北人南顾：攻击假设矩阵中的数据纽带

潘柱廷

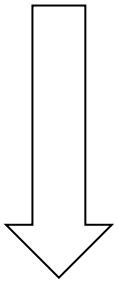
启明星辰　首席战略官

中国计算机学会　常务理事

北纬６６３４　发起人

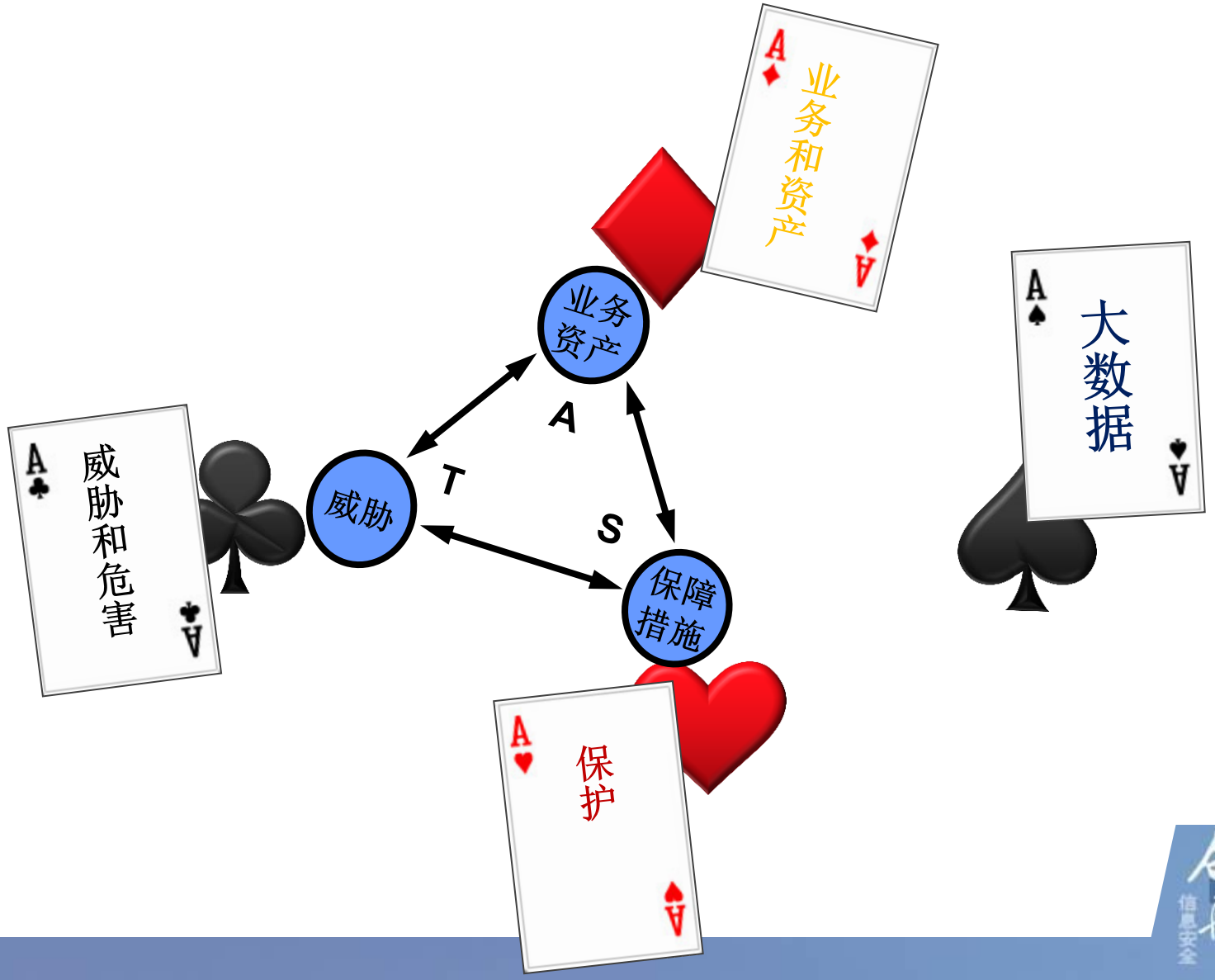
南人怎么看技术

看关系
看结构
看技术的关系
看技术的结构
看技术的过程
看技术的货币面
…




涉密
办公安全
网上银行
骨干网
网站安全
ERP
服务器
核心业务
终端安全
文档安全
业务连续性
卫星通讯
业务大集中
数据中心
病毒/蠕虫
拒绝服务攻击
火灾/水灾
设备故障
内部人员作案
网络渗透
误操作
垃圾信
安全事件
漏洞
线路中断
加密
强认证
防火墙
入侵检测
攻击检测
渗透测试
UTM
多功能网关
审计
管理平台
风险评估
等级保护
监控/预警
冗余/备份
应急响应
专属安全官
安全专家
国家战略
组织体系
制度/规则
工作流
体系结构
规划/设计
大数据
项目管理
合规性要求
三观论
宏观/中观/微观
量化/指标化
合作/外包
管理理念

大数据•(业务,威胁,安全)



