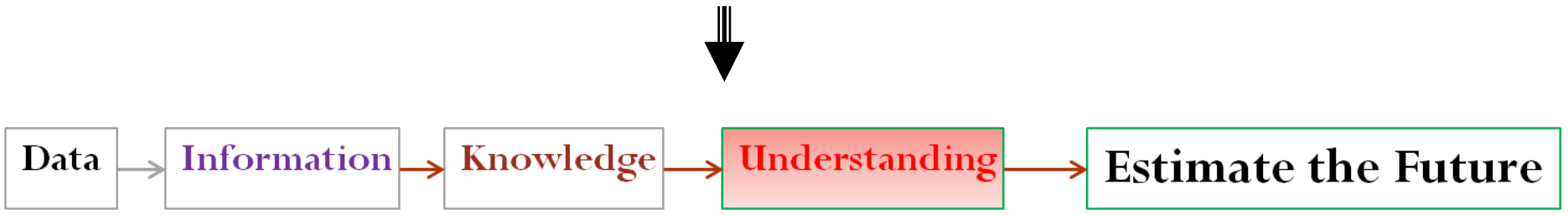
网络的安全态势感知

龚俭
东南大学计算机科学与工程学院
2013.10.15

Situation Awareness-认知过程

- 态势感知是在特定的时间和空间下，对环境中各元素或对象的觉察（L1）、理解（L2）以及对未来状态的预测（L3）。
  - 觉察：数据收集 -> 理解：对象行为及相互影响 -> 预测：基于规则的信息映射
  - a variety of cognitive processing activities



态势感知-决策支持 (Endsley)

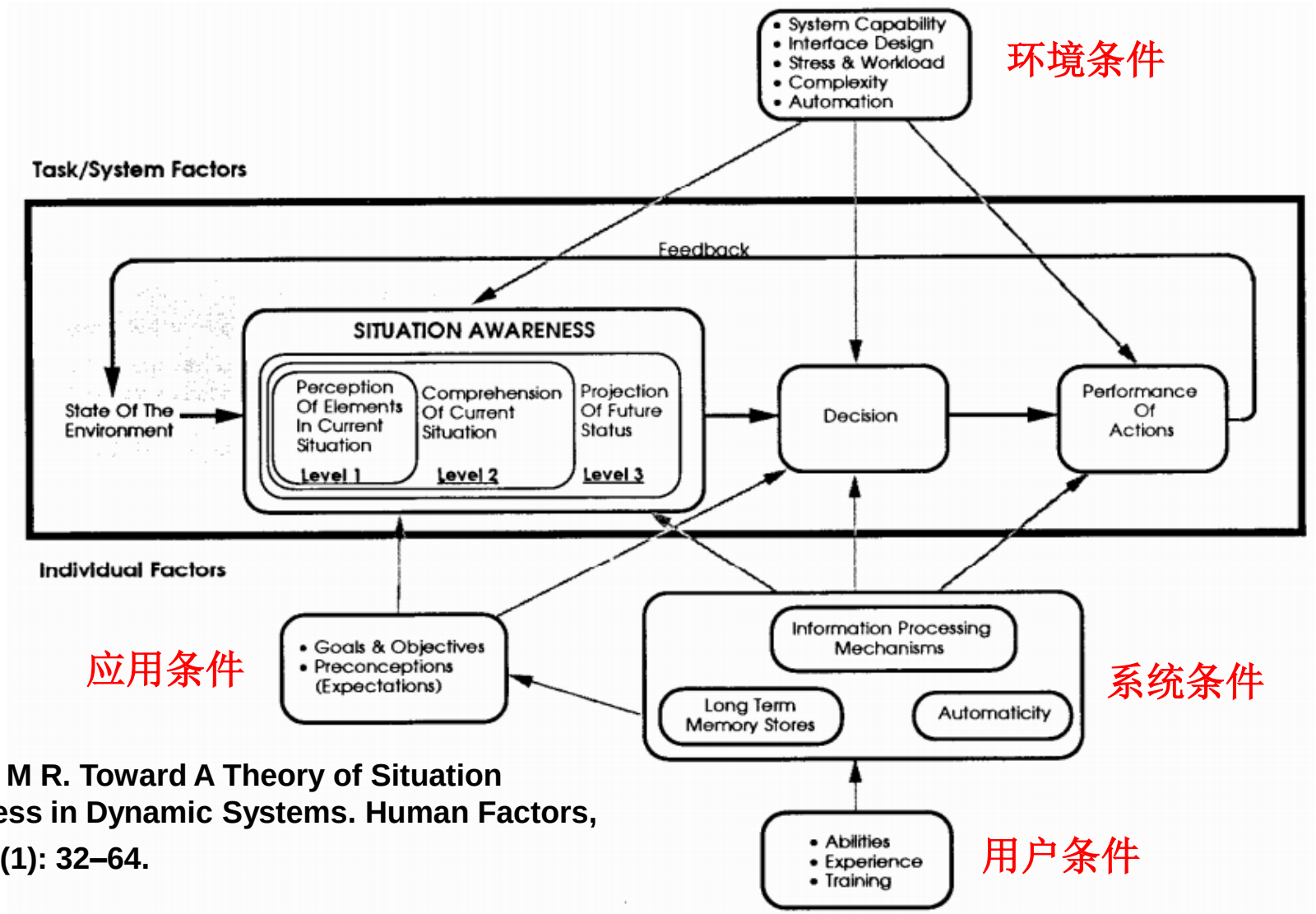


Figure 1. *Model of situation awareness in dynamic decision making.*

Endsley M R. Toward A Theory of Situation Awareness in Dynamic Systems. Human Factors, 1995, 37(1): 32–64.

态势感知在网络安全中的应用

- 美国空军通信与信息中心的**Tim Bass**在**1999**年首次提出将态势感知技术应用于多个**NIDS**检测结果的数据融合分析

Hierarchy of IDS Data Fusion Inferences	
Types of Inference	**Level of Inference**
- Threat Analysis	HIGH
- Situation Assessment	
- Behavior of Intruder	MEDIUM
- Identity of Intruder	
- Rate of Intrusion	
- Existance of Intrusion	LOW

Bass, T., *Intrusion Detection Systems and Multisensor Data Fusion: Creating Cyberspace Situational Awareness.* Communications of the ACM, 1999. **43**(4): p. 99-105.

