有用的文献是“钻石模型”，参阅塞尔吉奥 • 卡尔塔吉龙（Sergio Caltagirone）、安德鲁 • 彭德格斯特（Andrew Pendergast）和克里斯托弗 • 贝茨(Christopher Betz)，《入侵分析的钻石模型》ADAm86960（汉诺威，马里兰州：网络威胁情报与威胁研究中心，2013 年 7 月 5 日），以及“杀伤链”分析，参阅埃里克 • 哈钦斯（Eric M. Huntchins），迈克尔 • 克洛佩特（Michael J. Cloppert）和罗翰 • 阿敏（Rohan M. Amin），《在分析敌方行动和入侵杀伤链基础上受情报驱动的计算机网络防御》（马里兰州贝塞斯塔：洛克希德 • 马丁公司，2010 年）。

普遍和更具政治性。[11]

本文试图从打破已有立场的角度讨论溯源，并提出 3 个问题。从第一个问题开始：如果溯源首先不是技术问题，那么它是什么？接下来是第二个问题：如果溯源不是非此即彼而是一个程度的问题，那么什么是标准的溯源，如何区别高质量溯源与低质量溯源？第三个问题：若证据不明显且模棱两可，怎样进行整理和分析？如何把溯源各流程作为一个整体进行管理并与第三方沟通？

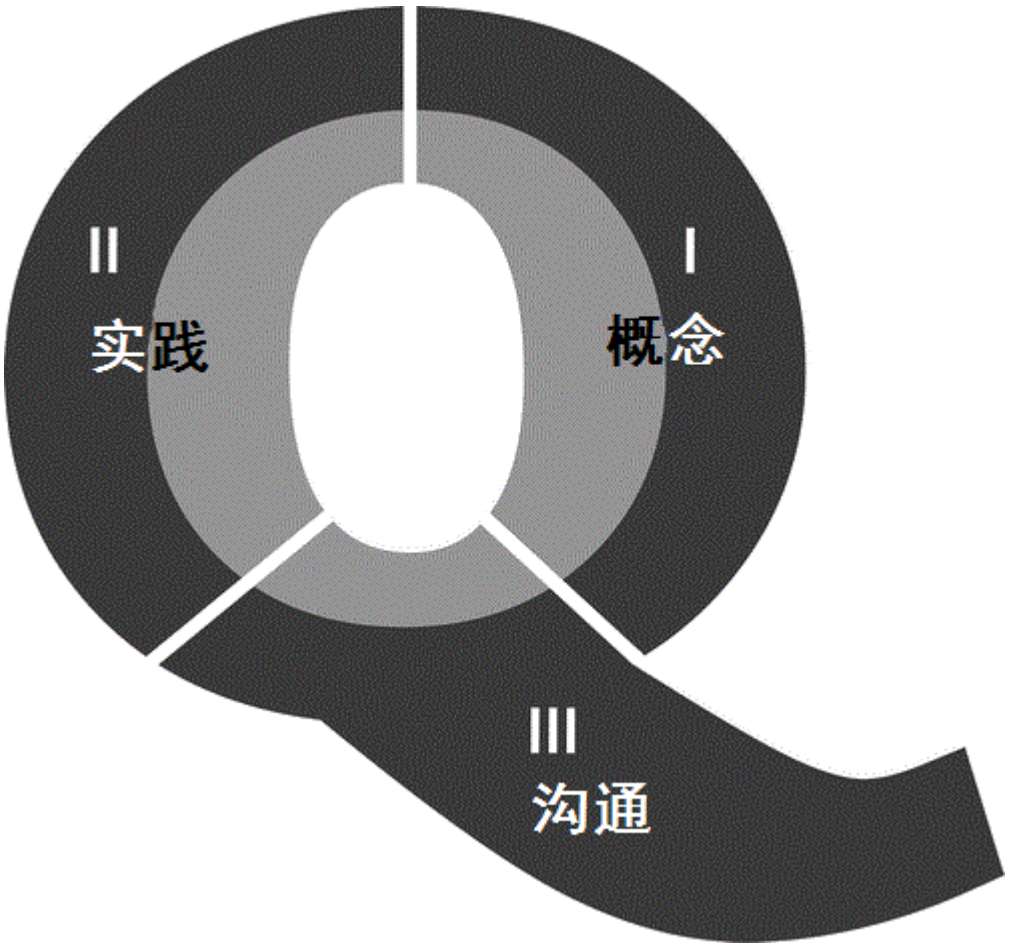
本文旨在描述溯源的来龙去脉。找到攻击背后的原凶是一个在多个层面上最小化不确定性的操作过程。技术层面，溯源与科学一样是一门艺术。正确的溯源没有放之四海皆准的秘诀、统一的方法、流程或清单。找到正确线索要求训练有素且专注于一系列细节，还有技术经验带给操作人员的本能。用熟知的军事术语来说，它需要“灵感闪现”。[12]操作层面，溯源是一个微妙的过程而不是简单的提问回答。溯源的过程不是非此即彼的，而要对参差不齐的程度进行衡量，它也不是非黑即白，非对即错的，而总是处在灰色地带。因此，它还是一项团队工作，成功的溯源需要更多的技能和资源，这远非任何单个人能做到的。最佳结果需要认真的管理与有序的组织。战略层面，溯源是厘清政治利害。政治的危急程度取决于多种因素，最重要的是遭受到的损失，它可能是经济的、物理的或名声的。在最高领导看来，溯源

[11] 参阅博伯特，“对溯源挑战的调查”，第 41-54 页。要想参考更全面的研究，可参阅埃米尔·卢波维奇（Amir Lupovici），“溯源问题与‘暴力’的社会建构”，《国际研究视点》，2014 年，第 1-21 页。

[12] 卡尔·冯·克劳塞维茨用“灵感闪现”来形容“军事天才”，即能让优秀指挥官在压力、信息过剩和时间紧迫的情况下做出正确战术决策的“慧眼”，参阅卡尔·冯·克劳塞维茨，《战争论》，迈克尔·霍华德（Michael Howard）和彼得·帕雷特（Peter Paret）翻译,（普林斯顿大学出版社，1976 年），第 100-112 页。

一部分是对国内相关流程的资源重组和指导，一部分是参与最终的评估与决策，还有一部分是把结果公布给第三方和公众。

为说明我们的观点，描绘出一个理想的溯源，我们引用了 Q 模型（参见图 1）。[13]技术上，这个模型能帮助分析人员提出所有相关的问题，帮助他们思考并把调查放在一个大背景下进行。[14]操作上，模型有助于把技术与非技术信息整合到一个竞争性假设之中。这包括从不同层面提出更具挑战性的问题，从细微的技术问题到更全面和解析性的操作问题。战略上，模型有助于用恰当的估算语言提炼出溯源的精髓并陈述出来。这种表述可能会形成会带来严重后果的政治决断。



[13] Q 有几层含义：首先它暗指问题，这是溯源的关键。Q 还与舵手相关，即负责发出信号和驾驶的海军军官。‘cyber’的词根是 κυβερνώ （kyvernǫ́），意指“操纵”。

[14] 这个模型有意不设计成一个流程图或清单的样子。在与操作人员的几次专题讨论后，大家都清楚任何一种线性的描述都不能真正反映出独特性和调查者面对案件的多样性。

图 1 本文的结构和详细图表（参见附录）

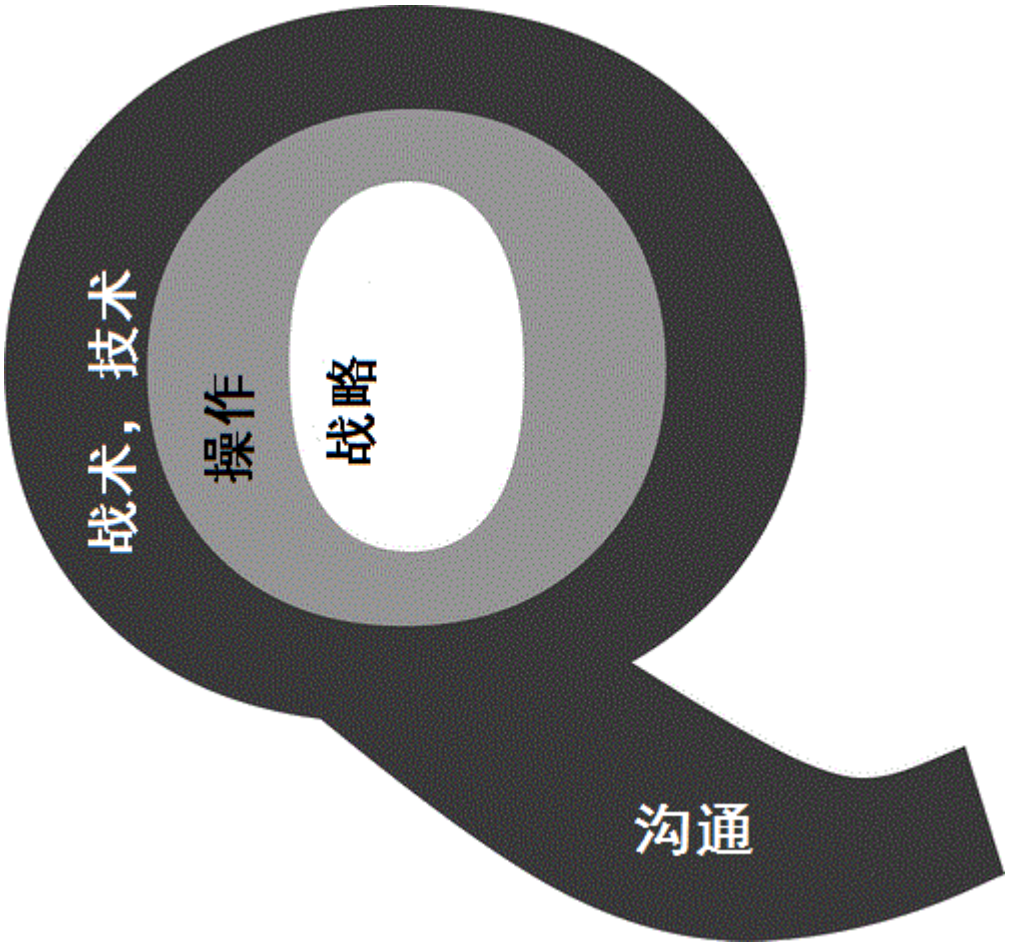
图 1 说明了本文如何进行论述，观点如何展开以及利用附录中更为详细的说明来读懂这个模型。第一部分是概念：用通用术语讨论模型、提出几个重要的区别和动力，说明溯源是一个过程。第二部分是实证：利用近期的几个事例列出溯源的步骤。第三部分将探讨 Q 带来的众所周知的问题，沟通面临的挑战，溯源的局限以及如何把结果转化成行动。结论部分则再次评估几个一直存在却始终没有答案的观点，思考追踪网络攻击的局限。

