

增强情报工程的对冲能力

在标题上，笔者原想写的是“增强情报工程的反情报能力”，但由于“反情报（Counterintelligence, CI）”一词已指特定场合下的具体事宜，容易引发文学遐想，故以“对冲能力”来表达。而且，人们也不难发现“情报的对冲能力”的意蕴要比“反情报”宽厚得多。虽然在竞争情报与反竞争情报类似的研究和操作中，决策主体可进行多维度的并行思考，但这里的“反”其中更多的意思是“防”，主要还是防泄露重于防干扰。但在今天大数据和信息过载情形下，应对虚假信息、干扰信息、冗余信息、污染信息、隐患信息、垃圾信息、僵尸信息等这一切正成为新的业务主流。面向种种的竞争与合作、对抗与联盟、差别与协同，我们所强调的情报对冲能力，则指的是对情报对冲策略谋划、对冲方案设计、对冲机制运行、对冲算法博弈、对冲利益评估、对冲风险化解、对冲危机防范，是将情报的对冲操作作为情报工程的内置功能予以统筹。

对冲（hedge/hedging）这个来自过去农庄和现在金融界的词汇，目前已遍及几乎所有带有风险议题的领域。一谈到风险，要么是趋利避害的条件反射，要么就是借力打力的对冲套路。金融领域的确是对冲策略快速应用、也会得到快速验证的场合。市场竞争以及公共场合的情报工程也已具备足够的资源和技术手段，来运行对冲策略或方案。

情报领域的对冲策略，不是简单地故意编排正反两方面的信息、或投放冗余信息以增加对方情报工程执行的复杂度，而是预先充分考虑到情报对冲的需要而进行的一体化功能设计。因为时间和投入成本、产出效益都不允许节外生枝；因为在多渠道信息获取的今天，人们很难做到让所有信道的信息在正反两方面都是一致的，无须做“此地无银”的标签；还因为 Intelligence（情报/智能）本身就包括了分析考量 If not（如果不）情形下的结果。

增强情报工程情报对冲能力，以“容”为先。情报工程要容信息、容数据、容算法、容软件、容方案、容网络、容感知、容智能，容得越多，

情报工程的对冲资源就越丰富，并且还要保证有在线的深度学习和推行能力，能随时随地进行前瞻并给出初级预案。

增强情报工程情报对冲能力，以“韧”为要。

“颠扑不破”这个成语最能表达韧字的神韵。韧性之极要抗得住任何风险的折腾，有自加压力，也有外部挑战。但无论怎样，韧性良好的情报工程总能保证全天候运行。这种韧性来自良好的技术体系设计和恰当的人机协作。

增强情报工程情报对冲能力，以“频”为常。在情报工程的运行中，对冲是永远在进行中的操作，而且在当下算力条件下还是高频操作。不论是处于风险环境下的决策主体还是竞争中的双方，都会不断升级完善自己的情报工程，将来自环境或对方的各种信息数据、对其中的预决策要在短时间内进行多频次的分析研判。常态化、高频次、快反馈将是对冲策略运行的基本特征。

增强情报工程情报对冲能力，以“控”为本。情报工程系统本身有一个可控制的要求，执行对冲策略和方案实际上还会带来一个超越原设想之外高阶的可控制问题，面对“升维思考、降维操作”、“不创新等死、创新找死”、“想颠覆他人、又不想被人颠覆”等众多复杂两难的博弈局面、各种疑阵和陷阱，找准其中可控制的抓手，是情报工程安身立命的根本点。

本期共收录 10 篇文章，其中专题聚焦于专利分析问题，特邀专题论文 3 篇，分别就专利联盟组建与运行模式、专利主题标注潜在语义分析、人工智能领域专利合作演化进行了探讨。有 2 篇文章分别面向国际期刊可重复性、中国情报领域核心作者进行了深入分析和研究。另外，本期还收录了关于动态技术轨道识别、弱信号介入的风险识别本体构建、近 10 年我国情报学领域核心作者计量分析等方面的 3 篇文章，以及区域产学研创新系统耦合协调度、高校大型仪器第三方机构运行模式等两篇文章，从科技管理和数据治理角度分析了影响因素、存在问题并提出了相应的政策建议。

刘琦岩

2020年6月于北京