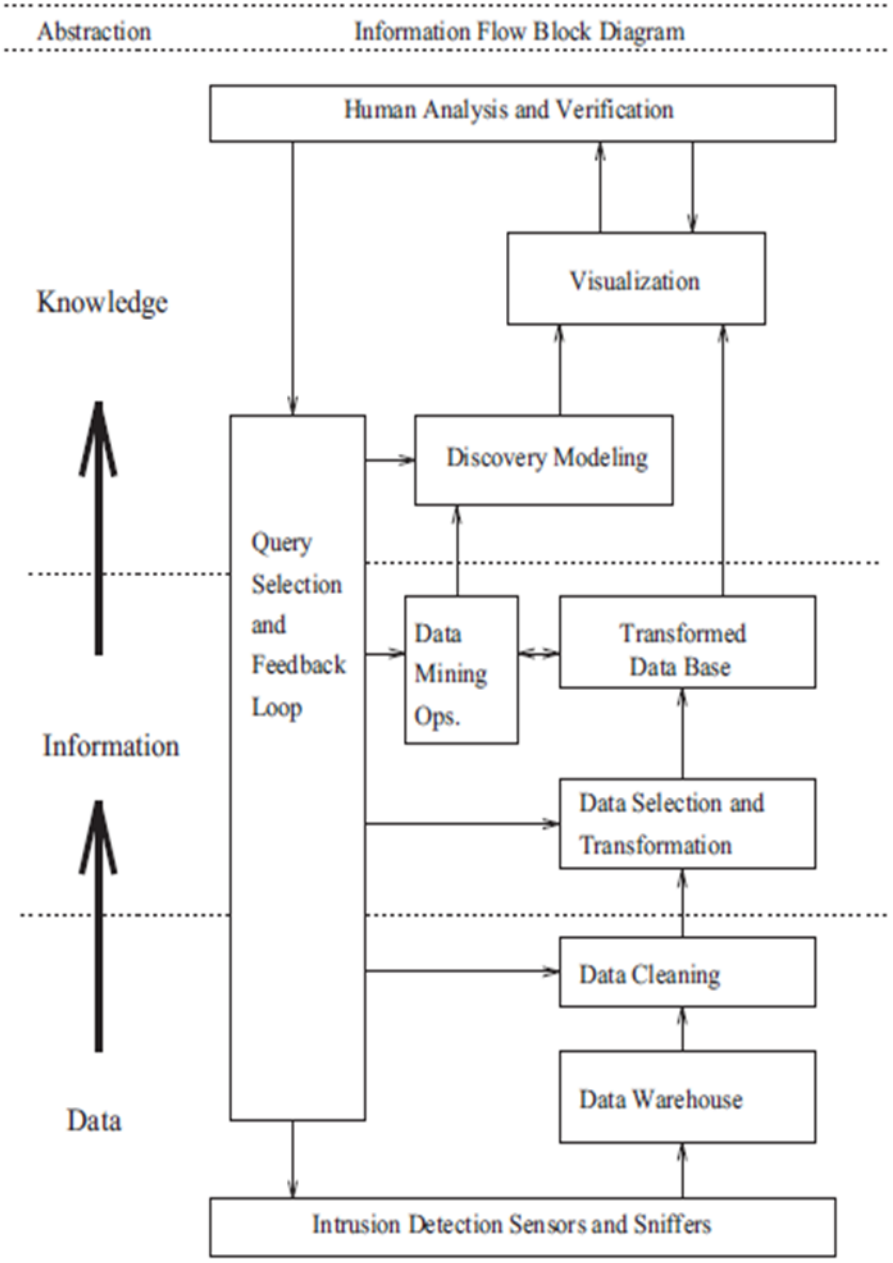


Fig. 3. Intrusion Detection Data Mining