第一部分

本研究旨在为参与溯源的所有相关方提供一个概念和实际操作的图景，从取证调查人员、情报分析者、国家安全官员、管理高层、政治领导到撰写网络安全和网络入侵文章的记者和学者。

溯源过程中的每个层级都面临不同的分析挑战，需要专门的数据和专业知识，还需要各自对成功溯源的看法（参阅图 2）。每个层级的分析人员都要向其他级别通报并进行调整。尽管溯源过程有始有终，但这个周期不必遵循专门的逻辑或时间顺序，原有的假设会与新发现的细节相矛盾，新发现的细节又会带来新的猜想。然而，不同层级有着不同的任务并独立进行分析，哪怕它们相互关联。通常情况下，所谓的“危害指标”启动溯源过程。这些指标带来了各种特定的技术问题。只有事实收集得足够多，更多的问题才被提出。溯源的启动偶尔也从操作或战略层开始。有时候一起事件的“第一知情者”会是技

术层之上的人员。借助未经鉴定的情报源，或者更宽泛的地缘政治背景——有时候甚至会是直觉——在用技术指标标注前、甚至事件发生前，分析者就确定了可能发生的恶意行为。溯源还会采取另一种方式：战略和操作层分析会启发后续的技术分析，或反之亦然。



溯源需要大量的技能。网络威胁的复杂程度非常高。通过溯源分析来应对和揭露它们的架构需要一个明确的分工。例如，一个反病毒专家团队可花费大量时间和精力对某个恶意软件的安装过程进行反向工程研究，控制工程师则侧重分析针对某个工厂的定向有效载荷的设计特点。震网病毒如此复杂，企业侧重从不同方面对它进行分析，

如传播机制、指挥与控制装置或针对工业控制系统的有效载荷。[15]在战场上，一个完整的战术行动的地位低于战役考虑，但它又很重要。对不同方面进行分析需要大量相异的技巧，这种专业化是网络和军事行动中已被广为接受的基本原则：没有指挥员会派拆弹专家去负责分析叛军网络的筹资情况或爆炸装置的来源。F-16 飞行员不会自己选择目标。导弹工程师不制订核战略。网络攻击情况下，最起码的期望就是组织一个超越小规模专家群来进行溯源。

溯源全过程的总目标常常取决于已遭受或可能造成的损害。在事件频发但调查人手不足的情况下，遭受或可能遭受损害的总量常常决定了追踪恶意行为所投入的资源。如果一次入侵事件并未造成显而易见的损失，某个公司甚或政府部门可能决定无视、部分调查或大致改善防御而不会对一起表面上未造成任何后果的事件启动一次昂贵的调查。因此，缺乏对后果的认识甚至在全面启动调查前就中止了溯源。某种程度上这种情况不可避免。

战术目标主要是掌握事件的技术细节，即怎么发生的。操作层的目标是认识攻击的来龙去脉和攻击者的身份，即事件是什么。战略层的目标是掌握谁对攻击负责，评估攻击的原因、重要性及恰当的应对方式，即回答是谁和为什么。最后，沟通也有自身的目标：把劳动密集型取证调查的结果公布出去是溯源过程的一个组成部分，它不应被忽视。事实上，公布溯源本身意义重大：攻击者可能中止行动，改变战术或公开回应指责，进而促成受害者的进一步回应。

[15] 大致情况可参阅乔恩·林赛（Joe R. Lindsay），“震网及网络战的局限”，《安全研究》22/3（2013），第 365-404 页。

细节是关键。但细节也会使人困惑。从技术人员流向操作层和战略层的信息必须经过加工处理。只有这样它们才能被理解和发挥作用。针对某一入侵，技术分析能产生大量的数据，常常包括被利用的漏洞、有效载荷机制、指挥-控制结构、目标数据、反向工程分析以及被攻击网络的原始数据。一些、也有可能大多数技术分析可能彼此没有关联。操作层和战略层并不觉得一些相关联的技术细节有多重要，就像取证调查人员不关心地缘背景一样。

确定性存在差异。随着信息从技术层面流向操作层及战略层，遇到的问题开始变少但更全面。因此，随着分析由技术人员转向政府部门，有关溯源的不确定性可能会增多。根据法医取证能够回答*入侵的机制是什么*的问题。*动机是什么*的问题则需要提出假设以及随之而来的验证。[16]技术取证的关注点相对狭窄和具体，能够找到答案。操作层提出的相互竞争的假设可能源自大量人力进行的取证结果，但却未得到可供使用的技术和非技术证据的充分支撑。战略层的结论也并未比技术取证高明多少，可能只是对大量假设与判断的整合。[17]接受过培训的资深决策者是管理这些问题的关键。

接下来是“光圈”。溯源过程中遇到的最困难的问题之一是情报圈称为“光圈”的问题：能够确定调查目标的情报源范围，类似于照相机的调焦。情报来源的增多可以提高溯源的质量。另外，随着溯源

[16] 一些形式的犯罪存在例外。证明趋利的动机要比政治动机容易得多。

[17] 接受过较为理论性和正式培训如有数学背景的员工可能倾向于程式化解决网络安全问题。这可能达不到预期目标。理论抽象会掩盖见地的缺失。受到高度质疑的程式化和人为精确的案例，可参阅罗伯特·阿克塞尔罗德（Robert Axelrod）和鲁门·伊利耶夫(Rumen Iliev)，“测定网络冲突的时间”，PANS111/4（2014年1月28日），第1298-1303页。数学公式是入侵分析中广泛使用的模式之一，所谓的“钻石模型”要求的精确度十分夸张。参阅卡尔塔吉龙、彭德格斯特和贝茨，《入侵分析的钻石模型》。

进程的逐级深入，大光圈变得更重要：在单纯的技术层面，对专门的事件划定范围（设定光圈）是有可能实现的，但有条件限制。某个入侵产生的数字证据取决于它发生的背景。网络刺探使用的代码几乎不暴露攻击者的动机。在操作、尤其是战略层面，其他情报来源将能描绘出更全面的图景，例如拦截那些指挥或组织者的电话通讯或电子邮件。全源情报的重要性、更大的“光圈”，是解释为什么那些拥有高水平情报部门的国家比一些能力强大的私企能更好掌控溯源进程的最重要的原因之一。

历史上首次大规模的国对国计算机网络入侵事件“月光迷宫”（Moonlight Maze）说明了全源情报和“大光圈”的价值。事件发生在 1998 年。[18]外国间谍把美国国防部、能源部、国家航空航天局（NASA）、国家海洋和大气局（NOAA）以及一些国防承包商和大学作为攻击目标。入侵者窃取了从头盔设计到大气数据等信息。调查开始时，美国联邦调查局（FBI）的特工不知所措。1999 年初，国防部开始支援调查。计算机网络防御联合特遣部队(JTF-CND)的情报人员“竭尽所能”，从执法部门获得的数字证据开始，但随后调用了信号情报、人力情报，甚至是一些可疑建筑物的过顶卫星图片记录以审查它们近期是否安装了通讯设备。最终，情报源得到的情况远远超过对入侵的数字取证，成功地确定“月光迷宫”造成的数据泄露源自俄罗斯政府。[19]

[18] 想大致了解“月光迷宫”，参阅亚当·埃尔克斯（Adam Elkus）在希利主编的《一个竞争激烈的领域》一书中撰写的章节，第 152-163 页。

[19] 本文作者与 JTF-CND 以及 FBI“月光迷宫”调查小组的一些前官员进行了访谈，华盛顿特区，2014 年 9 月-11 月。

在追溯网络入侵时，单个的个人值得重视。如果找到的证据能够把入侵指向某机构中的某个人，这一溯源十分有效。众多国际事件、尤其是军事事件中，可看出鲜明的对比：被标识的武器系统，身着军装的士兵，事件发生的地点常常说明入侵背后机构的身份。某个特殊的军事目标，例如叙利亚的实验核设施可能会遭到空袭。通过分析地缘政治背景、飞机型号或飞行路径——除了确认飞行员本人，叙利亚甚或第三方能够确认实施袭击的 F-15 战机来自以色列空军。识别一个军事机构首先不需要确认个人和较小的作战单元，这在网络行动中则完全不同。

溯源的终极目的是指出某个机构或政府而非个人。但与标识、军装和地理位置不同，单个行动人员可能是恶意行为与机构之间最强有力的联系者。最有说服力的例子是众击公司（Crowd Strike）2014 年 6 月 9 日发布的“推杆熊猫”（Putter Panda）报告。该公司位于英国分公司的研究人员纳撒尼尔·哈特利（Nathaniel Hartley），率先发现了一名恶意行为者，他用“cpyy”的名字来协调整个行动。第二步就是把“cpyy”与一个真实的人联系起来。哈特利依据注册数据知道这个名字背后的人叫陈平（Chen Ping）。接下来，陈或者“cpyy”要被关联到某个机构。哈特利通过多个渠道确定发现了更多可以确认身份的信息，包括博客和一个名为 Picasa 的相册。相册的“办公室”文件夹所提供的图片细节清楚地把陈或“cpyy”联系到上海的某个大楼，包括军事标识、大楼、设备甚至是陈自己的肖像。在这些照片帮助下，哈特利定位了一个地点：北纬 31° 17′ 17.02′ ，东经 121° 27′

14.51′，正位于上海市闸北区的中心。这个地址属于中国人民解放军总参谋部第三部 12 局，61486 部队。[20]哈特利的证据来自多个渠道，是可信的。[21]其他的例子还有曼迪昂特公司的 APT1 报告，以及美国司法部出人意料的起诉。[22]所有这些报告都通过个人在网上的作为把他们与机构联系在一起。仅凭这种个人关联并不足以带来高质量的溯源。然而，明确地指出一个机构首先需要把范围缩小至个人，然而再回放到机构或部门。这一系列行动取决于可掌握的“光圈”。个人的联系如果能与来自其他渠道的指标相契合，则证据将得以显著强化。

洞察力也很重要。先入为主、预判、偏见以及心理和政治倾向都有可能影响溯源，其中又涉及内部与外部两个方面：从内部看，各层级的分析员和管理者大多会从各自角度提供预期的结果和解读证据。机构设置的原因将使内部报告会被忽略，这一问题也因而被放大。1978 年对一个情报失败案件的杰出研究揭示，“政策前提约束了一个人的看法，高负荷的事务性工作则限制了一个人的思考能力”。[23]一个综合性的事例能够说明这一结论：假设沙特阿拉伯政府发现了“正义之剑”，该组织声称对 2012 年对沙特阿美石油公司发动了名为“沙蒙”（Shamoon）的网络攻击，其一部分成员来自位于沙特的什叶派激进分子。在逊尼派属于少数派的国家，对什叶派的偏见可能使沙特的调查人员会假设这个组织受雇于伊朗政府，即便手中的证据无法证明这

[20] 纳撒尼尔·哈特利（Nathaniel Hartley），“追溯到解放军 61486 部队”，众击网站，2014 年 6 月 9 日；还可参阅《推杆熊猫报告》，众击，2014 年 6 月 9 日。

