第四届全国网络与信息安全防护峰会

安全威胁与威胁情报

杜跃进　博士

阿里巴巴集团 安全部

行远不忘初心：我们为什么来到这里

概念：事件、威胁、风险

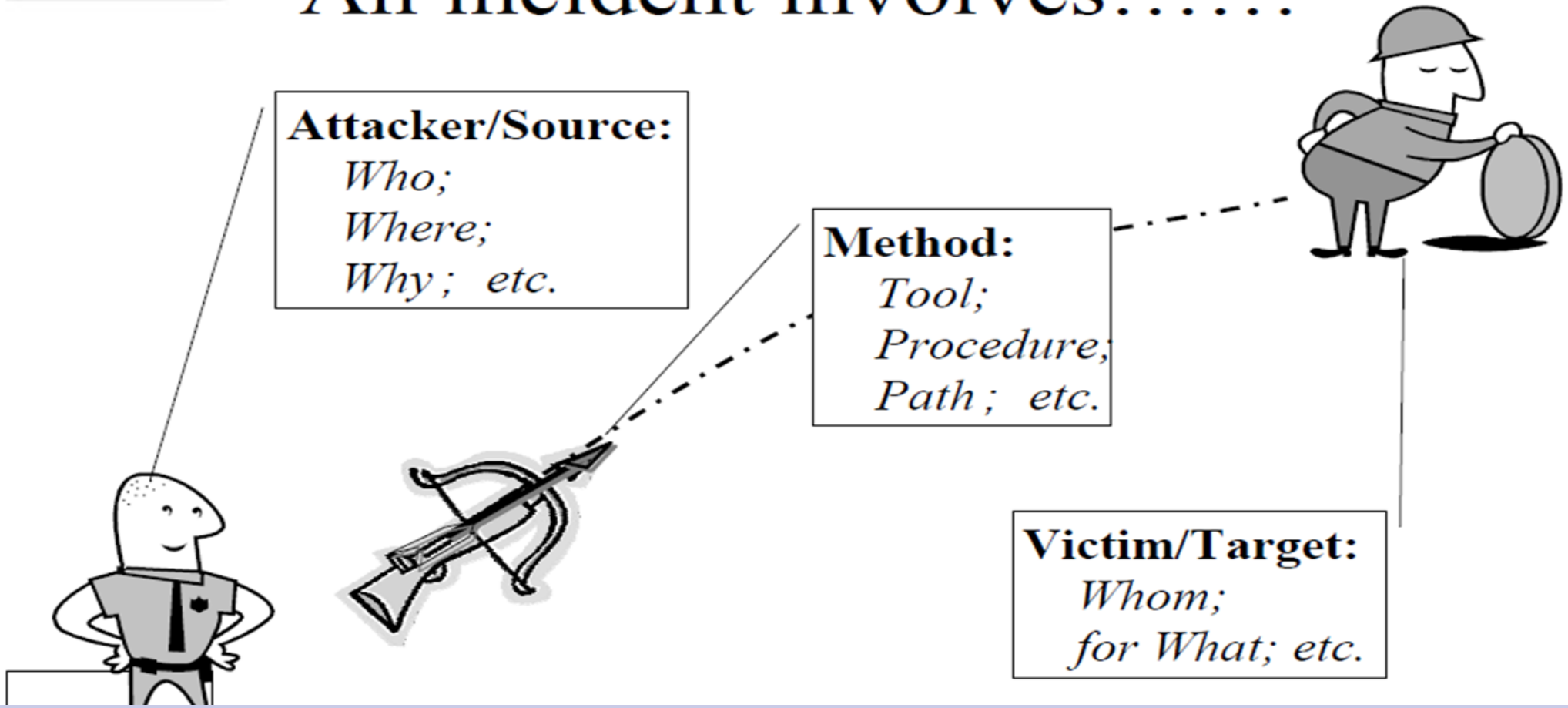
CN ERT/CC

An incident involves……

Attacker/Source:
Who;
Where;
Why ; etc.

Method:
Tool;
Procedure;
Path ; etc.

Victim/Target:
Whom;
for What; etc.