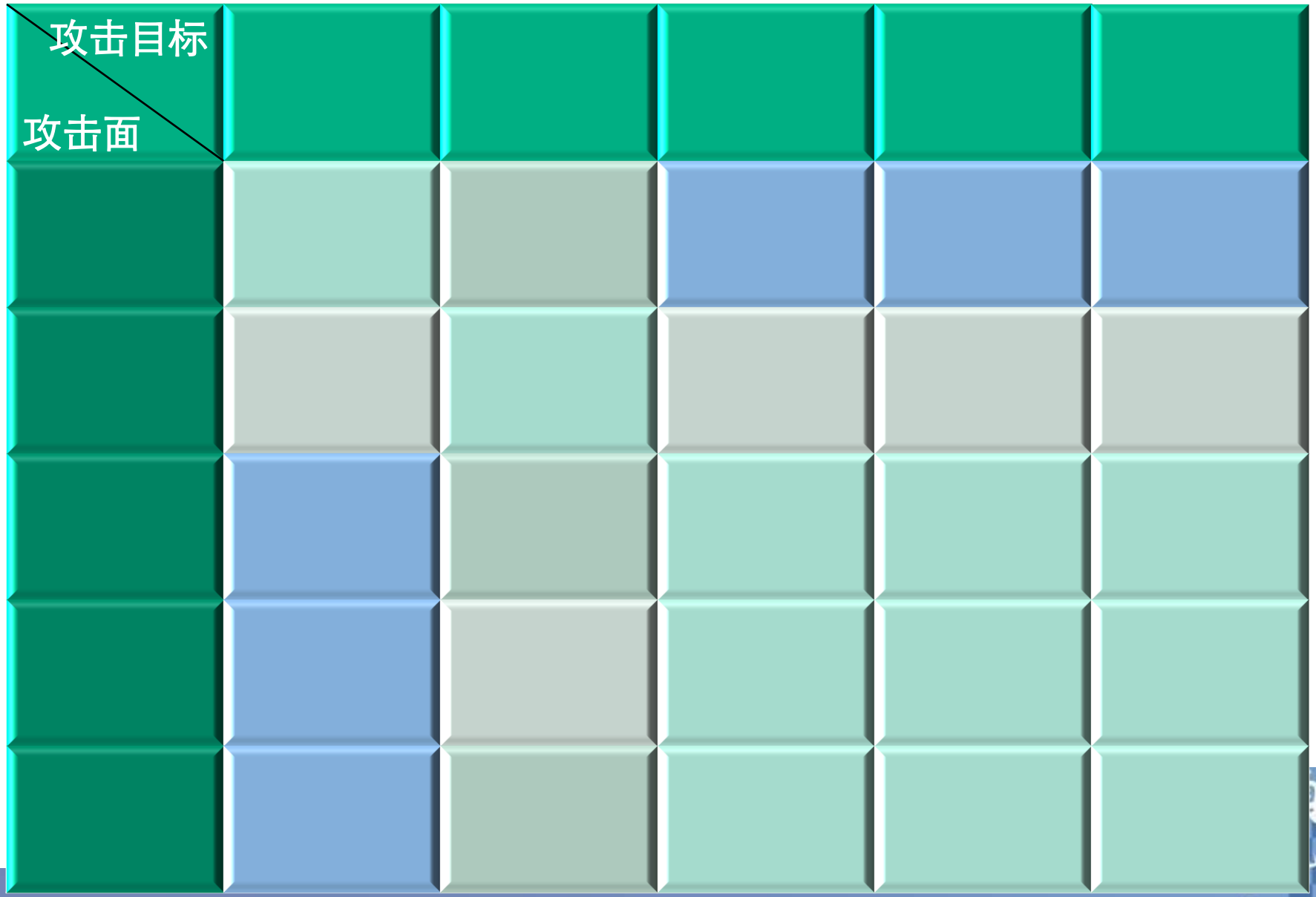
大数据安全九宫图

	业务	威胁	安全
大数据+安全		传统的安全威胁	网络安全大数据
		银行业务欺诈等威胁	银行反欺诈BD
大数据+威胁		**利用大数据分析攻击**	**数据隐藏**
		大数据侵犯隐私	大数据脱敏
大数据+业务	某种业务大数据	对于大数据的针对性攻击	保护大数据： 用传统的盒子组合
			保护大数据： 用大数据针对性模式

威胁用例、威胁场景

- **威胁的环境Environment：**
  - 前提、假设、条件等
- **威胁的来源Agent：**
  - 包括攻击者、误用者、故障源、自然（灾害）等，及其相关属性。
- **威胁的对象Object：**
  - 攻击目标和破坏对象，也就是要被保护的对象，及其相关属性。
- **威胁的内因**
  - 脆弱性Vulnerability：自身保护不当的地方
- **威胁的过程Process**
  - 威胁的途径Route：
    - 指威胁必须通过才能实现的一些部分。比如，通过网络、在物理上接近、欺骗人等等。
  - 威胁的时序Sequence：
    - 威胁要实现所必经的步骤和顺序。与威胁的途径是一个从空间上，一个从时间上表达。也可以将这两个因素结合起来表达威胁的过程。
  - 威胁的手法：
    - 威胁要实现所需要的手法。比如：通道劫持、暴力破解、欺骗等
- **威胁的结果——事件Event/Incident：**威胁具体实现之后所造成的结果
  - 威胁的可能性：威胁产生结果变成事件的概率。
  - 威胁的影响范围：威胁产生结果后的影响大小。以及影响进一步扩散的特性。

攻击假设矩阵，一个简单的工具



攻击假设矩阵

- **空间攻击假设矩阵**
  - 以网络拓扑空间位置为矩阵的边
- **时间攻击假设矩阵**
  - 以绝对时间为矩阵的边
  - 以时序步骤为矩阵的边
- **手法攻击假设矩阵**
  - 以手法和视角作为矩阵的边