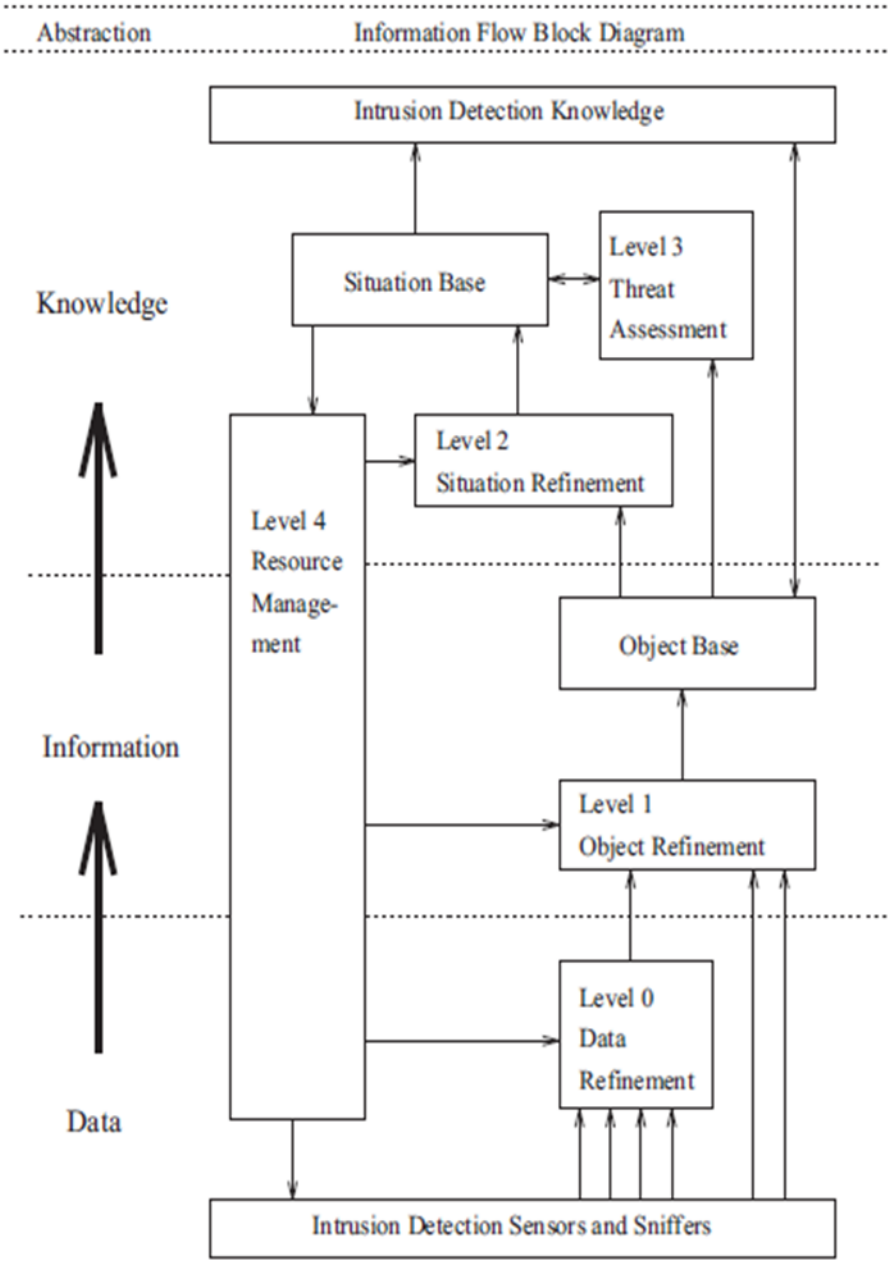
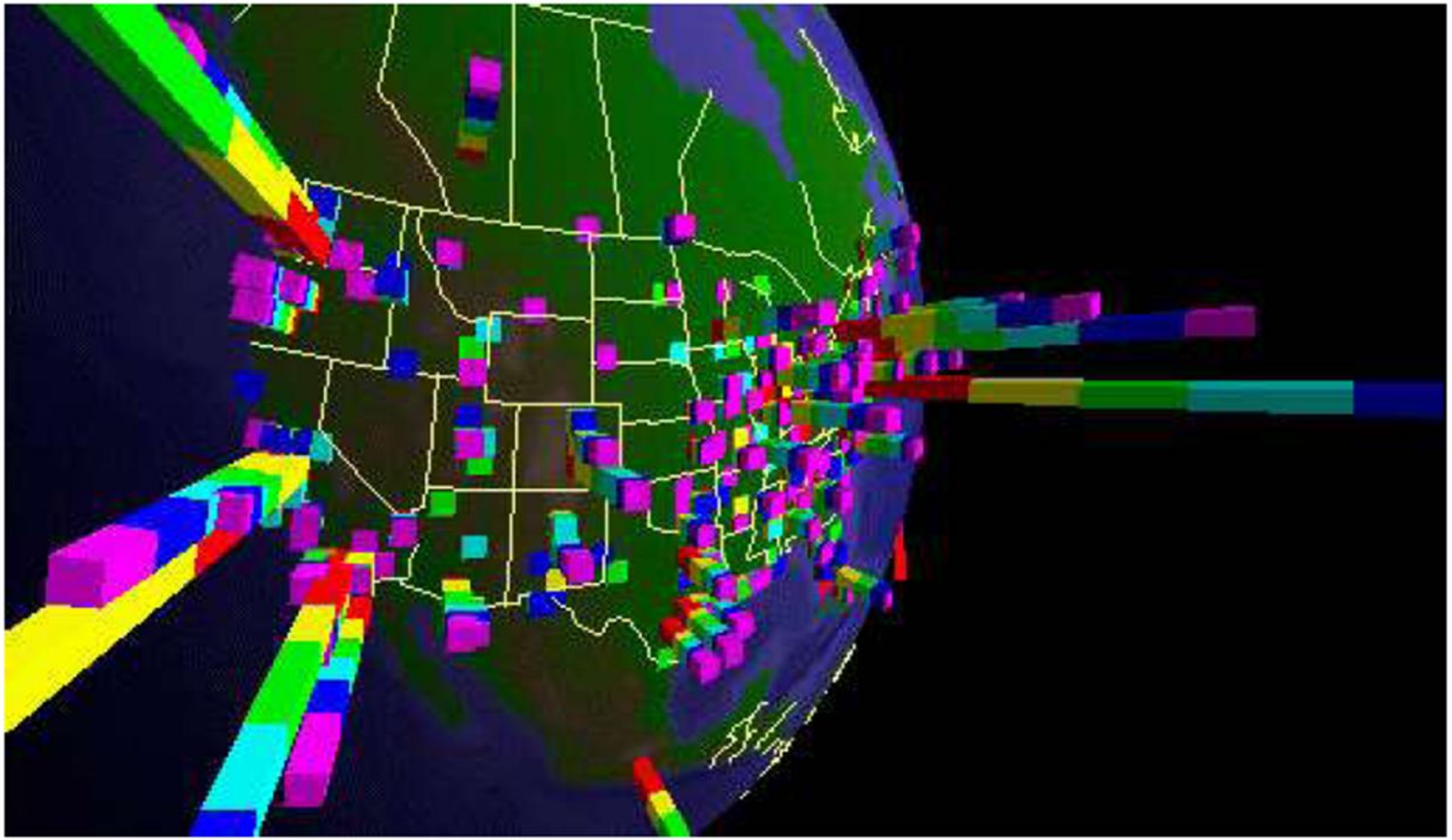