改变概念的价值？

避免雷达失灵


红动中国 Redocn.com
编号：89704　红动中国 (www.redocn.com)　chb031

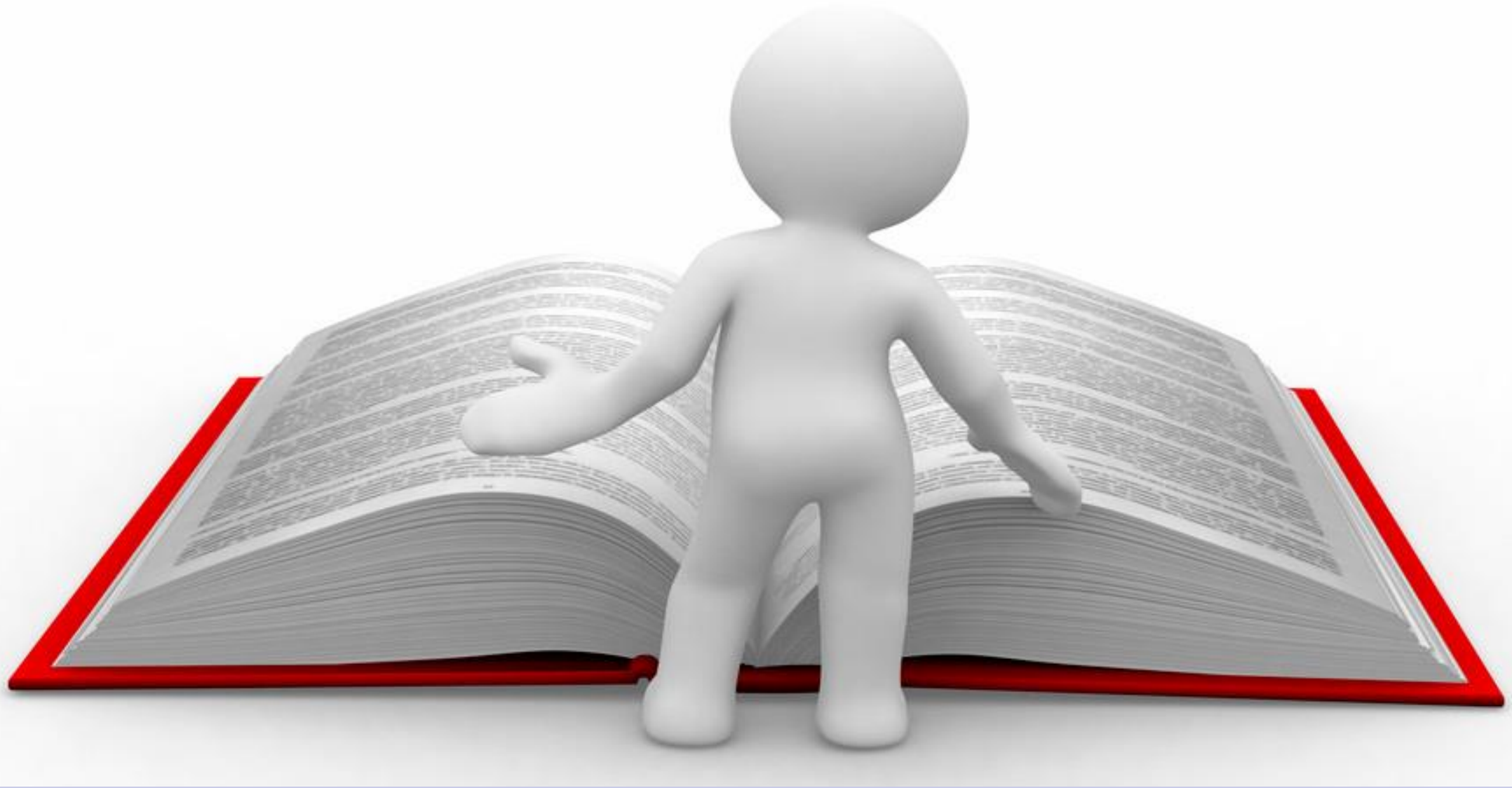

昵图网 www.nipic.com

避免视而不见

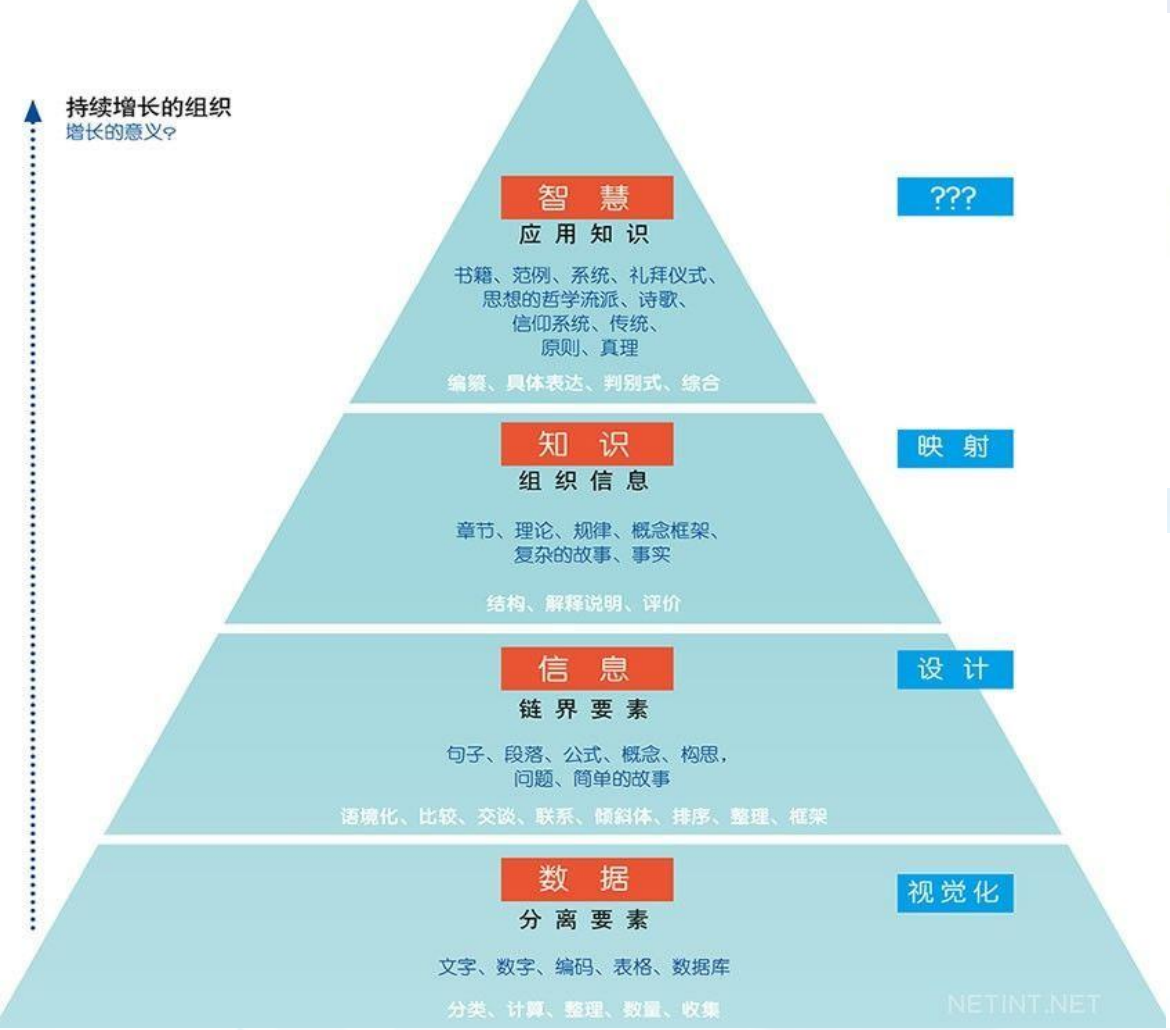