[21] 2014 年 8 月 6 日，作者通过电子邮件与哈特利本人联系。对个人研究重要性的认识，一些领先的网络安全公司的意见大相径庭，火眼（FireEye）和卡巴斯基公司较为谨慎。源自于与位于弗吉尼亚州雷斯顿火眼公司员工的讨论，2014 年 9 月 15 日，与位于巴塞罗纳卡巴斯基公司员工的讨论，2014 年 10 月 8 日。

[22] 本文后续将详细讨论起诉事件。

[23] 理查德·K·贝茨(Richard K. Betts)，“分析、战争和决策：情报失败为什么不可避免”，《世界政治》，31/1（1978 年 10 月），第 61-89 页，第 61 页。

些什叶派沙特公民得到德黑兰的支持。国内偏见最大，犯下严重错误的风险就越高。

第二部分

所谓溯源质量就是要“问对问题”。模型的每个层级都有一系列能推进本层级进程的具体问题。每个层级所含问题的答案就是向下一层级推进的起点。一个团队对整个过程的整体把握越好，溯源的质量就越高。这个过程是动态和非线性的：每个案例都不同，因此在调查中，任何固化的流程或线性的“清单”都是有问题的。[24]接下来将逐层讨论这个过程，从战术性的技术开始，逐渐向战略性考量深入。如果可能，每一方面的描述都将附有对实践案例的简短说明。[25]

技术层常常是调查的起点。它广泛且深入，给相关人员带来重要挑战。这需要分析者以一种高效的团队工作来回答关于计算机代码、网络行为、语言和其他更多技术问题。在许多案例中，技术证据都是溯源过程的基础。发掘这些证据并不总是充满荣耀的行为，而是生死攸关。

危及安全的指标很有可能开启一项调查。损害指标是指网络侵入或恶意行为的技术指征，常被简称为技术术语 IOCs（Indicators of compromise）。无论是通过广泛的自动扫描还是计算机异常行为报告，这些攻击迹象都能被发现。对大量计算机进行深入、个别和常规的证据分析对于网络管理者而言成本过高。IOCs 能够成为帮助进一步缩

[24] 2014 年夏天举行的系列公私部门小组研讨会上，分析人员普遍对线性“清单”提出怀疑。
[25] 本文没有足够的篇幅详细介绍这些案例，因此作者为每个案例都提供了最权威的参考来源。这些来源有些是学术出版物，但大多数是企业报告。

小调查范围的有用工具。一项有影响力的研究将这些指标划分为三个主要类别：原子的（atomic）、行为（behavioural）的和计算的（computed）。[26]

所谓原子指标（atomic indicators）是指离散的数据碎片，无法再进一步分解，否则将会失去其证据价值。通过原子指标本身能够查明恶意行为。一般包括 IP 地址、邮件地址、域名和文本碎片。计算类指标与这些数据碎片相似，但其中又包括一些计算成分。例如“哈希”（hash，也译作“散列”），一个从输入数据中获取的特有签名，如一个密码或一个程序。只要输入不变，一个散列的值不变。在网络计算机运行的程序散列可能符合已知的恶意程序散列。行为指标是行为和其他指标的结合，在一些案例中，既可揭示恶意行为，也可用来指认过去曾实施过类似行为的具体人。从社会工程学角度看，一项行为指标可能是一个不断重复的具体意图，如向低层雇员发送邮件以获取网络接入点，然后通过网络传输特定恶意软件，与其他计算机建立未经授权的远程桌面连接。关注计算机网络防御的机构收集上述三种攻击指标和定期监测其网络和计算机。一旦发现攻击证据，更多的技术问题接踵而至。这些问题根据技术指标（indicator）、敌对行为(adversary)和威胁(threat)排出先后顺序。

几乎所有攻击者都必须克服一个挑战：进入。[27]任何一个攻击者都必须具有在非授权系统执行代码的能力。这种代码利用系统漏洞，

[26] 埃里克·哈钦斯，迈克尔·克洛佩特和罗翰·阿敏，《在分析敌方行动和入侵杀伤链基础上受情报驱动的计算机网络防御》（马里兰州贝塞斯塔，洛克希德·马丁公司，2010 年）。

[27] 拒绝服务攻击是例外，它们通过向计算机系统发送大量基础性且常常是无意义的数据使其中断服务。

为攻击者提供更高的访问和执行授权。传送这种代码的通用方式不是利用技术弱点，而是利用人的弱点：鱼叉式钓鱼攻击，通过发送社会工程类信息欺骗使用者。著名的针对安全公司 RSA 的攻击就是始于一封发送给低层雇员的邮件。这封邮件的标题是“2011 年招聘计划”，足以诱导有些雇员将其从垃圾邮件夹中恢复并打开其附件。附件是一个包含着恶意软件的 Excel 表格，能帮助攻击者进入系统。通过这个“登陆点”，他们能够通过网络进入到更具价值的计算机。[28]这种事情非常普遍，甚至是用来实施更高级的攻击，[29]调查者关注他们以获取可能的溯源线索。与钓鱼活动相关的，除了技术数据，如邮件来源，还有社会数据，如语言错误和目标选择的老练程度。另一种进入方法是利用被远程接入软件感染的 USB 驱动器。攻击者或某个同伙，或某个不知情但却使用了被篡改的 U 盘的员工都有可能把它插入计算机中。还有更多实施侵入的纯技术手段。一个常用的方法是“水坑攻击”（watering-hole attack）。这种方式要求攻击目标可能会访问的某个网页——如外卖餐厅网站这样正当网站[30]，当目标雇员访问该网址时，网页浏览器中的漏洞会破坏他或她的计算机。许多侵入技术通过控制网络基础设施，操控和破坏对合法网页的访问，发动所谓“中间人攻击”（man-in-the-middle attack），或是在攻击者不能完全控制某个网络结点但仍能植入数据，发动“旁观者攻击”（man-on-the-side attack）。

[28] 乌里·瑞弗纳（Uri Rivner），“对一次攻击的剖析”，RSA，2011 年 4 月 1 日。

[29] 根据维基解密曝光的一份美国国务院内部电报，“2002 年以来，（美国政府）机构受到社会工程式网络攻击”，“数以百计的（美国政府）和拥有安全授权的国防承包商系统被入侵”。布雷恩·格罗（Brain Grow）和马克·霍森鲍尔（Mark Hosenball），“特别报道：在网络间谍对抗中中国领先”，路透社，2011 年 4 月 14 日。

[30] 尼科尔·帕尔斯（Nicole Perlroth），“隐藏在通风管道和自动售货机的黑客们”，《纽约时报》，2014 年 4 月 8 日，A1 版。

[31]

寻找目标的过程能够揭露破坏或侵入者的类型。针对信用卡信息和其他易于获利目标的攻击往往指向有组织犯罪。针对产品设计的攻击会指向从事经济间谍国家的一些存在竞争关系的公司。针对政治和军事战略细节的攻击则指向情报机构。技术层能够提供具体的与攻击有关的证据，帮助行动层推断。如通过观察侵入者在被破坏网络中不同计算机间的动向，调查者可观察攻击者在寻找什么。通过重建攻击者发出的具体指令，调查者能从被感染机器的存储记录中看出攻击者有无具体企图，或仅仅是在进行泛泛的搜寻以获取有价值的信息。有时代码还包含着搜索词：2014 年披露的一个有名的“毒蛇”（Ouroboros）行动，就包含了搜索词“北约”和“欧盟能源对话”。[32]

对攻击目标的分析还有助于搞清攻击者的组织架构。攻击者所调用的资源可作为一个指标，判断其对目标价值的估算。如果一个攻击使用了许多超过必要程度的资源——如，低水平的间谍活动使用了一个高级的 rootkit 攻击，这就能够表明实施该行动的不大可能是一个能有效评估攻击目标的团伙。还有一个类似的“实施过度攻击”的指标：一些攻击者可能会对同一目标用同样方式进行多次攻击，甚至是在一次破坏已成功实施之后。这种没必要的投入可能表明攻击者代表

[31] 例如，“此次‘旁观者攻击’（MITM）是针对谷歌邮件的安全套接层（SSL）吗？”，谷歌产品论坛，http://bitly.com/alibo-mitm+;还可参阅赛斯·舍恩（Seth Schoen）和伊娃·戈尔佩林（Eva Galperin），“伊朗针对谷歌的中间人攻击表明授权认证存在危险弱点”，电子前沿基金会，2011 年 8 月 29 日。亦可参阅尼古拉斯·韦弗（Nicolas Weaver），“近观美国国家安全局最强大的互联网攻击工具”，《连线》，2014 年 3 月 13 日。

[32] “Epic Turla 行动”，卡巴斯基实验室，2014 年 8 月 7 日。

着一个大型组织，目标混乱不明。这种针对大量目标的“喷射”式攻击还可能表明攻方内部破坏实施者与工具开发者间有分工。[33]

大部分恶意行为的实施依靠基础设施，在拒绝服务攻击案例中，它就是依靠向目标计算机发送大量无用信息来达到瘫痪的目的。其他一些恶意行动的案例，基础设施常常被用作“跳板”或向被感染机器发送代码指令（技术行话称之为命令与控制，command-and-control）。为了用最小成本获取最大收益，心怀恶意的一方会在破坏行动中多次重复使用同一个物理数字基础设施。因此，把不同行动与潜在的不同团体关联起来，对于溯源过程来说是一个很有价值的线索。在美国起诉五名中国军人一案中，起诉方专门将攻击者对域名服务器的使用作为溯源一部分。[34]攻击者获得基础设施的方式不同：有的能控制一台计算机，在不被机主察觉的情况把它变成僵尸网络(bot)的一部分；有的是通过服务器提供商合法租赁服务器，然后用它来作恶；或者攻击者本来就掌握着一些基础设施。攻击者操控基础设施的手法在许多方面决定了接下来的问题。比如，租赁来的基础设施，如虚拟机和服务器，可通过服务商公开获取更多的注册和日志信息。分析对方掌握的基础设施可获得地理位置等线索。一些情况下监控对手基础设施能获得新的分析线索，有助于未来行动。因此，一些精明的攻击者正在想方设法更好地掩藏他们的基础设施。[35]

[33] 源自 2014 年夏天作者对多名系统操作员的采访。

[34] “美国诉王栋、孙凯亮、文新宇、黄镇宇、顾春辉”，美国宾夕法尼亚州伊利市：宾州西区地方法庭，2014 年 5 月 1 日。

[35] 例如，2014 年 8 月 6 日，火眼公司揭露了一次行动，“恶意软件似乎指向合法的域名”，企图“欺骗防御者，给他们带来一种安全的假象”，参阅内德·莫兰（Ned Moran）和麦克·斯考特（Mike Scott），《毒飓风行动》，火眼公司，2014 年 8 月 6 日。