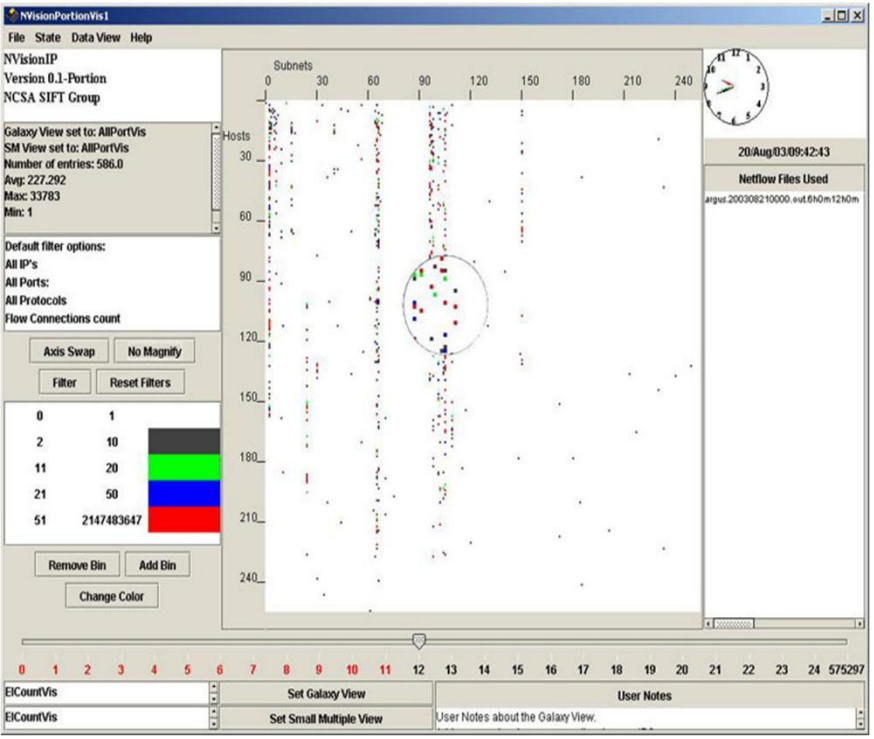
Fig. 2. Intrusion Detection Data Fusion

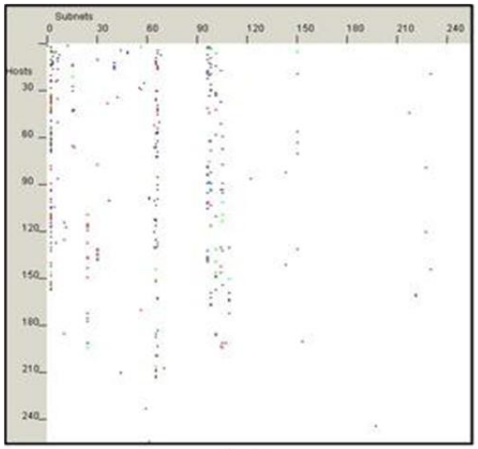


The real-time geographic visualization of World Wide Web Traffic, designed by Stephen E. Lamm and Daniel A. Reed of the University of Illinois-Urbana-Champaign and Will H. Scullin of Netscape Communications Corporation, is an example of the fusion of geographic space and network traffic parameters and characteristics. Data Bar with data bars represent attributes such as document type, Internet domains, services or time delays.

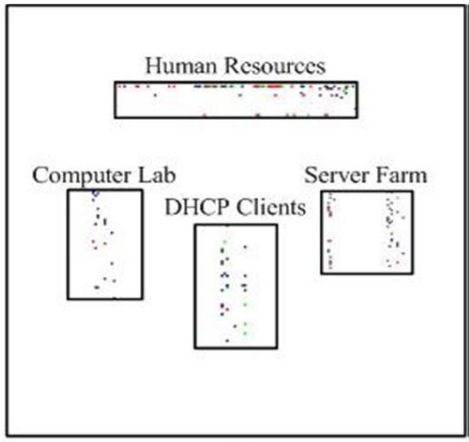
基于流记录的内容，将一个B类地址的流量情况集中展现。

2004: NVisionIP

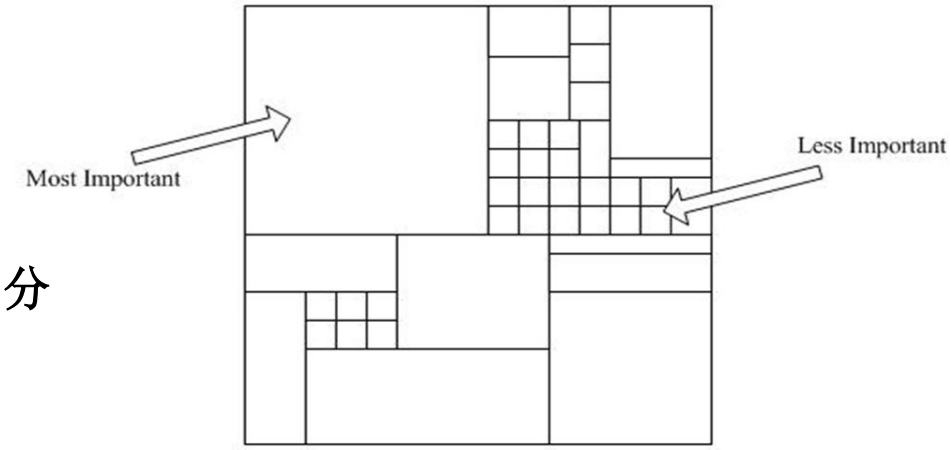




(a)



(b)



(c)