避免劳而无功

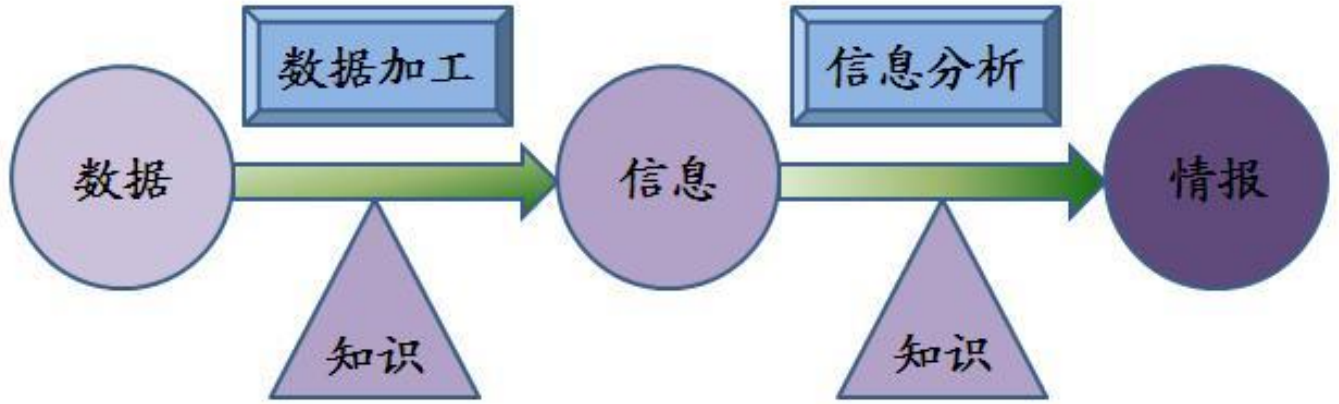
避免全无威慑

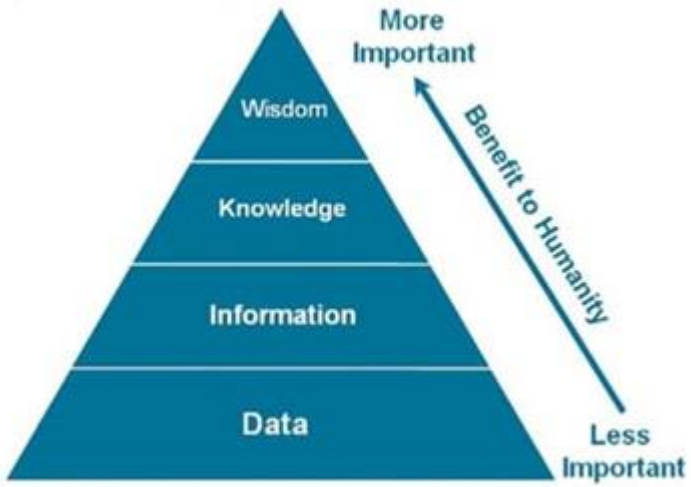
避免鸡同鸭讲

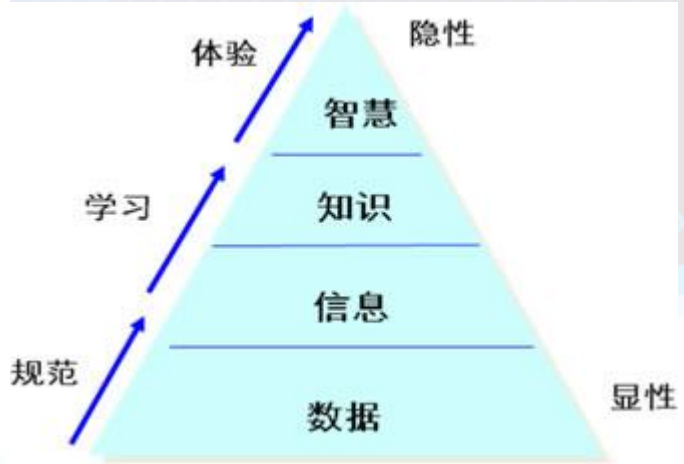