计算机代码最突出的特点之一就是模块化。出于效率的考虑，攻击者往往避免重新编写代码，而会重复使用相关软件来完成整个行动中的基本任务。作为攻击的一部分，这个软件常常直接植入目标网络，但事后会被调查者加以分析。攻击者使用的软件常常有着自己的签名和特点，能够为确认侵入者及其同伙的身份提供线索。著名的网络安全公司火眼在其报告中常常提到所谓的“数字军需官”（Digital Quartermaster）。他们往往会向各个恶意组织提供相同的软件。[36]不同案例这种分析的效果也有差别。一些被打包成模块的代码在攻击中的使用频率很高，但却对确认具体攻击者不是很有用。而其他一些像震网和 Duqu 恶意软件中使用的代码，是如此深奥而复杂，对确认攻击者身份很有价值。[37]在一些调查中，研究者有理由确定是同一个人编写了震网与 Duqu 的代码，因为两种恶意软件共享的一些关键模块和代码不是能轻易得到的。[38]

分析入侵者生活模式是调查获得突破的重要部分。为了效率的最大化，所有机构都有固定的日程和办事程序。黑客组织也不例外。时间和其他行为模式能够为确认其位置和身份提供线索。比如，美国起诉中国军人的案例表明行动者遵循了一定的行为模式。他们只在一些时间进行命令与控制，而在午饭时间、夜晚和周末的时候这些行动就

[36] 内德·莫兰和詹姆斯·班尼特（James Bennett），“供应链分析：从军需官到百货店”，火眼实验室，2013 年 11 月 11 日。

[37] 参阅考斯汀·拉伊乌（Costin Raiu），“走进 Duqu 的命令与控制服务器”，在 2012 年 5 月 4 日于波士顿召开的 SOURCE 大会上的演讲。

[38] 赛门铁克公司有关 Duqu 病毒的报告指出，“Duqu 与震网共用大量代码；然而二者的有效载荷却完全不同。Duqu 不是用来破坏某个工业控制系统，而是用一个具有远程进入能力的程度来取代它。Duqu 的编写者得到了震网的源代码，而不仅仅是编辑过的版本”，“W32. Duqu”，第 1.4 版，赛门铁克，2011 年 11 月 23 日。

停止了。[39]这些行为符合上海（美国政府声称的攻击者所在地）的工作时间。另外一个例子中，众击公司追踪了某攻击行为的实施者，判断其位于俄罗斯，因为大部“编辑时间”——即软件被打包使用的时间——就是俄罗斯的上班时间。[40]生活模式虽易造假，却被广泛用来证实调查者的推断。

恶意软件中的语言指标也能提供溯源线索。这里的语言主要分为两大类：被攻击者选中用来表达具体事务的文字——如变量、文件夹和文件的名字——以及通用配置参数。在复杂的“伪旗”行动中，二者相对容易伪装。然而溯源过程中语言分析仍十分有用。例子很多，最近的是卡巴斯基发现的名为“面具”（Careto）的恶意软件。软件开发者把间谍设备中的两个主要模块的一个命名为“面具”。按照惯例，此次行动的命令与控制服务器散布于很多国家，其中大部分位于非西班牙语国家，如马来西亚，澳大利亚，捷克，新加坡和美国。但语言指标却提出了相反的论断。[41]第一个指标是一些子域，冒充西班牙报纸而实际上却可能被用来实施网络钓鱼（虽然也会被伪装成英国和美国的报纸）。[42]第二个指标是计算机的设置数据暗示代码是在西班牙语界面的计算机中编写的。第三个指标是一些俚语的使用，俄罗斯研究者们怀疑：“在非西班牙母语者中很罕见”。[43]他们还给出了三个俚语使用的例子：重复使用“Careto”一词，它是“脸”或“面具”

[39] “美国诉王栋、孙凯亮、文新宇、黄镇宇、顾春辉”，美国宾夕法尼亚州伊利市：宾州西区地方法庭，2014 年 5 月 1 日。

[40] 作者在弗吉尼亚州阿灵顿访问德米特里·艾尔帕洛维奇（Dimitri Alperovich），2014 年 9 月 15 日，另可参阅《全球威胁报告》，众击公司，2014 年 1 月 22 日，第 18 页。

[41] 《揭秘“面具”》，第 1.0 版，卡巴斯基实验室，2014 年 2 月 6 日，第 46 页。

[42] 例如，elpais.linkcom[dot] net/and elespectador.linkconf[dot]net，同上，第 34 页。

[43] 同上，第 46 页。

的西班牙俚语；设置文件的一个密钥被命名为“Caguen 1 aMar”，很有可能是“Me cago en la mar”的缩写，卡巴斯基认为这应是西语“f-”；文件路径 c:\Dev\CaretoPurebas3.0\release32\CDllUninstal32.pdb 中包含的“pruebas”一词，西语意思是“测试”。

错误常常有启示作用。一些失误能够直接暴露攻击者试图隐藏的信息，如一个人或文件的名字，一个真实的 IP 地址，一个旧邮件地址，或是某个代码的注释。近来有两个突出的例子。第一个是“丝路”（Silk Road）网站，它以非法买卖毒品闻名，其运营者在网页上推销其非法运营活动和在网上寻求技术帮助时使用的竟然是同一个用户名。寻求技术帮助的帖子还留下了真实姓名和邮件地址，这些都为调查者提供了明显的线索。[44]第二个例子是黑客组织“匿名者”的领导人之一 Hector Xavier “Sabu” Monsegur。他曾经忘记登录“洋葱”（Tor）服务器而进入受 FBI 监视的“匿名者”聊天系统，从而导致真实 IP 地址泄露。[45]这两个人都因此被抓获。即使这些错误并没有直接揭示相关信息，但它们仍很有价值。如在常用的命令中频繁出现一些打字错误能为复杂分析提供一般线索。正如“大姆指原则”（亦称“经验法则”），组织在本质上更为官僚化，拥有经验更丰富的运作者和标准化程序，其犯错的可能性比单独行动者要小。[46]

讽刺的是，秘密行动也能被揭露。任何行动中，行动者会在速度

[44] 纳特·安德森(Nate Anderson)和赛勒斯·法里瓦尔（Cyrus Farivar），“联邦政府是如何击溃恐怖海盗罗伯茨的”，Ars Technica 网，2013 年 10 月 3 日。

[45] 约翰·莱顿（John Leyden），“致使 LulzSec 首脑萨布落入美国联邦调查局手中的一个小小失误”，Register 网，2012 年 3 月 7 日。

[46] 丹·维尔顿（Dan Verton），《青少年黑客的忏悔》（纽约：麦格劳·希尔出版社，2000 年），第 83 页。

与隐蔽性之间有取舍，而这种取舍会留下清晰的痕迹。反侦察行动——用以躲避监测和事后调查的措施——都是百密一疏和耗费功夫的。攻击者使用的反侦察手段会暴露他的意图，对报复的恐惧和精明程度。一些反侦察行为很普通，相对简单，直接关系到任务的成功与否。比如：攻击者在将盗窃数据偷偷绕过自动防御系统（用来监测是否有有价值的文件离开网络）传出之前，会对这些数据进行加密。其他一些反侦察行为则更复杂和少见，如使用工具修改日志文件中的时间戳，给随后的调查增加难度。攻击者的谨慎很难衡量。但是观察它们试图隐藏行迹的行为能提供很好的洞察角度。

一些国家将其行政部门、军队和情报机构置于法律监督之下。这意味着信息收集，尤其是破坏性行动必须得到法律部门的批准，而法律部门常常会约束这些行动。有时候借助技术分析，能明显看到这些限制措施，为溯源提供线索。对于震网，前反恐和网络安全官员理查德·克拉克（Richard Clarke）提到，他“强烈感觉到该行动是由华盛顿的一支律师团队操控或管理”，因为它的目标确认程序有意将间接损害最小化。[47]

溯源过程的行动层旨在合成不同来源的信息，包括来自技术层的信息，非技术分析和地缘政治背景信息。行动层的分析功能在于提出竞争性假设来解释事件。

分析计算机网络漏洞需要大量的准备工作。溯源中，分析破坏某个具体网络所需能力是一条有用的线索。如对伊朗核设施的震网攻击

[47] 罗恩·罗森鲍姆（Ron Rosenbum），“卡珊德拉综合症”，《史密森尼杂志》，43/1，（2012 年 4 月），第 12 页。

具有极高的人力密集特征。恶意软件的有效载荷需要极充分的具体目标信息，如控制发动机转速的变频器的细节，这些信息往往很难搞到；再如伊朗纳坦兹核电厂 IR-1 离心机的具体技术参数；以及有助了解机器构造的共振系统临界输入频率等。[48]震网使用零日漏洞的数量前所未有，约有 4-5 种，并首次使用针对可编程逻辑控制器（常用来控制工业机器）的 rootkit 攻击。[49]这些特点极大地缩小了目标的范围。其他一些准备还包括目标侦察和有效载荷测试。震网再一次提供了很好的范例：攻击改编了复杂的目标系统以获取动态效果。这需要提前测试。[50]测试环境必须使用 IR-1 离心机。这些机器很贵且难以获取。不用说非政府行为者，事实下只有极少数政府具备测试震网的能力，更何况编写和部署这一病毒。这进一步缩小了可能性。

计算机攻击的范围有变化。对一个目标的多起攻击可能是相互孤立的；也可能是相互关联，共同构成一个更大规模攻击行动，针对更多受害者，可能长期持续并影响更广泛的区域。这种多阶段打击行动常常被称为高级持续性威胁（APT）。黑客组织从一个行动到另一个行动，常常运用相同的战术，针对基础设施和一般目标，因此对某个 APT 的理解在溯源过程中常常带来重要启发。著名的例子是一个被冠名为 APT1 或“Comment Crew”的组织，它被认为由中国黑客组成，

[48] 伊万卡·巴尔扎什卡（Ivanka Barzashka），“网络武器有用吗？”，《英国皇家三军研究所期刊》，158/2（2013 年 4/5 月），第 48-56 页，第 51 页。

[49] 金姆·泽特（Kim Zetter），“数字侦探是如何发现史上危害最大的恶意软件震网的”，《连线》，2011 年 7 月 11 日。

[50] 威廉·布罗德（William Broad）等，“以色列测试蠕虫被认为在推迟伊朗核计划中发挥重要作用”，《纽约时报》，2011 年 1 月 15 日。

以粗心地重复使用社会工程战术和专门的基础设施而闻名。[51]另外一个可能更有经验的组织即曾被安全公司赛门铁克追踪的“Elderwood Project”。该组织以超乎寻常地频繁使用罕见漏洞而闻名，它依赖恶意代码 Hydraq，主要目标锁定在国防、信息技术和非赢利部门等。[52]判断一系列不同种类的事件是否构成一个 APT，取决于方法论。而在安全界，各方所采取的方法大相径庭。因此，一个公司或一个情报机构对一项攻击行动的总结可能有差异。[53]