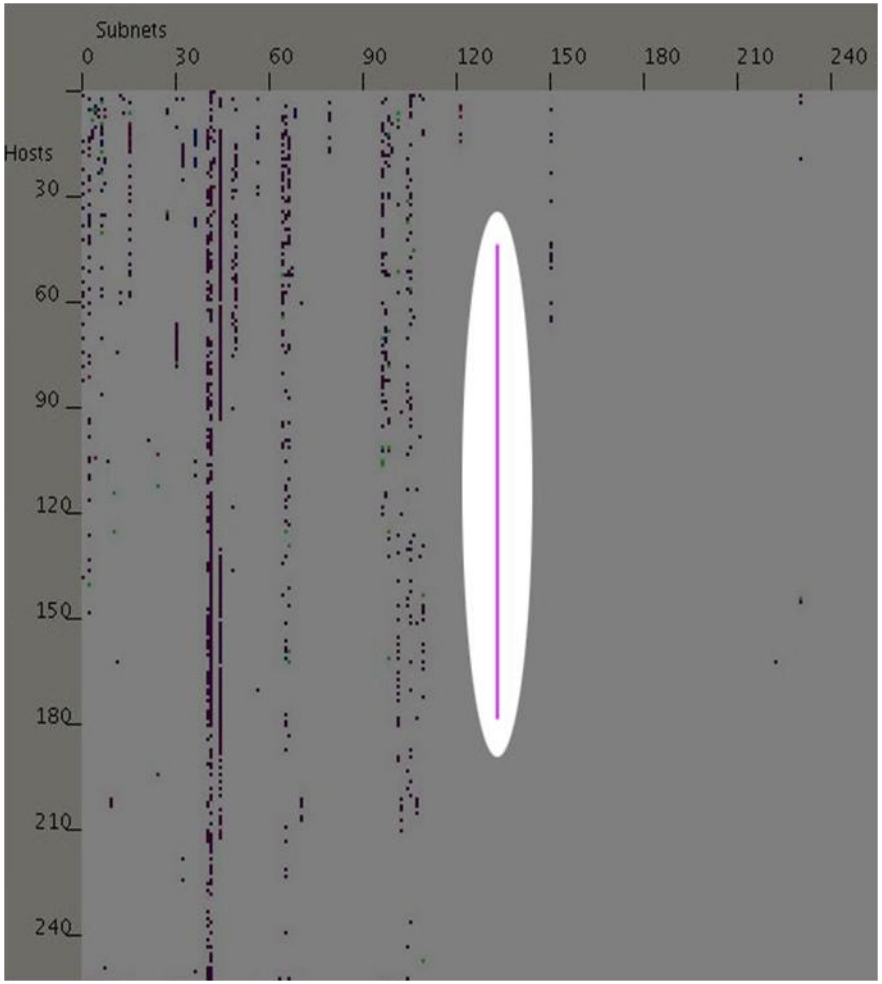
(a) 按主机在子网中的分布作图，用颜色区分它们的流量特性。

(b) 用同样的着色机制显示不同的网络簇。

(c) 主机用不同大小的方盒表示，越大越重要。

2004: NVisionIP

- **Worm Infection**
  - 依赖于对蠕虫网络流量特征的了解
- **Compromised Systems**
  - 如果发现主机参与DDoS攻击
- **Misuse**
  - 通过观察异常的大流量
- **Port Scans**
  - 观察异常的通信关系，尤其是密集的通信关系。
- **Denial of Service Attacks**
  - 通过对异常的高层协议流量的观察



More Works

- **2006: Study of Network Security Situation Awareness Model Based on Simple Additive Weight and Grey Theory**
- **2007: Multiclass Support Vector Machines Theory and Its Data Fusion Application in Network Security Situation Awareness**
- **2010: Employing Honeynets For Network Situational Awareness** ***2006***
- **2011: Situation Awareness for Networked Systems** ***SCADA、僵尸网络***
- **2012: Research of Network Security Situational Assessment Quantization Based on Mobile Agent**

Holsopple J, Sudit M, Nusinov M, Liu DF, Du H, Yang SJ. Enhancing Situation Awareness via Automated Situation Assessment. IEEE Communications Magazine 2010;48:146-52