威胁应对的前提：威胁知识/情报

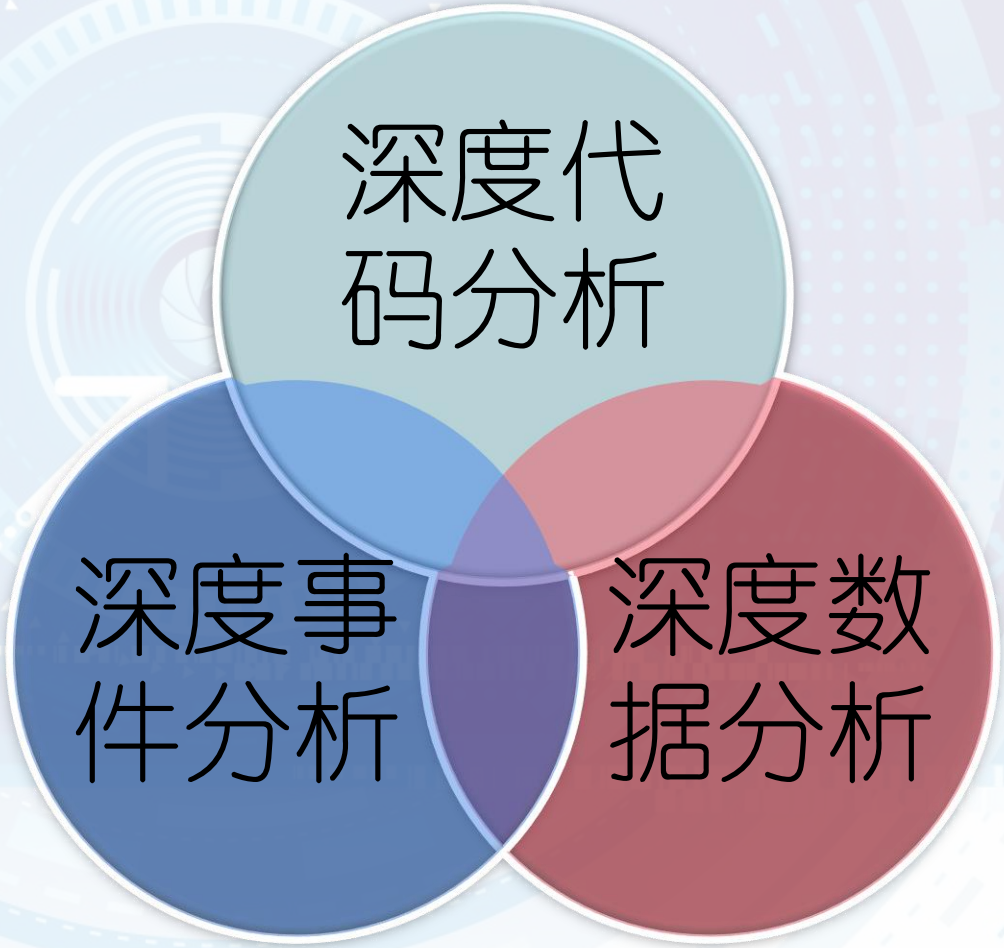

持续增长的组织
增长的意义?
智 慧
应 用 知 识
书籍、范例、系统、礼拜仪式、
思想的哲学流派、诗歌、
信仰系统、传统、
原则、真理
编纂、具体表达、判别式、综合
???
知 识
组 织 信 息
章节、理论、规律、概念框架、
复杂的故事、事实
结构、解释说明、评价
映 射
信 息
链 界 要 素
句子、段落、公式、概念、构思,
问题、简单的故事
语境化、比较、交谈、联系、倾斜体、排序、整理、框架
设 计
数 据
分 离 要 素
文字、数字、编码、表格、数据库
分类、计算、整理、数量、收集
视觉化
NETINT.NET