一些攻击分多个阶段。不同阶段可能针对不同受害者，这会妨碍对攻击行动的重建。换句话说，一种攻击行为可能仅仅是实施更大，更复杂破坏行动的步骤之一。大规模攻击的构成会明显不同，这就使得将这些碎片化信息综合在一起十分困难。如 2011 年对安全公司 RSA 的攻击是大型攻击的重要组成部分，且其本身又是一个多阶段行动。这种行动损害了 RSA 出售的、广泛应用于政府和商业部门的 SecureID 系统。据报道，其后对洛克希德·马丁公司的入侵正是利用了被破坏的 SecureID。[54]一个更加精心策划的分段攻击案例是 DigiNotar 事件。一个自称为“Comodohacker”的伊朗黑客首先黑进 DigiNotar，一个荷兰政府所属的认证授权系统，用于认证网页服务器。他破坏认证授权后立即颁发大量假证书，假冒成谷歌和其他网站。这些证书让他能

[51] 《APT1 报告》，弗吉尼亚州亚历山大市，曼迪昂特公司，2013 年 2 月 18 日。

[52] 加文·奥戈曼（Gavin O’Gorman）和杰夫·麦克唐纳（Geoff McDonald），《Elderwood 计划》，赛门铁克，2012 年 9 月 6 日。

[53] 2014 年春夏期间，作者在多伦多、伦敦和华盛顿与多名分析家进行交流。

[54] 克里斯托弗·德鲁（Christopher Drew），“失窃数据被追踪到对洛克希德的攻击”，《纽约时报》，2011 年 6 月 3 日。

够截取近 30 万对此毫无察觉的伊朗用户发出的加密邮件。[55]

攻击会发生演变。随着时间的推移，一些攻击会发生与事先计划所不同的变化，能提供有关不断演进的政治与技术现实和目标的线索。震网再一次提供了很好的分析案例。正如控制系统分析专家拉夫·兰纳（Ralph Langner）在分析震网时所指出的那样，破坏离心机的软件有不同的变种。[56]这些变种的攻击方式不同，并会在不同时间被释放。2010 年 7 月主软件被发现后，回顾分析揭示，这种开创性攻击工具的第一版早在 2005 年 11 月就已被发现。最早版本的传播机制不同，不携带任何微软的零日漏洞，主要针对的是西门子 417 可编程逻辑控制器（PLCs），后来的版本则对该控制器基本无效。[57]这种战术的变化意味着攻击者优先目标和环境的变化。

事件的地缘政治背景能够成为一个警告。事后分析表明，具体事件的地缘政治背景往往是显而易见的：如 2007 年在爱沙尼亚或 2008 年格鲁吉亚战争期间发生的 DDOS 攻击。[58]但这些案例可能只是例外。分析一项入侵活动的地缘政治背景要求对特定行为者及其组织所处的具体区域，历史和政治知识有所了解。以 2012 年夏公布的高斯病毒（Gauss）为例，该行动以黎巴嫩金融机构为目标。[59]观察者推测其

[55] 对该事件的详细描述，可参阅汤姆斯·里德，《网络战不会发生》（牛津/纽约：牛津大学出版社 2013 年），第 26-29 页。

[56] 拉夫·朗纳(Ralph Langer)，“震网的秘密孪生兄弟”，《外交政策》，2013 年 11 月 19 日。

[57] 杰夫·麦克唐纳（Geoff McDonald），利亚姆·欧默奇（Liam O’Murchu），斯蒂芬·道尔蒂（Stephen Doherty）和埃里克·钱（Eric Chien），《震网 0.5：遗漏的关联》，第 1.0 版，赛门铁克公司，2013 年 2 月 26 日。

[58] 罗纳德·戴伯特（Ronald J. Deibert），拉法尔·罗霍金斯基（Rafal Rohozinski）和西端雅史（Masashi Crete-Nishihata），“网络空间的旋风”，《网络安全》43/1（2012 年），第 3-24 页。

[59] 《“高斯”病毒》，卡巴斯基实验室，2012 年 8 月 9 日。

目的在于揭露真主党的洗钱活动。[60]那些无人承认的、目的性强的网络破坏，地缘政治分析尤其能有效锁定嫌疑目标的数量。技术人员由于缺乏必要的知识无法进行这种分析。

雇员和承包商代表着一个机构的最强实力，但同时也是最大风险。威瑞森公司（Verizon）2013 年发布的事故报告证实，内部威胁和失误是机构面临的最大风险之一。经确认，在超过 1.1 万起事故中，个人被作为优先选择的突破口。[61]损失最大的攻击之一，即针对沙特阿美石油公司的沙蒙病毒就是由内部人员发动的。[62]少数几起已知的针对工控系统的攻击事件中，内部人员是最常见的因素。如 2000 年 3 月澳大利亚皇后岛马奇河（Maroochy）供水系统被破坏事件[63]以及同年发生在俄罗斯天然气股份有限公司（Gazprom）的管线事故。[64]大量控制系统事故都由内部人员造成，即使是那些从未公之与众的事故。当一项恶意攻击要求很难获得的极专业技能时，虽然不能完全排除外部因素，但要多考虑一下内鬼的可能性。

在战略层面，领导者和顶级分析家们应致力于综合行动层获取的问题答案，形成有意义的结论。当领导者和高级分析者能有效质疑前期分析，查明细节并找到替代性解释时，溯源过程的战略分析才能做到最佳。

---

[60] 参阅大卫·萨马（David Shamah），“新病毒可能是美国和以色列对真主党发起的数字空袭”，《以色列时报》，2012 年 8 月 13 日。

[61] 《2014 年数据破坏调查报告》，威瑞森公司，2014 年 4 月 22 日，第 23 页。

[62] 吉姆·芬克尔（Jim Finkle），“独家报道：沙特网络攻击怀疑是内鬼所为”，路透社，2012 年 9 月 7 日。

[63] 吉尔·斯莱（Jill Slay）和迈克尔·米勒（Michael Miller），“从马奇河供水系统被破坏事件中学到的教训”，来自 E·格茨（E. Goetz）和 S·谢诺依（S. Shenoi）（主编）的《关键基础设施保护》，第 253 卷（马里兰州波士顿，斯普林格出版社，2008 年），第 73-82 页。

[64] 拉夫·朗纳，“震网的秘密孪生兄弟”，《外交政策》，2013 年 11 月 19 日。对震网的详细讨论，可参阅金姆·泽特《倒数至零日》（纽约：皇冠出版社 2014 年）。

网络攻击的后果并不都是相同的。其所造成的损失是识别网络破坏最重要的辨别性特征。相较于现实世界的物理攻击，网络攻击的损害总是难以阻止和衡量。损害往往可分为四类：第一类是直接且迅速的影响，如降低服务器的正常运行时间，影响文档的可用性、数据的完整性甚或是破坏硬件，如上文提到的针对沙特阿美石油的“沙蒙”攻击。此次攻击破坏巨大且立竿见影，3 万个工作站同时受到影响。[65]第二类是直接但滞后的影响。震网对伊朗核离心机的操控破坏其构造，使其在相当一段时期内（即使不是几年也是几个月）不断出现机械故障。[66]第三类是是间接但迅速的影响，如对声誉的破坏和信心的丧失。如对易趣网的大规模攻击，1.45 亿消费者记录被破坏。[67]第四类是是间接且滞后的影响，如知识产权的丧失，一旦被竞争者获取即可能丢掉市场竞争力。一个有争议的例子就是加拿大网络设备制造商北电网络（Nortel）的转让。[68]总而言之，网络攻击的后果越不直接和滞后，其越难衡量。

攻击带来的后果可揭示攻击者的意图，特别是在行动层进行恰当的综合分析之后。根据“大姆指原则”（经验法则），破坏总是试图将直接影响最大化，无论是公开的还是秘密的。然而信息收集则尽量避免造成直接损害，以躲避监测和在未来收集更多的情报。当然，受害

---

[65] 克里斯托弗·布朗克（Christopher Bronk）和埃尼肯·提克（Eneken Tikk），“针对沙特阿美的网络攻击”，《生存》杂志 55/2（2013 年 4-5 月），第 81-96 页。

[66] 拉夫·兰纳，“震网的秘密孪生兄弟”，《外交政策》，2013 年 11 月 19 日。对震网的详细讨论，可参阅金姆·泽特《倒数至零日》（纽约：皇冠出版社 2014 年）。

[67] 安德烈·彼得森（Andrea Peterson），“数据被破坏后，易趣要求 1.45 亿用户更改密码”，《华盛顿邮报》，2014 年 5 月 21 日。

[68] 希奥布翰·戈尔曼（Siobhan Gorman），“中国黑客被疑发起历时长久的北电网络破坏行动”，《华尔街日报》，2012 年 2 月 14 日。

目标的种类也能为意图分析提供线索，因为不同攻击者会选择不同的优先打击目标。

设想的后果并不总和实际造成的后果一致，有两种可能性。第一种，攻击者意图明显，但并未如愿。2012 年阿美石油公司遭受攻击时，管理层推测攻击者的真实意图是操纵其石油生产控制系统，但显然没有成功。相对应的另一种情况是攻击切实带来了损失，但攻击者本意并非如此。计算机系统是复杂的，攻击者可能不清楚网络的布局，他们开展侦察时可能会造成一些无意的破坏。因此，分析者们必须结合其他领域的分析来评估损失。某次导致较小损害的网络攻击会是一个警示，很可能是一项未成功的、旨在破坏重要战略网络的行动，也可能仅仅是一个侦察活动带来的无意破坏。

理解网络攻击的来龙去脉很难，但十分重要。了解对手的动机和行为有助于避免未来的破坏。这种战略分析从定义上看是非技术的。比如，它依靠来自行动层基于地缘政治背景下提出的确凿信息和分析。以此为背景，分析还需要了解其他国家的优先选择，无论这些选择是商业性的、军事性的或经济性的。所有这些综合在一起就能分析出网络攻击意欲何为。它还能为对手的未来行动提供线索。如果一次意图明显的行动失败了，理解它为什么会失败以及对方接下来可能会采取什么措施来纠正这一失败，有助于减少攻击带来的破坏和有效应对。

网络行动是一个不同寻常的新领域，会出现许多“先例”。分析这些先例和预测未来不是一件容易的事：一个新的方法可能是一次性

的，也可能是一个趋势的开始。一些攻击也许揭示新的可能性，如震网中可编程逻辑控制器组件对工控系统的控制。一些攻击可能很引人注意但重要性有限，如 2012 年秋天劫持数据中心对美国银行发起的分布式拒绝服务攻击，这是一种新的技术手段，但不具有更强的战略重要性。[69]确定一个事件能否构成一个有意义的先例能够帮助溯源和后期的应对。

验证溯源过程的结果是重要的。所掌握的证据和初步结论需要查验。取证专家能获取最切实的证据，如日志文件和代码。行动分析家根据其他资源继续这一工作。在战略层，决策者和高级分析人员一道查明来自下层做出的竞争性假设，最终推动整个溯源过程。对分析进行严格的测试能暴露经不起推敲的假设，想像的缺乏和思维定式。对附加细节、替代性解释的分析与探查，可能需要对整个过程细节性知识的把握。本文的分析和提出模型意图促进这种探查。如果事件特别重要，还可选派一支红队回顾整个过程，或是对原有团队的工作进行重审。丘吉尔有句名言：“调查总是正确的。”[70]