防御效果矩阵

- **以各种攻击假设矩阵为底板，可以在上面点出防御措施的矩阵标注**
  - 也可以在空间、时间、手法上

攻击假设矩阵@网络拓扑，简单示例

攻击目标 / 攻击面	外网网关	核心网	终端区	运维区	服务器
外网网关					
核心网					
终端区					
运维区					
服务器					

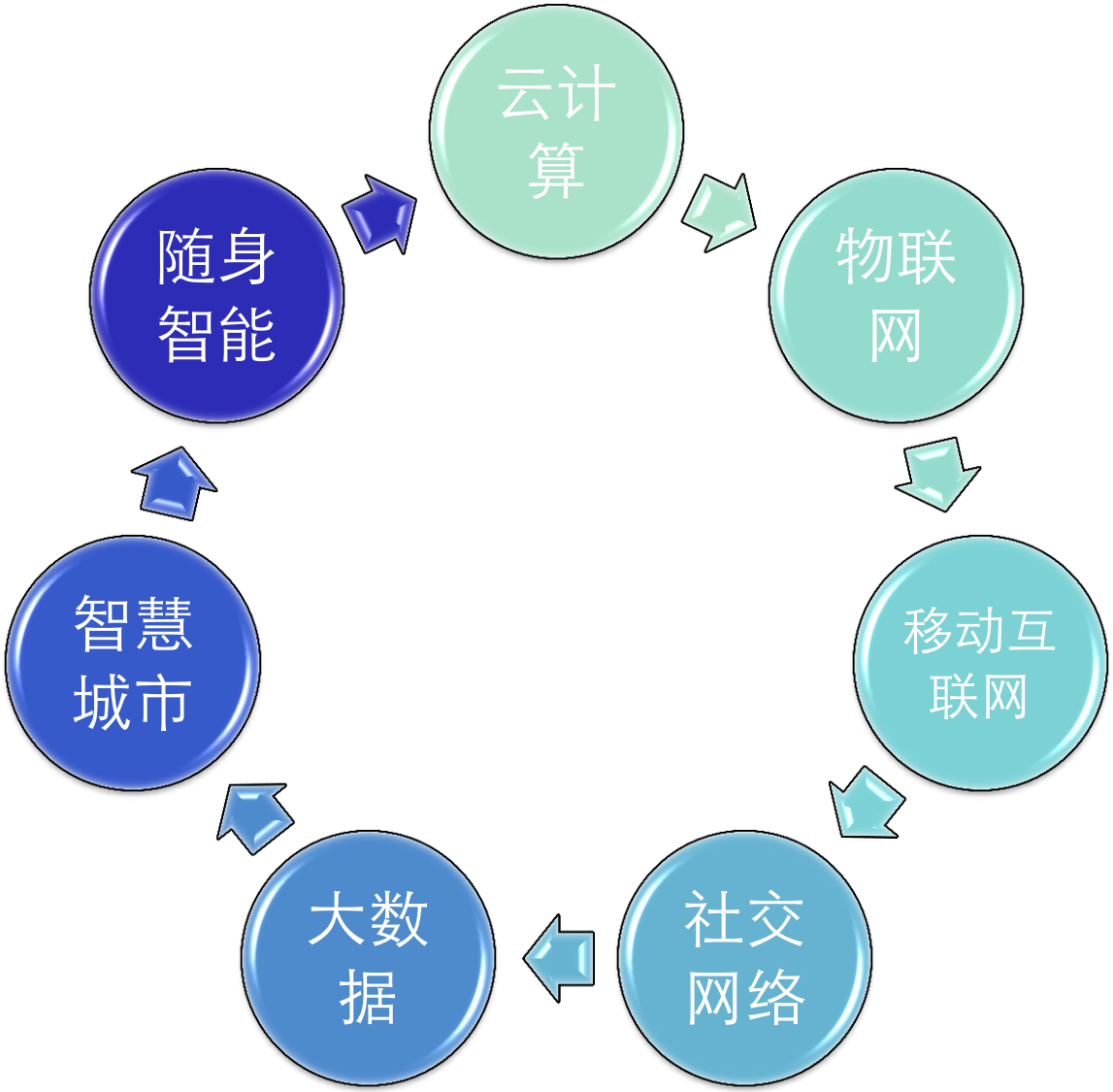
攻击假设矩阵@时间，简单示例

攻击目标 / 攻击面	再前	事前	事中	事后	再后
再前					