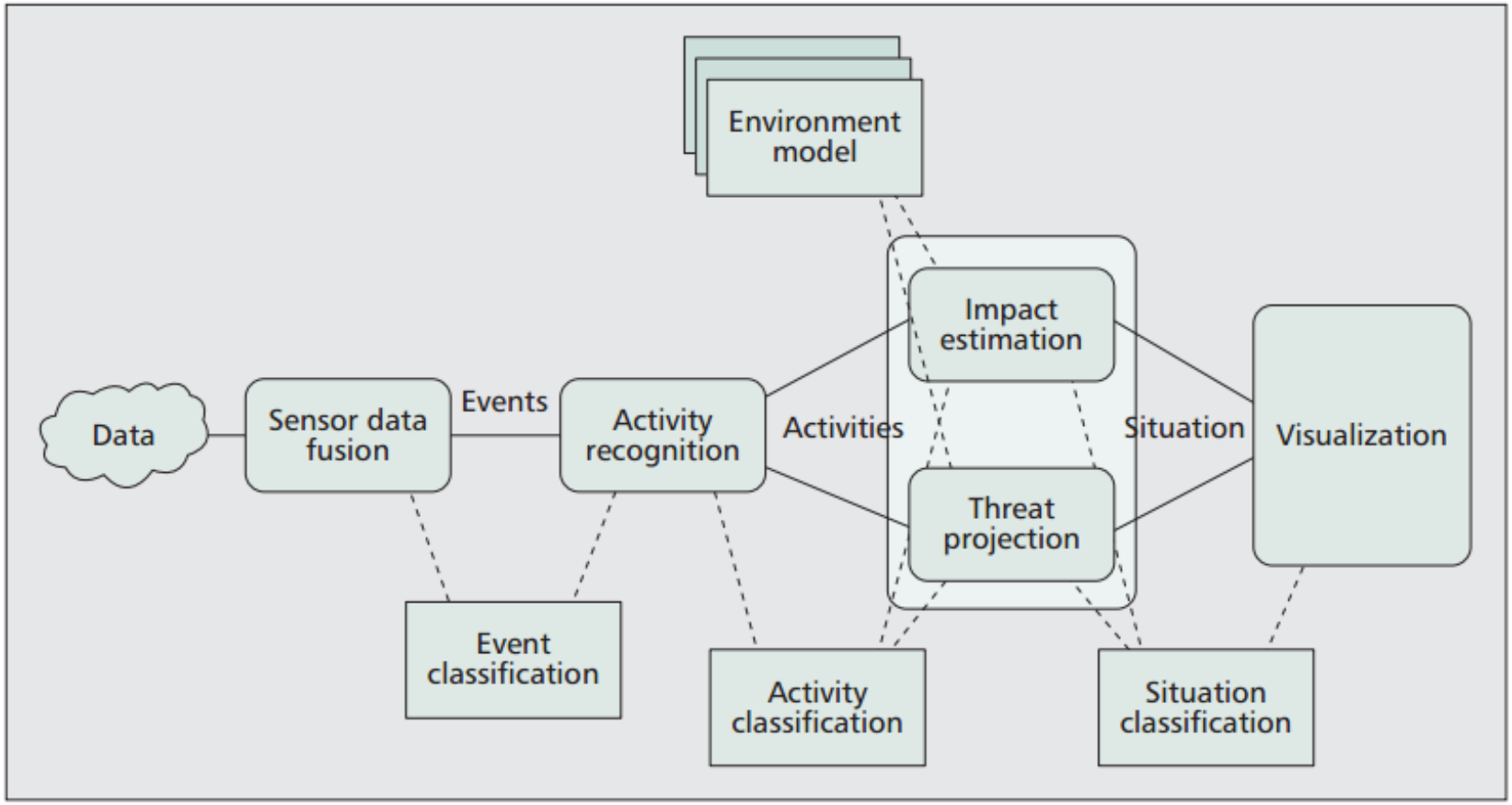


Figure 1. *The supporting elements of situation assessment.*

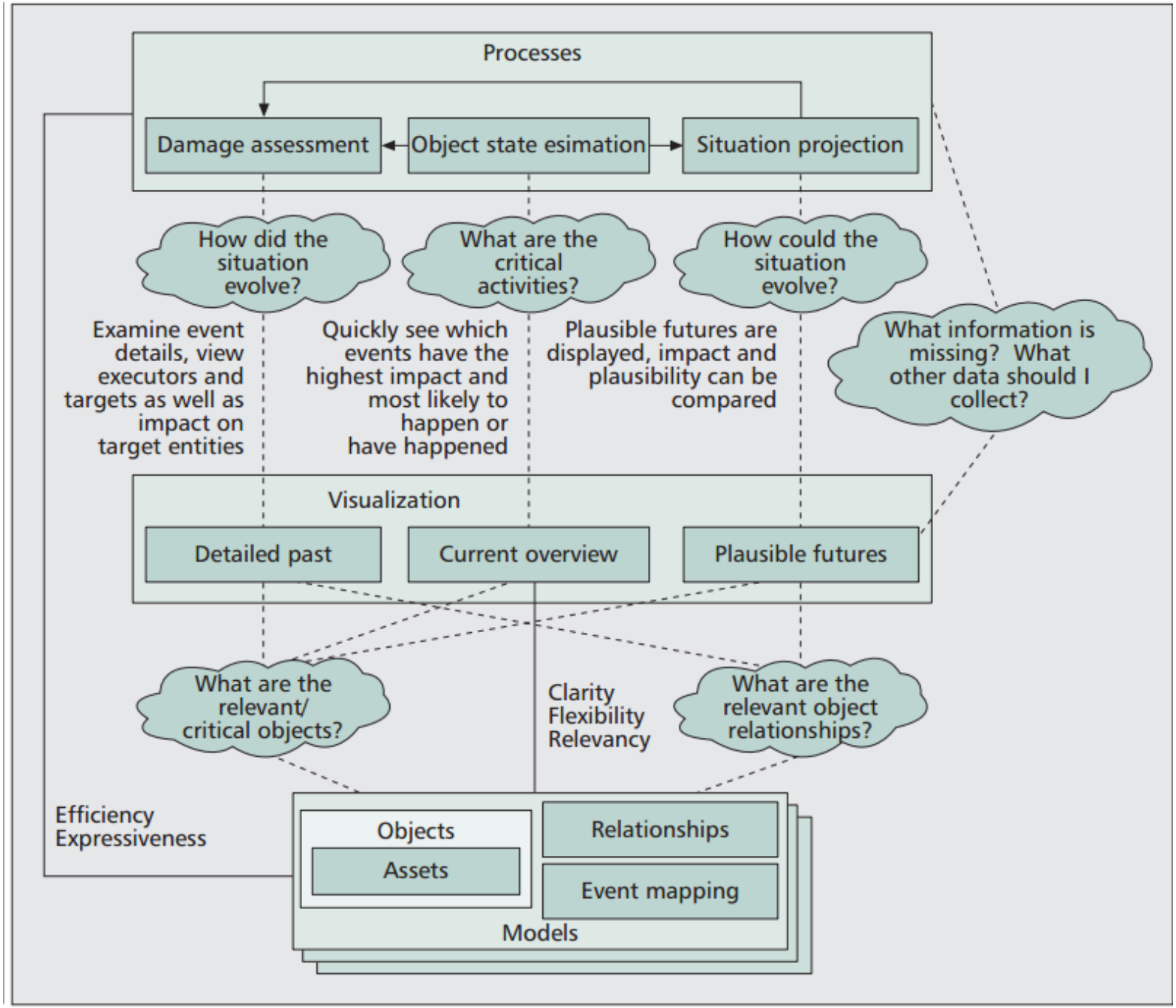


Figure 3. *Human-centered situation assessment.*

风险评估 (威胁和影响评估) 方法

Threat projection algorithms		Event-based	Environment-based	
		VLMM [11]	Statistical inference	Ontology/graph model [12]
	Learning	Unsupervised	Unsupervised	N/A
	Analysis perspective	Sequential causal relationship exhibits **behavior patterns**	Nonsequential casual relationship reveals adversary **capability**	Accessible objects identified to determine adversary **opportunity**
	Memory complexity	$O\left(\frac{t \cdot n(n+1)}{2}\right)$	$O(t \cdot v)$	$O(t \cdot v)$
	Computational complexity	$O\left(\frac{n(n+1)}{2}\right)$	$O(t + n + v)$	$O(v)$
	Scalability	Limited without optimization	Linear	Linear

t: number of activities *n*: number of events in an activity *v*: number of objects in an environment