数据
数据加工
信息
信息分析
情报
知识
知识

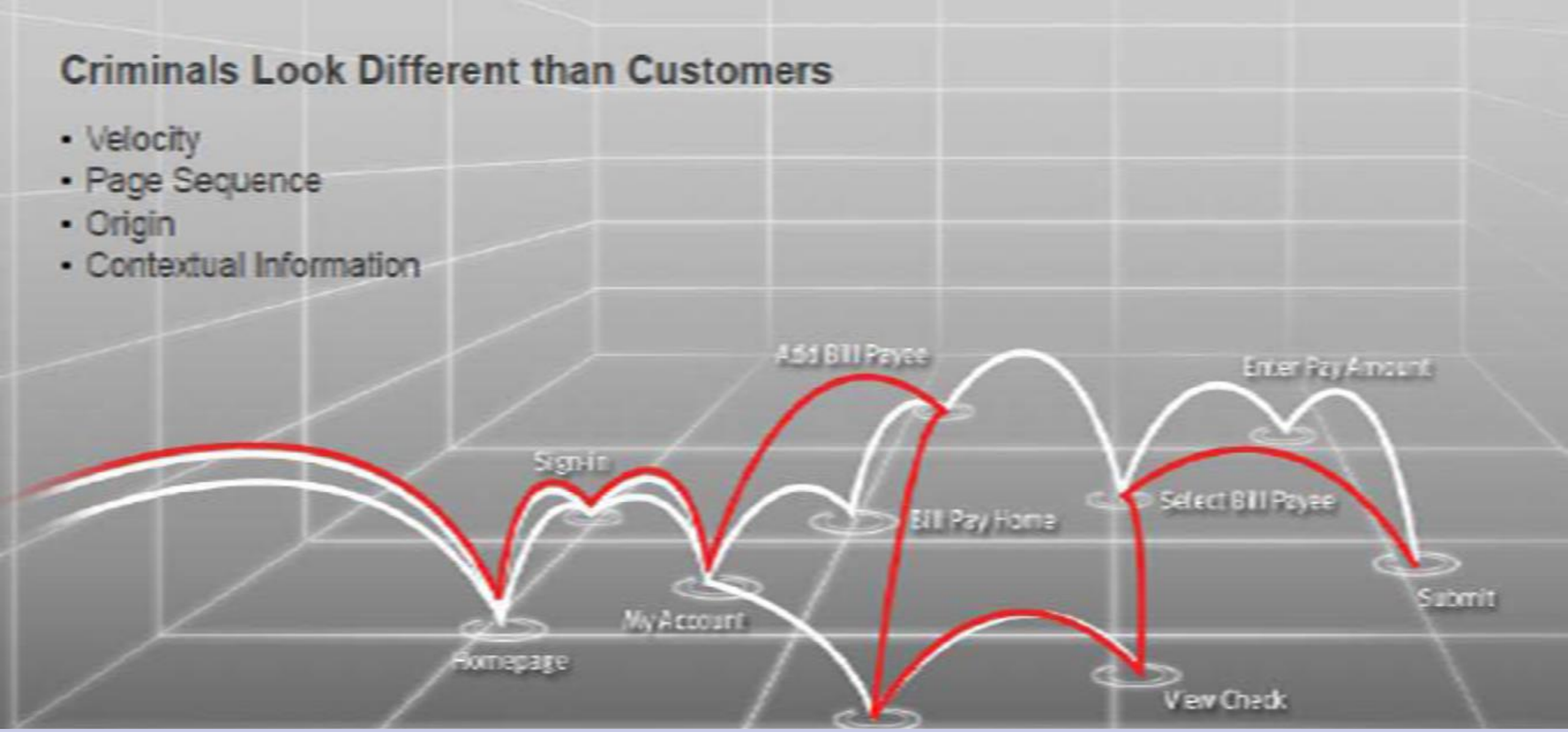

More
Important
Wisdom
Knowledge
Information
Data
Benefit to Humanity
Less
Important


隐性
体验
智慧
学习
知识
信息
规范
数据
显性

不同的视角，相同的本质



情报/知识来源于深度分析



情报/知识来源于持续、深刻的观察

情报/知识来源于多维、多路（带内外）

挑战：来源够多吗？视野够大吗？

挑战：能力够强吗？

挑战：用得上吗？

挑战：等得急吗？

挑战：（*be your own police*）做得到吗？

总结：都讲了些什么

- 为什么转而讲安全威胁、解决什么问题
- 什么是威胁情报、威胁情报的来源
- 威胁情报分析与威胁应对的主要挑战

我们缘何来到这里？我们要到哪里去？

ONE MORE THING：我们追求的目标

感谢您的关注！

Thank you for your attention