第三部分

就溯源结果进行沟通是溯源过程的一部分。面对复杂的场景，高级官员和政治家只掌握溯源过程中的很小一部分，对公众而言，了解的则更少。信息披露的比例将决定外界（包括政治领导人，技术专家

[69] 尼科尔·帕尔斯（Nicole Perlroth）和昆廷·哈迪（Quentin Hardy），“官员称银行黑客攻击是伊朗人所为”，《纽约时报》，2013 年 1 月 8 日。

[70] 温斯顿·丘吉尔（Winston S. Churchill），《暴风前夕：第二次世界大战》，第 1 卷（纽约：罗塞塔出版社 2002 年），第 415 页。

社群和普通大众）如何知晓一个机构的工作。溯源各过程的特点在很多方面取决于各过程的沟通。情报曝光会损害情报源及情报搜集的方式。是否公开溯源结果难以决定，官员们常常过于谨慎和三缄其口。这么做的原因有很多。然而，对那些深陷秘密文化、不相信直觉的人而言，更多的公开性能带来三大重要好处：更多的细节交流意味着可信性、溯源和防御能力的提高。

首先，*公布更多细节将提升信息发布人和信息本身的可信度*。最近发生在美国的两个案例提供了很有价值的对比。2012 年 10 月 11 日，美国国防部对一项记录在案的著名攻击事件进行评论。五角大楼的头号人物帕内塔，对聚集在海洋航空航天博物馆的商业领袖们发表了引人注目的演讲。演讲地点颇有深意：该博物馆设在泊于纽约哈德逊河码头一艘经历过二战的无畏号航空母舰（埃塞克斯级航母）上：

“过去两年里，国防部为解决溯源问题投入巨资，我们现在正看到这些投资已有所回报。潜在的敌人应该知道美国有能力定位他们，让他们对损害美国及其利益的行为付出代价。”[71]

演讲中他还提到一个“令人震惊”的“发生在两个月前”的事件，一个名为沙蒙的高级病毒感染了沙特阿美石油公司的计算机。帕内塔提到了一些这次攻击的细节，但并没有提供任何溯源证据。几段话后，他紧接着提到了德黑兰：“伊朗也已采取切实的行动利用网络空间来夺取优势”。国际媒体的报道普遍将其解读为美国高官在指责伊朗。然而这位负责世上最先进信号情报设备的最高级国防官员只是暗示，

[71] 利昂·帕内塔，“出于国家安全目的对商界高管有关网络安全的演讲”，纽约，华盛顿特区：国防部，2012 年 10 月 12 日。

并没有提供任何能将伊朗和阿美公司攻击联系起来的证据。

20 个月后，美国政府选择了一个完全不同的策略。2014 年 5 月，美国司法部采取了一个极不寻常的举动：它起诉一个外国情报机构，即中国解放军 61398 部队的五名军人，称其进行计算机欺诈与滥用，破坏计算机，盗取身份和从事经济间谍活动。起诉文件十分详细：异于寻常地列出了位于宾州西部的六个受害公司、被盗数据的类型与价值及被盗时间。但此次指控并未提供大量溯源证据。司法部的声明称："这些共犯使用跳板窥探受害者，发送钓鱼邮件，储备和传播恶意软件，控制这些软件并传送盗来的数据。"[72]其潜台词是美国政府能够提供具体的 IP 地址，恶意软件样本和被盗文件，但起诉书本身并没有提供取证细节。从这方面来看，司法部文件的详尽程度不及曼迪昂特公司 15 个月前针对同一个中国军方部门的报告。然而，公布这些细节能支撑案件的审理，提高溯源的整体可信度。

第二个好处：*公布更多细节将提升溯源本身的质量*。当一个案子及其细节公之于众时，溯源的质量就可能提高。印象最为深刻的案例也许仍是对震网的多层面和高度创新性综合分析：不同的公司和研究机构对此恶意软件进行剖析，形成了大量侧重不同方面的极详细的报告。[73]另外一个例子是对中国间谍活动越来越多的详细报告，部分原因是安全公司之间的竞争。[74]因此，溯源市场得到大力发展：见诸于世的最有用和最详细的溯源报告由公司而非政府发布。本文研究中使

[72] "美国诉王栋、孙凯亮、文新宇、黄镇宇、顾春辉"，美国宾夕法尼亚州伊利市：宾州西区地方法庭，2014 年 5 月 1 日 。

[73] 要想全面了解，可参阅金姆·泽特，《倒数至零日》（纽约：皇冠出版社 2014 年）。

[74] 两个最著名的报告是《APT1》和《推杆熊猫》，《APT1》，弗吉尼亚州亚历山大曼迪昂特公司，2013 年 2 月 18 日，《推杆熊猫》，众击公司，2014 年 6 月 9 日。

用的证据与案例几乎都来自这些公司报告。情报机构已从事溯源工作几十年，甚至是几个世纪。然而它们的工作相对封闭，创新的动力来自秘密而非公开的竞争。要特别指出的是，这种情况的一个结果就是：公开并不意味着整个溯源过程的结束，而仅仅是进入一个新阶段。这个新阶段反过来又会催生新的证据和分析，进而要求调整相关的评估和对外行动。

第三个好处也是最重要的好处：*公开更多细节有利于更好地综合防御*。就结果进行沟通并不仅针对个案，而要提升综合安全。比如，讨论某次破坏活动所使用基础设施的细节能让其他网络管理者采取专门的防御措施。公布恶意程序新的病毒特征也有类似作用，因为他们能被其他管理者下载或加载到自动入侵监测系统。即使没有具体的好处，对攻击者所用新技术的细节性讨论也能为其他案件的调查者们提供有利信息。按高价提供威胁指标和更好的防御是网络安全公司的商业运营模式。政府如何应对这种发展态势无疑是一个公开而重要的问题。

公开结果常常影响攻击行为本身。随着更多溯源报告的出现，研究特定攻击者对意料之外的曝光采取何种反应已成为可能。比如，2014 年 2 月 10 日，卡巴斯基公布的“面具行动”报告中对西班牙语入侵设置进行了分析，“1 小时”后该行动就销声匿迹了。[75]2012 年 5 月，关于火焰病毒（Flame）的报告公布，侵入者在近 2 周后停止了

[75] 2014 年 10 月 8 日，作者在巴塞罗那采访考斯汀·拉伊乌，亚历克斯·古斯德夫（Aleks Gostev），库尔特·鲍姆加特纳（Kurt Baumgartner），文森特·迪亚兹（Vicente Diaz），伊戈尔·苏门科夫（Igor Soumenkov），谢尔盖·密涅瓦（Sergey Mineev）等人。参阅《揭秘“面具”》，第 1.0 版，卡巴斯基实验室，2014 年 2 月 6 日。

行动。[76]行动消失的方式能提供更多的溯源线索，比如行动的取消是否够专业，能否保持高水平的行动安全性。如果行动取消缓慢也许表明该行动的取消需经过大型官僚机构或组织的授权。当 Duqu 被发现时，其运行者忘记粉碎文件，这些文件虽然被删除但可恢复，从而使得行动的许多细节被揭露出来。[77]卡巴斯基公布的几个攻击行动都是在公布后消失，一些结束的比其他更快，一些结束的比其他更顺利："红色十月"、"小公爵"（Miniduke）和"冰雾"都在 2013 年全部消失。[78]尤其是后两者，卡巴斯基的报告并没有确定嫌疑攻击者甚至没有指出嫌疑国，攻击者仍撤退了。最值得注意的是，就在卡巴斯基报告公布*前*两周，2012 年 5 月 14 日，火焰病毒的操控者开始拆除其精心设计的命令控制设施，这表明攻击的高度复杂，甚至可能是一种预警。[79]2013 年 2 月 18 日，曼迪昂特公布 APT1 报告时，被披露的恶意行动先是停止了 41 天，但一直维持着低水平活动，持续到报告公布后近 160 天。[80]同年 3 月，该公司位于弗吉尼亚的网站受到来自中国的持续拒绝服务攻击。[81]如果是技术含量不高，来自中国的攻击会超乎寻常地持久，甚至是在溯源报告对行动敏感细节予以公布之后亦会持续。[82]

---

[76] 亚历山大·高斯德夫，《火焰病毒问答》，卡巴斯基实验室，2012 年 5 月 28 日。

[77] 维塔利·卡姆路克（Vitaly Kamluk），"Duqu 的秘密之六"，Securelist 网站，2011 年 11 月 30 日。

[78]《"红色十月"外交网络攻击调查》，第 1.0 版，卡巴斯基实验室，2013 年 1 月 14 日；考斯汀·拉伊乌，伊戈尔·苏门科夫，库尔特·鲍姆加特纳和维塔利·卡姆鲁克（Vitaly Kamluk），《Miniduke 的秘密》，卡巴斯基实验室，2013 年 2 月 25 日；《"冰雾"APT》，卡巴斯基实验室，2013 年 9 月 25 日。

[79] 10 月 8 日在巴塞罗那与卡巴斯基实验室人员进行专题讨论，2014 年 10 月 12 日与考斯汀·拉伊乌进行电邮沟通，英国夏令时 11：49。

[80] 《威胁报告：破坏之外》，弗吉尼亚州雷斯顿，曼迪昂特公司，2014 年 2 月 18 日，第 18 页。

[81] 理查德·贝杰特里奇（Richard Bejtlich），电邮沟通，2014 年 10 月 11 日，英国夏令时 1：41。

[82] 一个例子是所谓的 NetTraveler 行动，它只是简单地把命令与控制服务器转移到了香港，然而继续通过这些服务器发起攻击，与考斯汀的电邮沟通，2014 年 10 月 12 日，英国夏令时 11：49。参阅《NetTraveler

公开交流最终反映出溯源是渐进的而非绝对的。安全公司和政府在操作中应注意一点：使用评估可能性的词语。情报分析先趋舍曼·肯特（Sherman Kent）1968 年写道：“在情报机构，正如在其他行当一样，评估是在你不知所措时应做的事情”。[83]评估性语言是“事实与判断的混合”。这种事实与判断的混合特别适用于网络安全领域。估计是有意以一种易受攻击的方式进行表达，从而公开接受批评。一份报告对于其知识的有限性和评估的表达越诚实，其整个分析的可信度越高。因为正如肯特所言：“情报评估是接下来最好的事情”。[84]