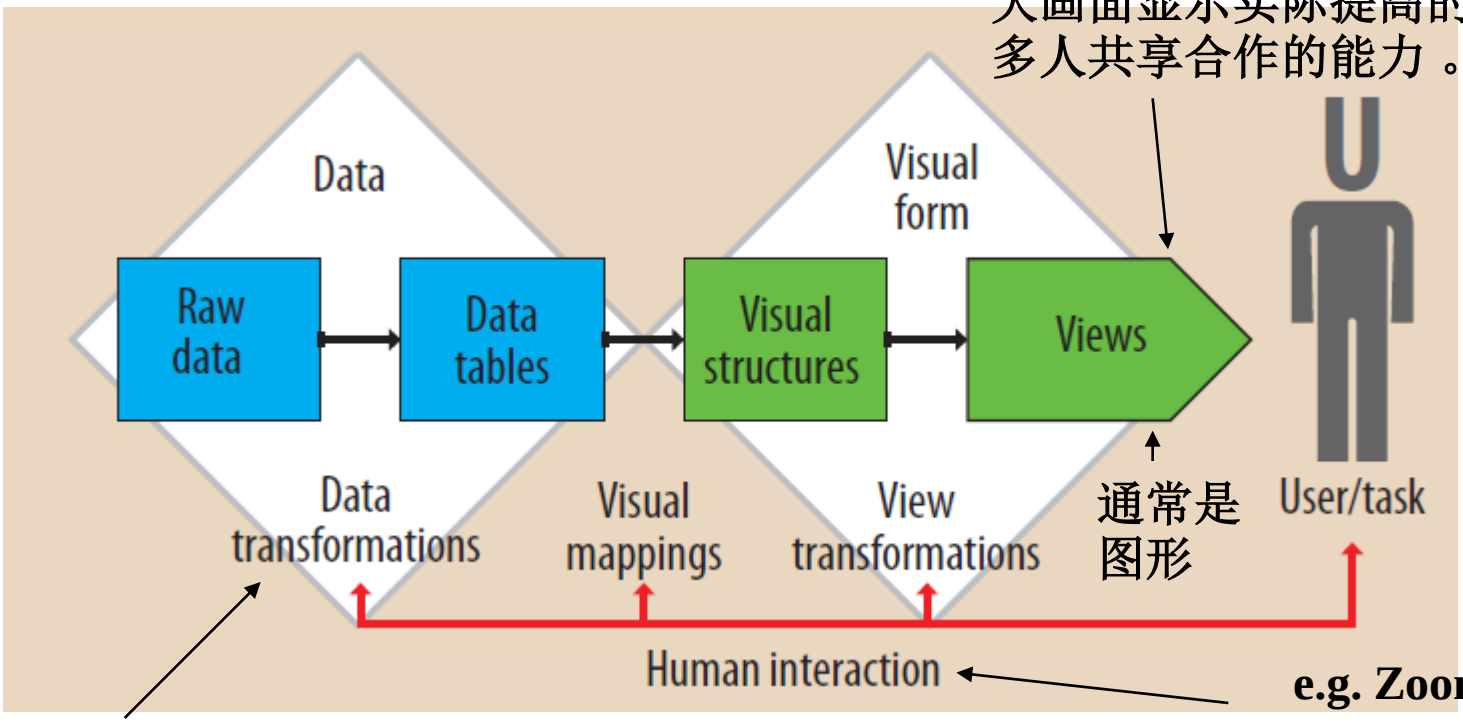
Table 1. *Threat projection works that analyze adversary activities from specific perspectives.*

VLMM：variable length Markov model，通过因果关系分析行为模式
Statistical Inference：通过事件统计，揭示对手的能力；
Ontology/graph model：本体论模型，考察“暴露给对手的弱点”

威胁评估的**3**个方面：
意图、能力、机会

信息可视化的抽象参考模型

由于人的知觉能力限制，大画面显示实际提高的是多人共享合作的能力 。



通常是图形

e.g. Zooming and Panning

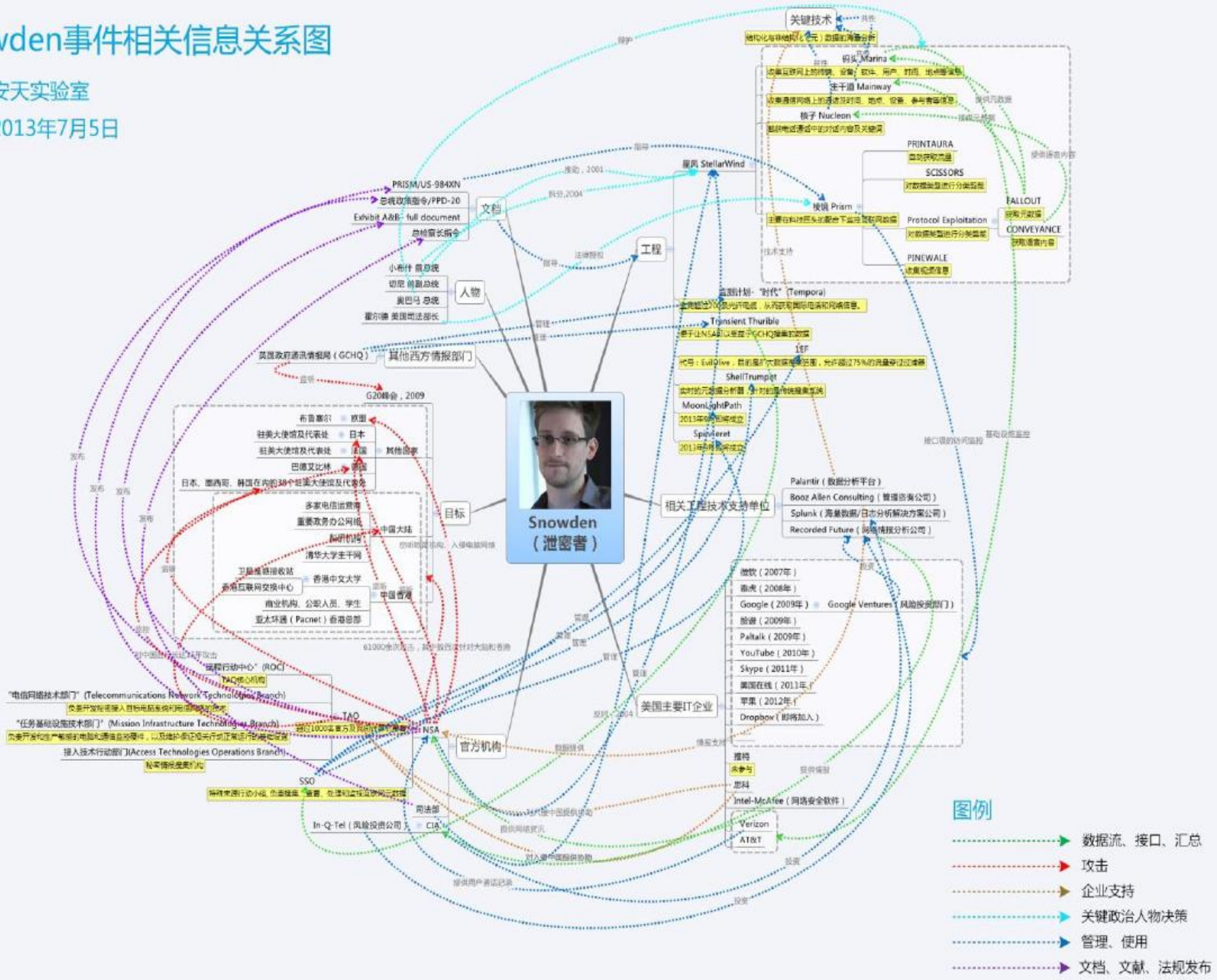
出于性能考虑，通常需要在内存中建立独特的数据（库）存储结构，缺乏标准化，不利于第三方组件的加入，需要在接口上进行数据结构转换。