事前					
事中					
事后					
再后					

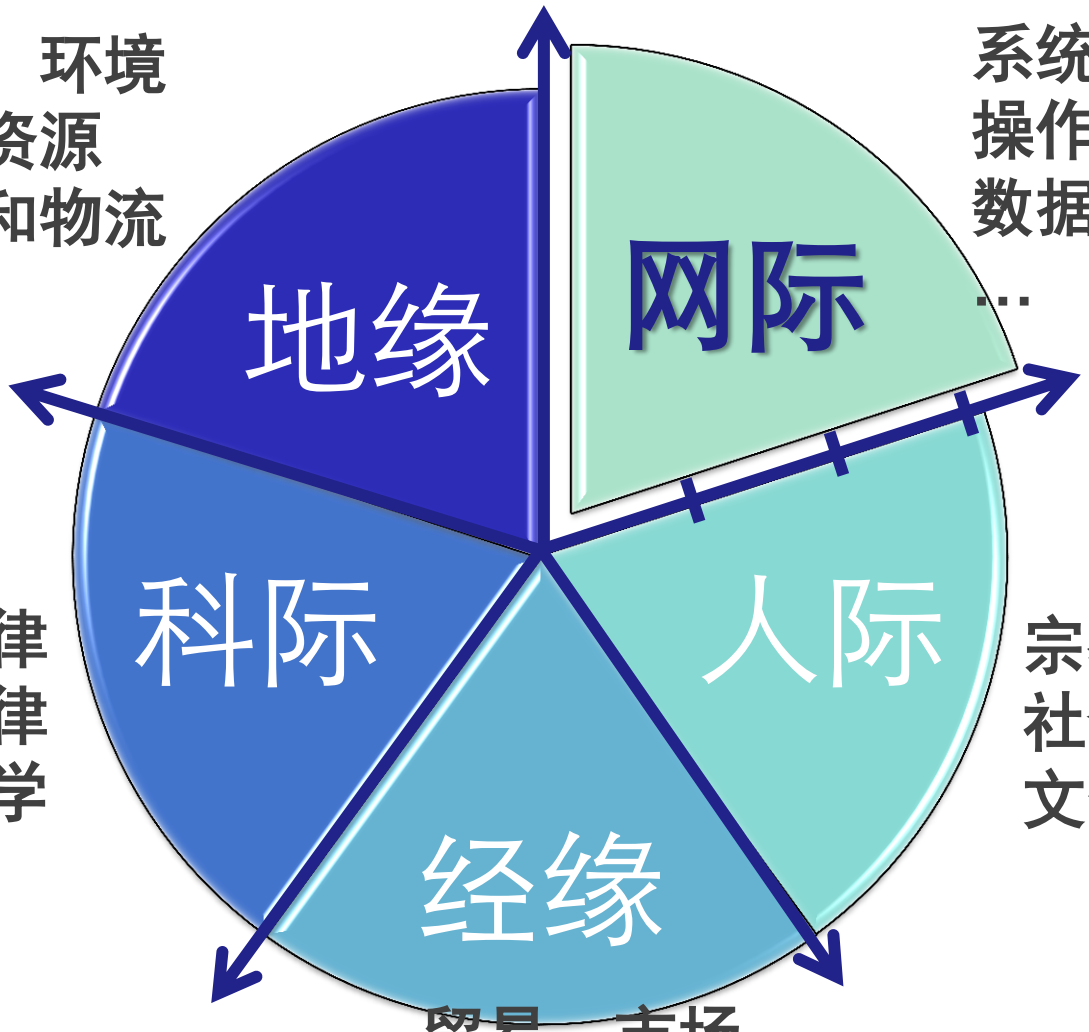
数据资产：一种新型资产的认识

- **数据资产**
  - 区别于实体资产
  - 区别于网络空间中的系统资产、服务资产（过程）
  - 数据本身、数据的所在(载体)
  - 数据本事、数据的语义(理解)、数据的价值
  - 源数据、元数据
  - …
- **数据和人**
- **数据的合法所属及其侵犯**
  - 5W1H
  - 价值驱动、价值评判