结论

本文的研究介绍了一个追溯网络攻击的系统模型，并提出了三个核心观点：第一，溯源是一门艺术：没有单纯的技术方法可能程式化、计算、量化或全自动实现溯源，无论这种技术是简单的还是复杂的。高质量的溯源取决于各种技巧、工具以及组织文化：合作顺畅的团队、能力突出的个人、丰富的经验以及从一开始就出现的、难以描述的“有问题”的感觉。[85]第二，溯源是一个微妙的、多层次的过程，而非一个能简单回答的问题。这个过程要求谨慎的管理、培训和有效的领导。第三，溯源依赖于政治风险。某个事件带来的后果越严重、造成的损失越大，政府在确定攻击者时可投入的资源和政治资本就会越多。在对某次攻击所采取的所有响应，包括执法、外交或军事手段中，溯源

行动》，卡巴斯基实验室，2013 年 6 月 4 日。

[83] 舍曼·肯特（Sherman Kent），“评估与影响”，《情报研究》 12，（1968 年夏），第 11-21 页。

[84] 同上。

[85] 与来自私营和公共部门的分析人员进行的小组讨论，2014 年 9 月。

是最基本的一项工作，即首先需要明确攻击者是谁。政府决定如何开展溯源，以及溯源到何种程度就足以采取回应行动。

我们对实际溯源的分析引发了对网络安全争论中的一些共识性观点的怀疑。第一个观点是包括罪犯、间谍到破坏者在内的攻击人能够掩盖他们的踪迹，在网上能隐瞒自己的真实身份，进而逃避追踪。[86]但溯源不仅仅是可不可能的问题，很久以来它已取得了成功。攻击者不能假设能掩盖真实身份制造破坏，而且还能侥幸逃脱处罚。即便溯源问题不能从根本上解决，但它原则上是可以管理的。

第二个迂腐的观点是，互联网剥夺了国家的权力而且把这个权力转移到了非国家行为体、私人机构和罪犯手中，技术使得大家平起平坐。[87]对溯源而已，事情则正相反：只有国家拥有把光圈打开得足够大、准确追踪到最复杂行动的能力。2013 年美国国家安全局（NSA）、英国政府通讯总部（GCHQ）信息的泄露并未阻止它们，讽刺的是，对那些倾向于高估这些部门能力的局外人来说，曝光反而增强了它们溯源的可靠性。

第三个常见的观点是，工业化程度最高、彼此联系最密切的国家最脆弱，不发达且不怎脆弱的国家拥有优势。[88]溯源再一次反证了这一逻辑：政府的技术能力越强，拥有的人才与技术越多，国家隐藏自身秘密行动、揭发其他国家及作出响应的能力越大。

---

[86] 对这个观点最好的阐述可能是理查德·克莱顿（Richard Clayton），《网络空间的匿名和追踪》，《技术报告》第 653 卷（剑桥：剑桥大学计算机实验室 2005 年）。

[87] 例如可参阅约瑟夫·奈，《网络权力》（弗吉尼亚州贝尔沃堡：国防技术信息中心，2010 年）。

[88] 例如，迈克尔·麦康奈尔（Michael McConnell），“网络战是新的原子时代”，《新观点季刊》26/3（2009 年夏），第 72-77 页。

本文分析可能挑起的另一个争论是互联网是一个攻方占优的领域。[89]持这一观点的人认为，入侵者相较下防御者拥有结构性优势，这一优势根源于互联网的技术架构。守方在所有时候都不能做错，攻方只需做对一次就成功。溯源再一次证明这是错的：入侵者只需犯一个错误，防御者的取证分析就能发现被遗漏的线索来揭露整个行动。

然而，进一步研究溯源的局限性很关键。第一个突出的局限性就与资源、尤其是技术和能力有关。*溯源的质量是关于可用资源的函数*。即使国际网络安全市场快速成长，老道的取证技巧以及复杂行动中的组织经验仍然稀缺。溯源过程中掌握的资源越少，它的质量就最难以保证。第二个重要的局限性是时间：*溯源的质量是可用时间的函数*。即便对最专业、拥有最好资源的团队、企业和部门而言，在有限的时间里分析一次精心设计的行动都是一个重大的挑战。在一些重大的案子中，当高层决策者不得不在高压下做出决定时，政治局势的发展远远快于溯源进展。溯源所能得到的时间越短，其质量也越低。

第三个重要的局限性是敌方的行为：*溯源的质量是关于敌方老练程度的函数*。现已公布的最为令人信服的证据获得前，一些操作人员曾犯过错误，或者没有考虑到使用某些方法可能影响取证。老练的攻击者往往老谋深算，最大程度地掩盖并扰乱他们留下的痕迹。这需要运用多种资源来揭露证据，从而使溯源更困难。但敌人会犯错误使溯源看到一线曙光。完美的网络攻击就像完美犯罪一样难以捉摸。然而，

[89] 最早的研究可参见约翰·阿奎拉（John Arquilla）和大卫·朗斐德(David Ronfeldt)，《网络战的到来》（加利福尼亚州圣莫尼卡，兰德公司，1996 年），第 94 页；还有国防部《网络政策报告》，2011 年 11 月，第 2 页。

敌人越是老练，溯源花费的时间越长也越困难。

未来溯源仍将保持其独特性。1999 年以来，网络发生了显著的变化，但互联网本身没有变化，它根本构架的变化也很缓慢。因此，溯源本身也不会出现太大变化——但是它会以一种自相矛盾的方式在演变。一方面，溯源正在变得*更容易*。更完善的入侵侦测系统能实时发现攻击，能更快地调用更多数据。适应性更强的网络将提高攻击行动的成本，能消除不确定因素，节省出资源以更好地识别高级攻击。网络犯罪增多，能推动执法部门、甚至是不友好国家间执法部门的合作，这也能使国对国的间谍行动更难以隐藏，政治成本更高。

但同时溯源也正变得更困难。攻击者能从被公开的错误中汲取教训。强加密技术使用的增多也给取证制造了更多问题，制约了大规模数据的搜集。过度的夸大和危机将阻碍微妙的沟通。溯源疲劳症开始出现。事实上，由于没有出现重大的后果，国家与非国家行为体可能不怎么担心被抓个正着，一个宽松的后果可以忽略不计的规则正在出现。讽刺的是，比起公开问责的自由民主政府，非民主国家可能更不担心被抓。因此，讨论也回到文章的起始点：溯源过程是一个技术-政治问题，是由国家决定的，通过投入时间、资源、政治资本以及战胜敌人的努力。

溯源面临的核心局限同样展现了本文的局限。一些最成功的溯源仍然不为人知，被一些国家封锁。未来，政府部门或安全公司将开发出更多的工具，或者把这些公诸于世，由此为溯源打开一个新的视角。一些信号情报能力可能已经为溯源提供了更多的可能性：甚至那些很

少甚至不犯错误的极其高明的敌人理论上也可能被发现。本文并未得益于公众并不了解的进展和能力。然而，文章的分析在很长时间内将能自圆其说。自 1998 年第一次重大的国对国行动“月光迷宫”被揭露以来，溯源最核心的变量始终保持不变。

本文旨在实现两个目标。第一目标是提高官僚部门工作的质量。时间给高质量的溯源带来高压，尤其在利害攸关时。模型是为了确保质量，使溯源更高效和有弹性：我们详尽的图表能帮助公共部门和国会的高层领导理解证据是如何收集的，能够提出更确切的问题，能够发现判断上的偏差，进而能证实和完善他们的观点。与此同时，模型使得各层级的分析人员能够在复杂的政治背景下各司其职。第二个目标更大：提高公共讨论的质量。让人失望的是，较大范围的网络安全辩论质量不高。这包括在世界一流的新闻媒体中有关的技术报道。政治科学和国际关系学者的论述显然都受源自技术细节及其局限性的影响。我们希望 Q 模型将有助于提高大家讨论的水平。

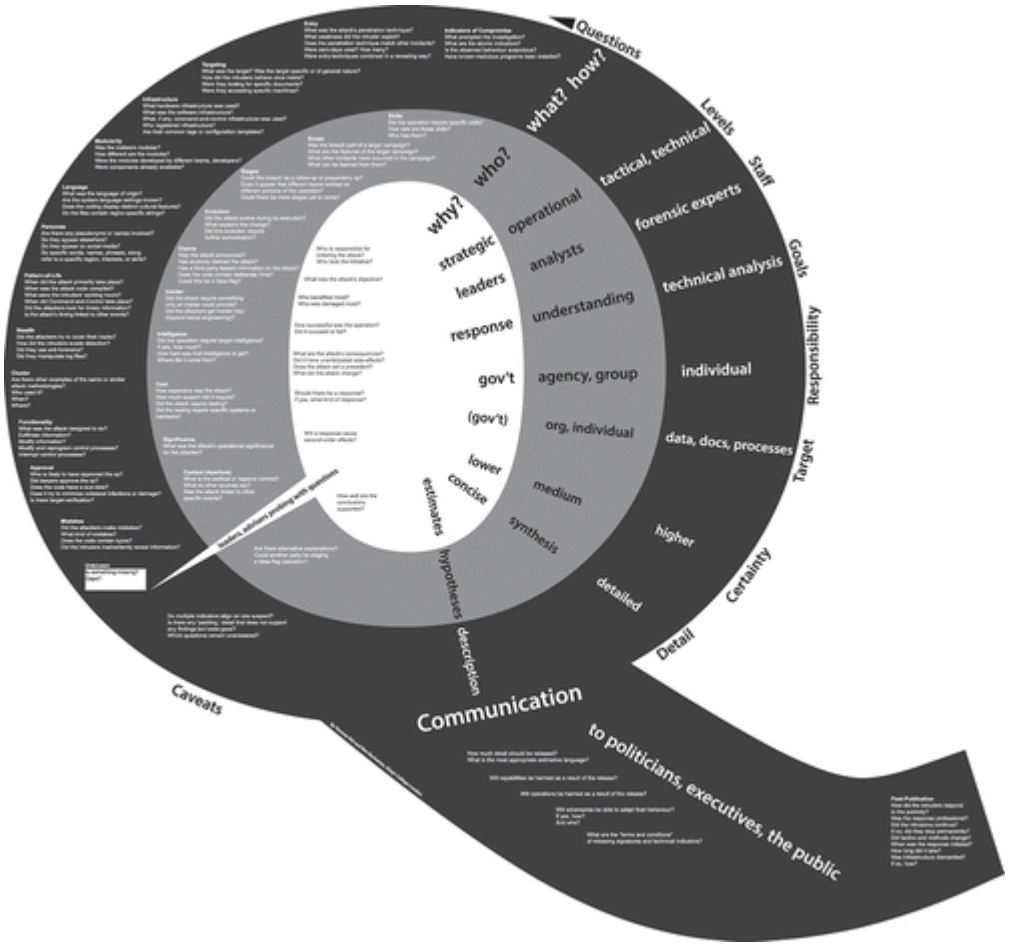


表 3：详细的 Q 模型。

附录

Q 模型是一张溯源过程的地图：它可以让那些没有技术背景的人大致了解溯源的过程；可以让学者、政治家或高管详细了解技术细节，与技术专家进行有意义的对话。反之，模型可以让证据分析者了解战略与政治背景。