Jean-Daniel Fekete. Visual Analytics Infrastructures: From Data Management to Exploration. IEEE Computer Magazine, Vol.46 No.7, pp22-29, 2013.7

Snowden事件相关信息关系图

绘制：安天实验室

更新：2013年7月5日

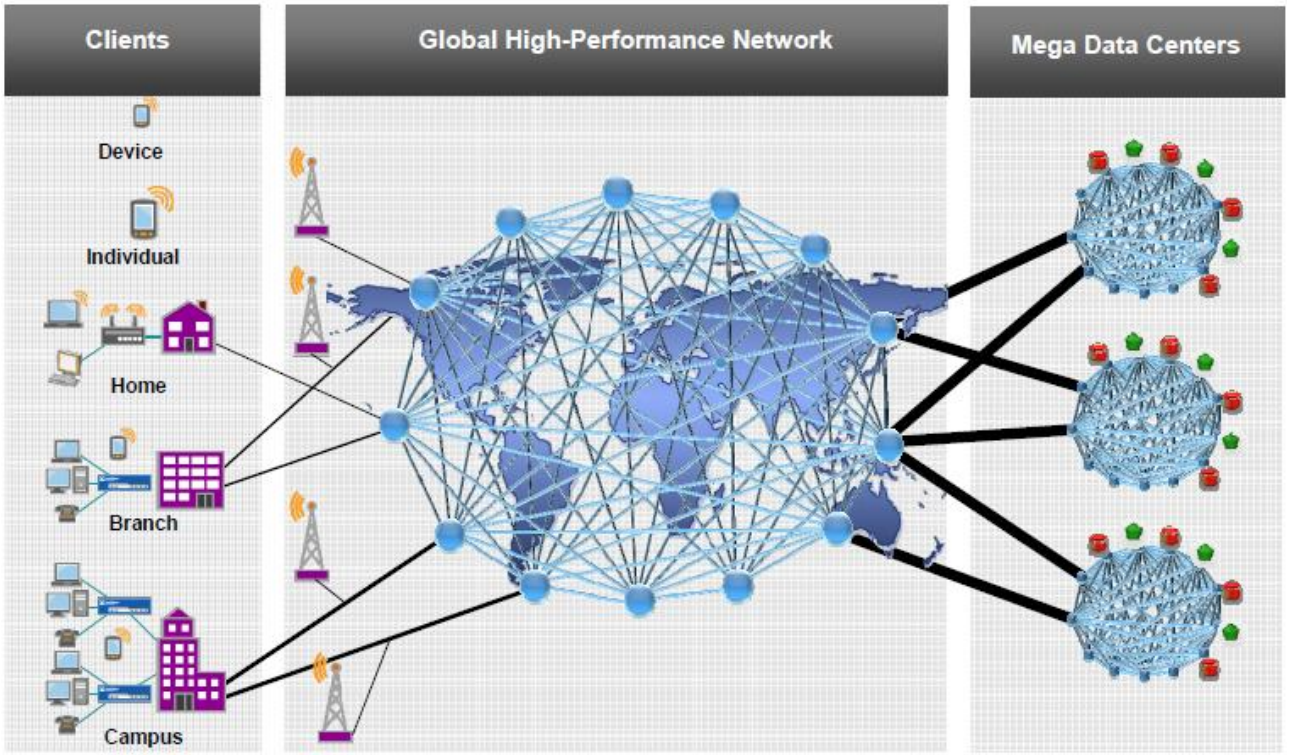


研究内容

- 与被管网络相关IP地址和域名的辨识 *对象*
  - 管理归属信息 Objects / Assets
  - 使用位置信息
  - 承载服务的角色信息
- 被管网络中IP地址和域名的行为语义 *行为*
  - 对象的行为模型：时间、空间
  - 对象的行为分类：语义、异常
  - 对象的行为关联性：活动的语义
- 被管网络的威胁评估与响应 *态势*

观察点的选择

- 主流的流量模式是什么？
- 非主流的流量模式非正常的吗？



面临的问题-数据

- 相关数据的获取与管理
  - 类大数据问题：**Volume**、**Variety**、**Velocity**，弱语义
    - 收集什么，保存多久，抽样方法，隐私与安全
  - 高性能问题：万兆网络和多处理器环境
    - 非标准内存数据库
- 观测对象选择
  - 热点对象
  - 黑名单
  - 安全事件
  - 活跃对象
  - 元数据：流记录、IP报文、IP地址、域名、URL

面临的问题-对象

- 对象的标识
  - 机器域名的检测
  - IP的前缀识别
  - IP的角色分类
  - 域名与IP的关联
- 对象的物理/逻辑定位
  - IP的地理定位
  - 域名的归属
- 对象的行为轨迹模型与分类
  - 空间关联性
  - 时间关联性
  - 服务关联性
- 对象行为轨迹的可视化方法

面临的问题-行为语义

- 恶意服务检测
  - 僵尸网络的活动
  - 恶意服务活动
  - 信息泄露
- 流量异常检测
  - **DDoS**
  - 热点与奇异点
    - 流量聚类问题
- 入侵检测
  - 后门及其活动
  - 恶意代码及其活动
- 协议分类
  - 服务识别
- **基于流记录和DPI**

面临的问题-威胁

- 活动识别：网络流量的意图
  - 行为语义
  - 异常检测
  - 跟踪
- 威胁的描述
  - 用哪些测度描述
  - 如何描述：形式化、可视化
- 威胁评估的量化模型
  - 恶意服务/威胁的规模测量
  - 恶意服务/威胁的动态行为模型

小结

- 基于对象活动的网络安全态势感知及其表示
  - 洞察**insight**是：复杂的，涉及大量的协作数据；会随时间的推移而深化的；量化的、客观的、非精确和不确定的；其获得是不可预期的、不可预测的、侥幸的；与特定领域的知识有密切相关的联系。
  - 理论模型：需要先明确输入和目标
- 可视化分析　　先由人来做
  - 支持数据探索 **(exploration)**：快速获得尝试性结果
  - 恶意服务/威胁的可视化
    - 大规模图的可视化：考虑知觉能力的限制

谢谢！