“云物移社大智随”的影响



五际缘的弈局



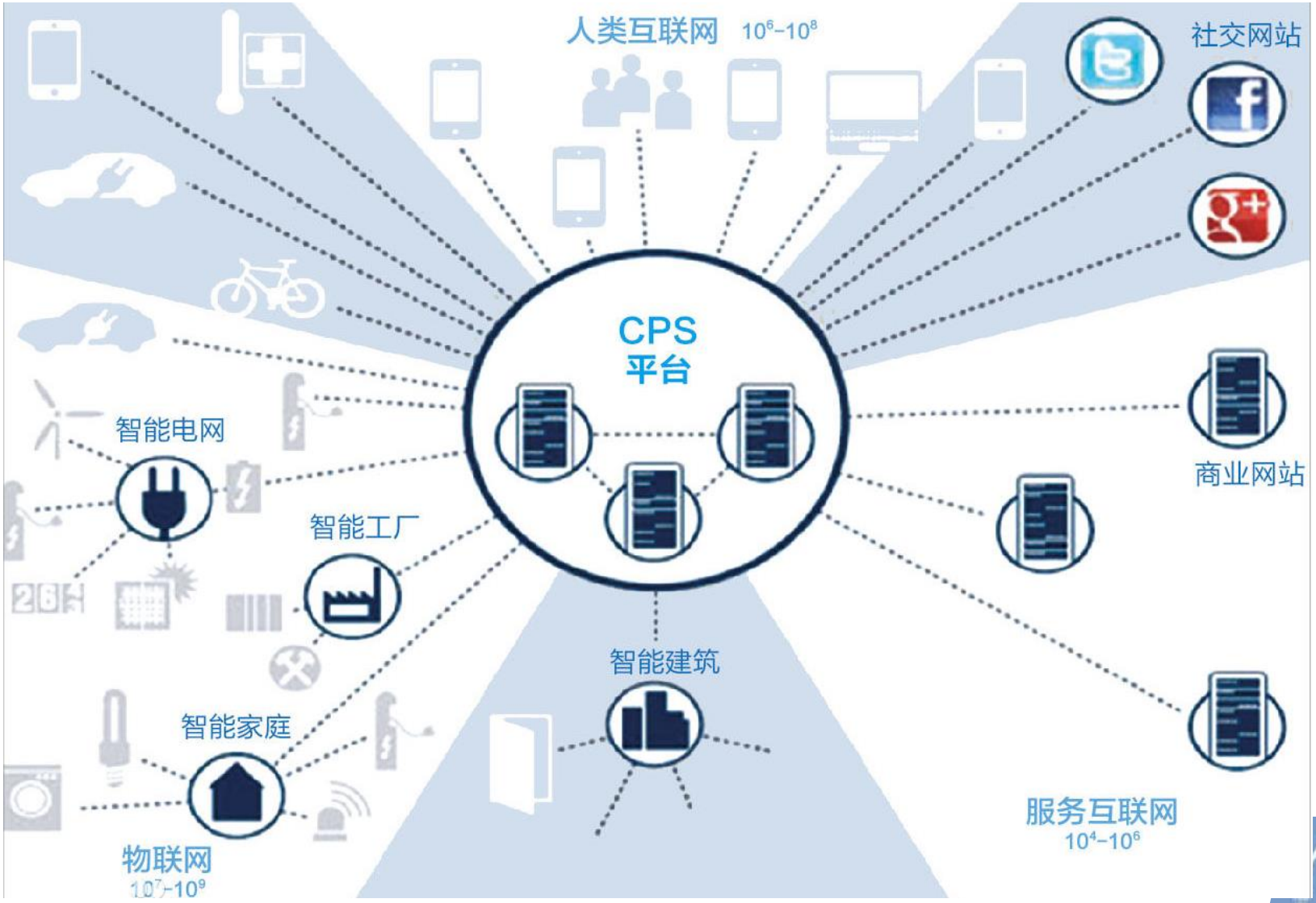
地理、环境
自然资源
交通和物流
制造
…

系统和网络
操作和服务
数据和内容
…

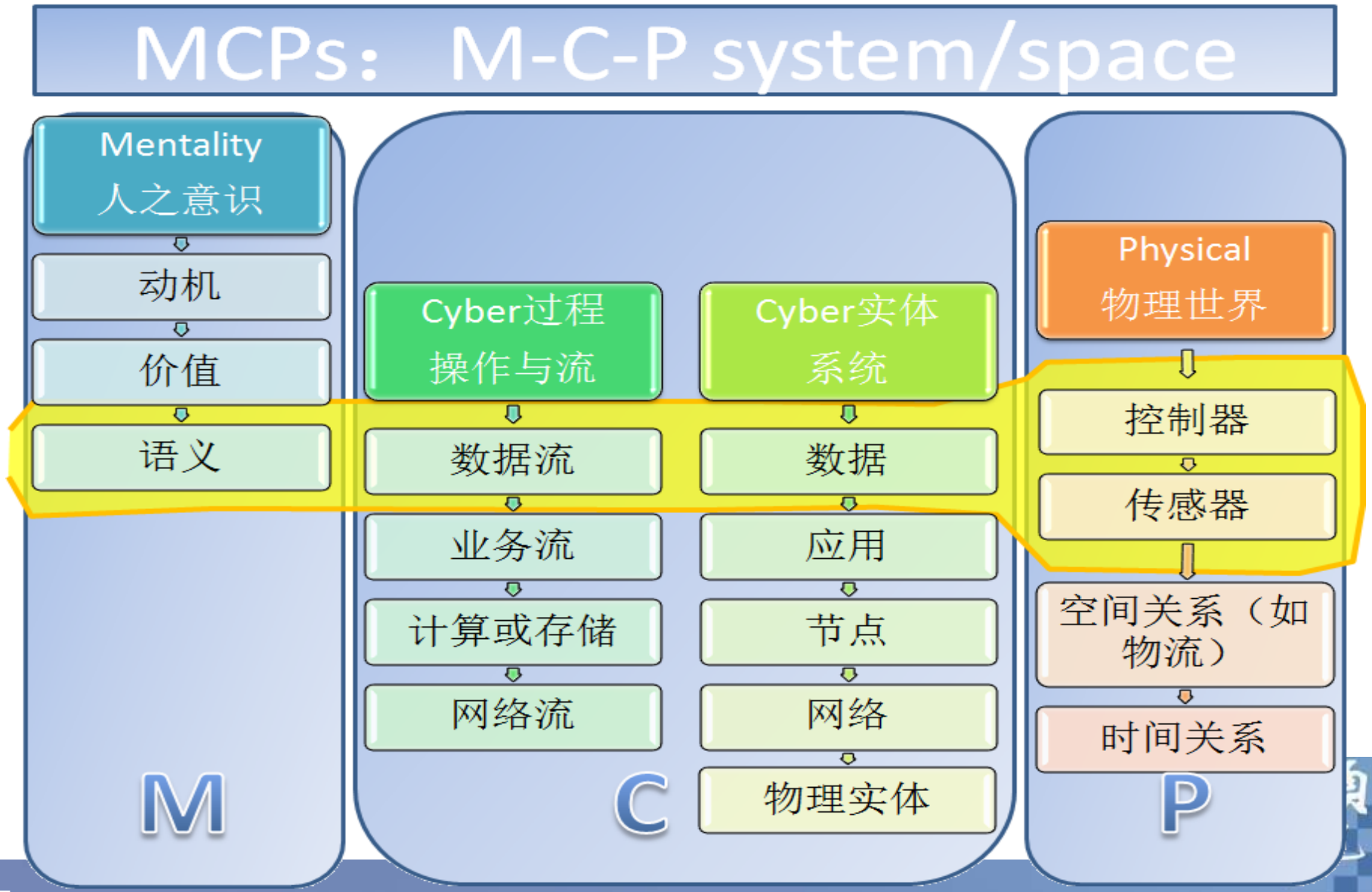
自然规律
数学规律
科学哲学
…

宗教、意识形态
社会组织、舆论
文化…

贸易、市场
金融、货币…


人类互联网 10^6–10^8
社交网站
CPS
平台
智能电网
智能工厂
商业网站
智能建筑
智能家庭
物联网
10^7–10^9
服务互联网
10^4–10^6

意识-信息-物理系统/空间


MCPs： M-C-P system/space
Mentality
人之意识
动机
价值
语义
M
Cyber过程
操作与流
数据流
业务流
计算或存储
网络流
Cyber实体
系统
数据
应用
节点
网络
物理实体
C
Physical
物理世界
控制器
传感器
空间关系（如物流）
时间关系
P

从MCPs攻击假设矩阵看“大数据攻击”

攻击目标 / 攻击面	Mantelity 意识空间	Cyber 网络空间	Physical 物理世界