在本文的在线 PDF 版本中，上图有更为清晰的版本。单独的图表可参阅 http://figshare.com/articles/Attributing_Cyber_Attacks/1284592。

最好的格式是 A0， 打印尺寸是 841 毫米×1189 毫米。

致谢

作者感谢德米特里·艾尔帕洛维奇（Dmitri Alperovitch），罗斯·安德林（Ross Anderson），詹姆斯·艾伦（James Allen），理查德·贝杰特里奇（Richard Bejtlich），库尔特·鲍姆加特纳（Kurt Baumgartner），克里斯汀·丹尼森（Kristen Dennesen），布兰登·迪克森（Brandon Dixon），韦森特·迪亚兹（Vicente Diaz），亚历山大·古斯德夫（Alexander Gostev），迈克·古德曼(Mike Goodman)，鲍勃·戈尔利（Bob Gourley），克莱蒙特·吉顿（Clement Guitton），纳撒尼尔·哈特利（Nathaniel Hartley），杰森·希利（Jason Healey），伊莱·杰伦齐（Eli Jellenc），罗伯特·李（Robert Lee），乔伊·马伊奥洛（Joe Maiolo），谢尔盖·密涅夫（Sergei Mineev），丹尼尔·摩尔（Daniel Moore），内德·莫兰（Ned Moran），大卫·欧曼德（David Omand），考斯汀·拉伊乌（Costin Raiu），马库斯·萨库斯（Marcus Sachs），伊戈尔·索门科夫（Igor Soumenkov），珍·威登（Jen Weedon），两位匿名受访者，以及几位不愿具名的英国和美国情报与安全界人士。一些公司提供了有价值的观点，尤其是众击，火眼，卡巴斯其实验室和布兹·艾伦·汉密尔顿。本文陈述的观点仅仅代表作者个人，文中可能出现的纰漏也由作者本人负责。

作者简介

托马斯·里德是伦敦国王学院战争系教授，著有《网络战不会发生》（牛津大学出版社，2013 年）。

本·布坎南是战争系在读博士生，马歇尔奖学金获得者。他还是一名获得了资格认证的计算机取证分析师。

参考文献

内特·安德森和赛勒斯·法里瓦尔，“联邦政府是如何击垮‘恐怖海盗罗伯茨’的”，科技博客 Ars Technica 网站，2013 年 10 月 3 日 。

《APT1》，亚历山大，弗吉尼亚州曼迪昂特公司，2013 年 2 月 18 日。

约翰·阿奎拉和大卫·朗斐德，《网络战的出现》（兰德公司，加利福尼亚州圣莫尼卡，1996 年）。

罗伯特·阿克塞尔罗德和鲁门·伊利耶夫，“网络冲突的时间”，PNAS，111/4（2014 年 1 月 28 日），第 1298-1303 页。

“网络武器有效吗？”英国皇家三军联合研究所（RUSI）期刊 158/2，（2013 年 4/5 月），第 48-56 页。

理查德·K·贝茨， “分析，战争与决策：情报失败为什么不可避免“，《世界政治》，31/1，（1978 年 10 月），第 61-89 页。

大卫·贝茨和蒂姆·斯蒂文斯，“网络空间与国家”，阿德尔菲系列丛书（伦敦，国际战略研究所，劳特里奇出版社，2011 年）。

W·厄尔·罗伯特，“对溯源面临挑战的调查”，“制止网络攻击委员会”主编《制止网络攻击研讨会进展》（华盛顿特区：国家学术出版社,2011），第 41-54 页。

苏珊·布伦纳，“光速：网络犯罪、恐怖主义和战争的溯源与响应”，

《刑法与犯罪学期刊》，97/2（2207 年），第 379-475 页。

克里斯托弗·布朗克和埃尼肯·提克，“针对沙特阿美石油公司的网络攻击”，《生存》55/2（2013 年 4-5 月），第 81-96 页。

谢尔盖·卡塔吉拉诺，安德鲁·鼓德格斯特和克里斯托弗·贝茨，《入侵分析的钻石模型》，ADA586960，（马里兰州汉诺威，网络威胁情报与威胁研究中心，2013 年 7 月 5 日）。

温斯顿·S·邱吉尔，《暴风前夜：第二次世界大战》，第一卷，（纽约罗塞塔出版社，2002 年）。

大卫·D·克拉克和苏珊·兰道，“解决溯源问题”，“制止网络攻击委员会”主编《制止网络攻击研讨会进展》（华盛顿特区：国家学术出版社,2011），第 25-40 页。

卡尔·冯·克劳塞维茨，《战争论》，由迈克尔·霍华德和彼得·帕雷特翻译（普林斯顿大学出版社，1976 年）。

理查德·克莱顿，“网络空间的匿名与追踪”，第 653 卷，《技术报告》（剑桥大学计算机实验室，2005 年）。

罗纳德·J·戴伯特，拉法尔·罗霍金斯基和西端雅史，“网络空间的旋风”，《安全对话》43/1（2012 年），第 3-24 页。

美国国防部《网络空间政策报告》，2011 年 11 月。

卡巴斯基实验室《高斯行动》，2012 年 8 月 9 日。

众击公司《全球威胁报告》，弗吉尼亚州阿灵顿，2014 年 1 月 22 日。

杰克·戈登史密斯和蒂姆·吴，《谁控制互联网？无边界世界的幻

觉》(牛津大学出版社，2006 年)。

亚历山大·古斯德夫，“火焰：问与答”，卡巴斯基实验室，2012 年 5 月 28 日。

纳撒尼尔·哈特利，《追溯到中国人民解放军 61486 部队》（众击，2014 年 6 月 9 日)。

杰森·希利，《一个斗争激烈的领域》(华盛顿特区：大西洋理事会，2013 年)。

埃里克·M·哈钦斯，迈克尔·克洛佩特和罗翰·阿敏，《在分析敌方行动和入侵杀伤链基础上受情报驱动的计算机网络防御》（马里兰州贝塞斯塔，洛克希德·马丁公司，2010 年)。

舍曼·肯特，“评估与影响”，《情报研究》 12，(1968 年夏)，第 11-21 页。

罗伯特·内克，“解决溯源：迈向网络空间的问责，谋划网络攻击的未来”，华盛顿特区：技术与创新附属委员会，第 111 届国会，2010 年 7 月 15 日。

拉夫·朗纳，“震网的秘密孪生兄弟”，《外交政策》，2013 年 11 月 19 日。

马丁·利比基，《网络威慑与网络战》(加利福尼亚州圣莫尼卡，兰德公司，2009 年)。

乔恩·R·林塞，“震网及网络战的局限”，《安全研究》22/3（2013 年)，第 365-404 页。

埃米尔·卢波维奇，“溯源与暴力的社会建构”，《国际研究视点》

2014 年，第 1-21 页。

迈克尔·麦康奈尔，“网络战是新原子时代”，《新视点季刊》26/3（2009 年夏），第 72-77 页。

杰夫·麦克唐纳，利亚姆·欧默奇，斯蒂芬·道尔蒂和埃里克·钱，《震网 0.5：遗失的环节》，第 1 版，赛门铁克公司，2013 年 2 月 26 日。

内德·莫兰，詹姆斯·班尼特，《供应链分析：从军需官到百货店》，火眼实验室，2013 年 11 月 11 日。

约瑟夫·奈，《网络权力》（弗吉尼亚州贝尔沃堡，国防技术信息中心，2010 年）。

加文·奥戈曼和杰夫·麦克唐纳，《Ederwood 计划》，赛门铁克公司，2012 年 9 月 6 日。

里昂·帕内塔，“对企业高管发表的国家安全中网络安全的讲话”，纽约，美国国防部 2012 年 10 月 12 日。

《推杆熊猫》，众击公司，2014 年 6 月 9 日。

考斯汀·拉伊乌，伊戈尔·苏门科夫，库尔特·鲍姆加特纳和维塔利·卡姆鲁克，《Miniduke 的秘密》，卡巴斯基实验室，2013 年 2 月 25 日。

卡巴斯基实验室《红色十月：外交网络攻击调查》，第 1 版，2013 年 1 月 14 日。

托马斯·里德，《网络战不会发生》（牛津/纽约，牛津大学出版社，2013 年）。

乌里·瑞弗纳，《对一场攻击的剖析》，RSA 公司，2011 年 4 月 1 日。

马尔科·罗西尼，《网络行动和国际法上的使用武力》，（牛津大学出版社，2014 年）。

罗恩·罗森鲍姆，“卡珊德拉综合症”，《史密森尼杂志》43/1（2012 年 4 月），第 12 页。

赛斯·舍恩和伊娃·戈尔佩林，“伊朗对谷歌的中间人攻击表明认证授权存在危险的漏洞”，电子前沿基金会，2011 年 8 月 29 日。

P·W·辛格和艾伦·弗里德曼，《网络安全与网络战》（纽约/牛津，牛津大学出版社 2014 年）。

吉尔·斯莱和迈克尔·米勒，“马奇决堤的教训”，来自 E·格茨和 S·谢诺依主编的《关键基础设施保护》，第 253 卷（马里兰州波士顿，2008 年春），第 73-82 页。

克利福德·斯托尔，《布谷鸟蛋》（纽约，双日出版社，1989 年）。

《Epic Turla 行动》，卡巴斯基实验室，2013 年 9 月 25 日。

《“冰雾”高级持续性威胁》，卡巴斯基实验室，2013 年 9 月 25 日。

《Net Traveler 行动》，卡巴斯基实验室，2013 年 6 月 4 日。

《威胁报告：远不止于泄露》，弗吉尼亚州雷斯顿，曼迪昂特公司，2014 年 2 月 18 日。

尼古拉斯·查哥里亚斯，“网络攻击，自卫与溯源问题”，《冲突与安全法律期刊》17/2（2013 年），第 229-244 页。

“美国诉王栋、孙凯亮、文新宇、黄镇宇、顾春辉”，美国宾夕

法尼亚州伊利市：宾州西区地方法庭，2014 年 5 月 1 日 。

《起底“面具”行动》，第 1 版，卡巴斯基实验室，2014 年 2 月 6 日。

丹·维尔顿,《少年黑客的忏悔》(纽约：麦格劳·希尔出版社，2000 年)。

马修·韦克斯曼,“网络攻击与使用武力”,《耶鲁大学国际法期刊》36（2011 年），第 421-459 页。

尼古拉斯·韦弗，“近观美国国家安全局最强大的互联网攻击工具”,《连线》，2014 年 3 月 13 日。

大卫·惠勒和格里高里·拉森,《网络攻击的技术溯源》(弗吉尼亚州亚历山大，国防分析中心，2003 年)。

《“W32. Duqu”行动》，第 1.4 版，赛门铁克公司，2011 年 11 月 23 日。

金姆·泽特,“数字侦探是如何发现史上危害最大的恶意软件——震网的”,《连线》，2011 年 7 月 11 日。

金姆·泽特,《倒数至零日》(纽约皇冠出版社，2014 年)。