Mantelity 意识空间	意识形态博弈	社会工程攻击 谣言冲击系统	某种理论影响经济走势
Cyber 网络空间	传说中的人工智能危机	网络和系统攻击	社交网络策动群体事件 系统故障扰动经济
Physical 物理世界	灾难对社会信心的打击	切断传感体系 破坏物理系统	物理破坏对抗 经济对抗

从MCPs攻击假设矩阵看“大数据攻击”

表1 MCPs攻击假设矩阵（14x14）

MCPs攻击假设矩阵（14x14）

	Mm	Mv	Ms	Cd	Cm	Ca	Cc	Cs	Cn	Cp	Pc	Ps	PS	PT
Mm						4.6								
Mv														
Ms														
Cd			4.5											
Cm											4.7			
Ca														
Cc							4.1							
Cs			4.5	4.4 4.5										
Cn					4.7		4.2		4.3		4.7			
Cp					4.8									
Pc														
Ps														
PS								4.8						
PT														

动机
价值
语义

数据
元数据
应用
计算
存储

网络
设备

控制
传感
空间
时间

威胁用例、威胁场景

- **威胁的环境Environment：**
  - 前提、假设、条件等
- **威胁的来源Agent：**
  - 包括攻击者、误用者、故障源、自然（灾害）等，及其相关属性。
- **威胁的对象Object：**
  - 攻击目标和破坏对象，也就是要被保护的对象，及其相关属性。
- **威胁的内因**
  - 脆弱性Vulnerability：自身保护不当的地方
- **威胁的过程Process**
  - 威胁的途径Route：
    - 指威胁必须通过才能实现的一些部分。比如，通过网络、在物理上接近、欺骗人等等。
  - 威胁的时序Sequence：
    - 威胁要实现所必经的步骤和顺序。与威胁的途径是一个从空间上，一个从时间上表达。也可以将这两个因素结合起来表达威胁的过程。
  - 威胁的手法：
    - 威胁要实现所需要的手法。比如：通道劫持、暴力破解、欺骗等
- **威胁的结果——事件Event/Incident：**威胁具体实现之后所造成的结果
  - 威胁的可能性：威胁产生结果变成事件的概率。
  - 威胁的影响范围：威胁产生结果后的影响大小。以及影响进一步扩散的特性。